MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
NATIONAL TECHNICAL UNIVERSITY OF UKRAINE
"IGOR SIKORSKY KYIV POLYTECHNIC INSTITUTE"

O. Synekop, I. Lytovchenko, O. Chugai

ENGLISH FOR PROFESSIONAL PURPOSES. INFORMATION TECHNOLOGIES & CYBERSECURITY

Coursebook

In 2 parts

Part I

Recommended by the Methodological Council of the Igor Sikorsky Kyiv Polytechnic Institute
as a study aid for bachelor's applicants
on the educational program "Systems of Technical Protection of Information",
"Systems, Technologies and Mathematical Methods of Cyber Security",
"Mathematical Methods of Cryptographic Security",
"Mathematical Methods of Modelling, Pattern Recognition and Computer Vision"
of the specialty F5 "Cybersecurity and data protection", F1 "Applied Mathematics"
of the field of knowledge F "Information technologies"

Electronic network educational edition

Kyiv
Igor Sikorsky Kyiv Polytechnic Institute
2026

UDC 811.111:004](075.8)
S 38

Authors: *Oksana Synekop*, Doctor of Pedagogical Sciences, professor of Department of English for Engineering No. 2 of the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
Iryna Lytovchenko, Doctor of Pedagogical Sciences, professor of Department of English for Engineering No. 2 of the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
Oksana Chugai, PhD, associate professor of Department of English for Engineering No. 2 of the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"

Reviewers: *Olena Ilienko*, Doctor of Pedagogical Sciences, Professor, Head of the Department of Foreign Philology and Translation of O.M. Beketov National University of Urban Economy in Kharkiv
Olena Sachuk, PhD, associate professor of the Department of Language Studies of the National Medical University named after O.O. Bogomolets
Iryna Stavytska, PhD, associate professor of Department of English for Engineering No. 2 of the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
Tetiana Lytvynova, PhD, associate professor of Department of Information Security of the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
Inna Antonenko, PhD, associate professor of the Department of English Language for Humanities No. 3 of the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"

Responsible editor *Tetiana Golub*, PhD, associate professor, associate professor of Department of English for Engineering No. 2 of the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"

The approval was granted by the Methodological Council of Igor Sikorsky Kyiv Polytechnic Institute
(minutes of meeting No. 6 dated 03.04.2026)
upon the submission of the Academic Council of Faculty of Linguistics
(minutes of meeting No. 13 dated 26.03.2026)

Synekop O.

S 38 English for Professional Purposes. Information Technologies & Cybersecurity. In 2 parts. Part I. [Electronic resource] : coursebook for bachelor's applicants on the educational program "Systems of Technical Protection of Information", "Systems, Technologies and Mathematical Methods of Cyber Security", "Mathematical Methods of Cryptographic Security", "Mathematical Methods of Modelling, Pattern Recognition and Computer Vision" of the specialty F5 "Cyber security and data protection", F1 "Applied Mathematics" / O. Synekop, I. Lytovchenko, O. Chugai; Igor Sikorsky Kyiv Polytechnic Institute. – Electronic text data (1 file). – Kyiv : Igor Sikorsky Kyiv Polytechnic Institute, Publishing House "Polytechnica", 2026. – 406 p.

ISBN 978-966-990-285-6 (e-Book)
ISBN 978-966-990-283-2 (e-Book, Part 1)

English for Professional Purposes. Information Technologies & Cybersecurity (Part I) is a coursebook designed for differentiated instruction, tailored to university students pursuing careers in the IT field. This coursebook is suited for intermediate to advanced university students. It enhances their professional communication skills in English. It also advances their technical, career and critical thinking abilities. By engaging with the content, students are not only able to refine their language proficiency but also cultivate essential IT competencies and foster creativity and analytical skills necessary for success in the IT industry.

The units cover a range of IT topics: "IT Project Management Methods", "Types of Websites", "Website Design. Security of Websites", "Web Servers. Security of Webservers", "Classical Cryptography. Ciphers and Codes", "Cryptanalysis", "Steganography", "Digital Watermarking", "Identification. Verification. Authentication. Authorisation. Accounting", "Passwords", "Biometrics", "Security Tokens".

Each unit includes a set of tasks and exercises designed for all students in the group, and with tailored activities for students' varying levels of foreign language proficiency (B1 and B2) and diverse learning styles.

One of the obvious advantages of the proposed coursebook is its interactivity, which involves links to additional sources of information, videos, dictionary, tasks.

UDC 811.111:004](075.8)

ISBN 978-966-990-285-6 (e-Book)
ISBN 978-966-990-283-2 (e-Book, Part I)

Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

О. С. Синекоп, І. М. Литовченко, О. Ю. Чугай

АНГЛІЙСЬКА МОВА ПРОФЕСІЙНОГО СПРЯМУВАННЯ. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА КІБЕРБЕЗПЕКА

Навчальний посібник

У 2-х частинах

Частина І

Рекомендовано Методичною радою КПІ ім. Ігоря Сікорського
як навчальний посібник для здобувачів першого (бакалаврського) рівня вищої освіти
за освітніми програмами «Системи технічного захисту інформації»,
«Системи, технології та математичні методи кібербезпеки»,
«Математичні методи криптографічного захисту інформації»,
«Математичні методи моделювання, розпізнавання образів та комп'ютерного зору»
спеціальності F5 «Кібербезпека та захист інформації», F1 «Прикладна математика»
галузі F «Інформаційні технології»

Електронне мережеве навчальне видання

Київ
КПІ ім. Ігоря Сікорського
2026

УДК 811.111:004](075.8)
С 38

Автори: *Синекоп Оксана Степанівна*, д-р пед. наук, доц., професор кафедри англійської мови технічного спрямування № 2 Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»
Литовченко Ірина Миколаївна, д-р пед. наук, проф., професор кафедри англійської мови технічного спрямування № 2 Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»
Чугай Оксана Юріївна, канд. пед. наук, доц., доцент кафедри англійської мови технічного спрямування № 2 Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»

Рецензенти: *Ільєнко О. Л.*, д-р пед. наук, проф., завідувач кафедри іноземної філології та перекладу Харківського національного університету міського господарства імені О. М. Бекетова
Сачук О. В., канд. пед. наук, доц., доцент кафедри мовної підготовки Національного медичного університету імені О. О. Богомольця
Ставицька І. В., канд. пед. наук, доц., доцент кафедри англійської мови технічного спрямування № 2 Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»
Литвинова Т. В., канд. техн. наук, доц., доцент кафедри інформаційної безпеки Навчально-наукового фізико-технічного інституту Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»
Антоненко І. І., канд. пед. наук, доц., доцент кафедри англійської мови гуманітарного спрямування № 3 Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»

Відповідальний редактор *Голуб Т. П.,* канд. пед. наук, доц., доцент кафедри англійської мови технічного спрямування № 2 Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»

Гриф надано Методичною радою КПІ ім. Ігоря Сікорського
(протокол № 6 від 03.04.2026 р.)
за поданням вченої ради факультету лінгвістики
(протокол № 13 від 26.03.2026 р.)

Синекоп О. С.

С 38 Англійська мова професійного спрямування. Інформаційні технології та кібербезпека. У 2-х ч. Ч. І [Електрон. ресурс] : навч. посіб. для здобувачів першого (бакалаврського) рівня вищ. освіти за освіт. програмами «Системи технічного захисту інформації», «Системи, технології та математичні методи кібербезпеки», «Математичні методи криптографічного захисту інформації», «Математичні методи моделювання, розпізнавання образів та комп'ютерного зору» спец. F5 «Кібербезпека та захист інформації», F1 «Прикладна математика» галузі F «Інформаційні технології» / Уклад. : О. С. Синекоп, І. М. Литовченко, О. Ю. Чугай ; КПІ ім. Ігоря Сікорського. – Електрон. текст. дані (1 файл). – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2026. – 406 с.

ISBN 978-966-990-285-6 (Ел.)
ISBN 978-966-990-283-2 (Ел., Ч. 1)

Перша частина навчального посібника «Англійська мова професійного спрямування. Інформаційні технології та кібербезпека» призначена для диференційованого навчання професійно орієнтованого англомовного спілкування здобувачів першого (бакалаврського) рівня вищої освіти, студентів – майбутніх ІТ-фахівців університетів. Метою навчального посібника є розвиток професійно орієнтованих англомовних компетентностей в аудіюванні, говорінні, читанні й письмі на достатньому рівні володіння мовою (B2) у студентів – майбутніх ІТ-фахівців.

Навчальний посібник містить три розділи, кожен з яких охоплює чотири підрозділи: «Методи управління ІТ проєктами», «Типи вебсайтів», «Вебдизайн та безпека вебсайтів», «Вебсервери та їх безпека»; «Класична криптографія. Шифри і коди», «Криптаналіз», «Стеганографія», «Цифрові водяні знаки»; «Ідентифікація. Верифікація. Аутентифікація. Авторизація», «Паролі», «Біометрія», «Токени безпеки».

Кожен підрозділ містить вправи однакові для всіх студентів, вправи для студентів з різним рівнем володіння іноземною мовою та стилем навчання. Доцільними і цікавими є вправи і завдання із залученням інструментів штучного інтелекту у різні блоки навчального посібника.

УДК 811.111:004](075.8)

ISBN 978-966-990-285-6 (Ел.)
ISBN 978-966-990-283-2 (Ел., Ч. 1)

CONTENTS

Foreword 9
Передмова 11
UNIT 1 13
1.1. IT PROJECT MANAGEMENT METHODS 14
WARM UP 14
READING 16
USE OF ENGLISH 22
VOCABULARY 22
PHRASAL VERBS 25
GRAMMAR 27
LISTENING 29
SPEAKING 30
WRITING 33
REFLECTION AND SYNTHESIS 35
1.2. TYPES OF WEBSITES 36
WARM UP 36
READING 38
USE OF ENGLISH 44
VOCABULARY 44
IDIOMS 47
GRAMMAR 49
LISTENING 51
SPEAKING 54
WRITING 55
REFLECTION AND SYNTHESIS 57
1.3. WEBSITE DESIGN. SECURITY OF WEBSITES 58
WARM UP 58
READING 60
USE OF ENGLISH 67
VOCABULARY 67
PHRASAL VERBS 69
GRAMMAR 70
LISTENING 76
SPEAKING 79
WRITING 81
REFLECTION AND SYNTHESIS 83
1.4. WEB SERVERS. SECURITY OF WEB SERVERS 84
WARM UP 84
READING 86
USE OF ENGLISH 93

VOCABULARY 93
IDIOMS 94
GRAMMAR 96
LISTENING 99
SPEAKING 101
WRITING 103
REFLECTION AND SYNTHESIS 104
1.5. UNIT 1. REVISION 1 105
UNIT 2 119
2.1. CLASSICAL CRYPTOGRAPHY. CIPHERS AND CODES 120
WARM UP 120
READING 123
USE OF ENGLISH 130
VOCABULARY 130
PHRASAL VERBS 132
GRAMMAR 133
LISTENING 137
SPEAKING 139
WRITING 141
REFLECTION AND SYNTHESIS 142
2.2. CRYPTANALYSIS 143
WARM UP 143
READING 144
USE OF ENGLISH 151
VOCABULARY 151
IDIOMS 152
GRAMMAR 153
LISTENING 159
SPEAKING 160
WRITING 163
REFLECTION AND SYNTHESIS 163
2.3. STEGANOGRAPHY 164
WARM UP 164
READING 165
USE OF ENGLISH 173
VOCABULARY 173
PHRASAL VERBS 174
GRAMMAR 176
LISTENING 180
SPEAKING 182
WRITING 183
REFLECTION AND SYNTHESIS 185

2.4. DIGITAL WATERMARKING 186
WARM UP 186
READING 187
USE OF ENGLISH 194
VOCABULARY 194
IDIOMS 195
GRAMMAR 197
LISTENING 200
SPEAKING 203
WRITING 204
REFLECTION AND SYNTHESIS 205
2.5. UNIT 2. REVISION 2 206
UNIT 3 221
3.1. IDENTIFICATION. VERIFICATION. AUTHENTICATION. AUTHORISATION. ACCOUNTING 222
WARM UP 222
READING 223
USE OF ENGLISH 230
VOCABULARY 230
PHRASAL VERBS 231
GRAMMAR 232
LISTENING 236
SPEAKING 238
WRITING 239
REFLECTION AND SYNTHESIS 240
3.2. PASSWORDS 241
WARM UP 241
READING 243
USE OF ENGLISH 249
VOCABULARY 249
IDIOMS 250
GRAMMAR 251
LISTENING 256
SPEAKING 258
WRITING 261
REFLECTION AND SYNTHESIS 262
3.3. BIOMETRICS 263
WARM UP 263
READING 264
USE OF ENGLISH 271
VOCABULARY 271
PHRASAL VERBS 272

GRAMMAR 273
LISTENING 278
SPEAKING 279
WRITING 283
REFLECTION AND SYNTHESIS 285
3.4. SECURITY TOKENS 286
WARM UP 286
READING 287
USE OF ENGLISH 294
VOCABULARY 294
IDIOMS 296
GRAMMAR 297
LISTENING 300
SPEAKING 301
WRITING 303
REFLECTION AND SYNTHESIS 304
3.5. UNIT 3. REVISION 3 305
References 318
Appendix 1. Mini-Dictionary 326
Appendix 2. Phrasal Verbs & Idioms 340
Appendix 3. Grammar Bank 345
Appendix 4. Tapescripts 369
Appendix 5. Psychological Tests 404
Appendix 6. Roadmap for Teachers and Students on How to Use this Coursebook 406

Foreword

English for Professional Purposes. Information Technologies & Cybersecurity (Part I) is a coursebook designed for differentiated instruction, tailored to university students pursuing careers in the IT field. This coursebook is suited for intermediate to advanced university students. It enhances their professional communication skills in English. It also advances their technical, career and critical thinking abilities. By engaging with the content, students will not only refine their language proficiency but also cultivate essential IT competencies and foster creativity and analytical skills necessary for success in the IT industry.

The material is designed to be flexible. The tasks and exercises are tailored to students with different learning styles and levels of foreign language proficiency.

At the core of the material is the belief that students are able to learn more effectively if they are actively and personally involved in their foreign language learning. Therefore, throughout the units, students are encouraged to express their opinions on issues relating to different aspects of the IT sector, discuss and evaluate its role in society.

The units cover a range of IT topics: "IT Project Management Methods", "Types of Websites", "Website Design. Security of Websites", "Web Servers. Security of Webservers", "Classical Cryptography. Ciphers and Codes", "Cryptanalysis", "Steganography", "Digital Watermarking", "Identification. Verification. Authentication. Authorisation. Accounting", "Passwords", "Biometrics", "Security Tokens". Authentic texts from websites, video and audio materials, books and articles are included in a coursebook. Each sub-unit provides a warm up section, a reading section, a use of English section, a listening section, a speaking section, a writing section, and a reflection and synthesis section. The coursebook also includes different appendices.

Special attention is given to the *Revision Section* offered at the end of the units. In this section, the students can not only review the material but also complete interesting projects.

The coursebook is accompanied by different appendices such as Mini-dictionary, Phrasal Verbs & Idioms, Grammar Bank, Tapescripts, Psychological Tests, Roadmap for Teachers and Students on How to Use this Coursebook. In the Grammar Bank section students can review grammar rules and do additional exercises.

Each unit includes a set of exercises designed to cater to diverse learning needs:

1) exercises marked "A. & B." – for all students in the group;
2) exercises tailored to different levels of foreign language proficiency, with Exercise A for B1 and Exercise B for B2;
3) exercises adapted to various learning styles, considering modality preferences – such as visual, auditory, kinesthetic, or mixed modalities.

Throughout the course, students can switch between different learning styles (dominant and non-dominant) to enhance their ability to develop various language skills more effectively.

The exercises can be carried out independently, in pairs or in small groups. The units are developed for either classroom or self-study use.

One of the key advantages of the proposed coursebook is its interactivity, which involves links to additional sources of information, videos, and dictionary. In addition, the format of the material presentation involves students in creating mind maps, filling in tables, and conducting surveys, designed to construct professionally oriented English-language knowledge by consolidating their own experience.

The exercises and tasks involving AI tools throughout various sections of the coursebook are both engaging and relevant. These activities enable students to enhance their lexical and grammatical skills, analyse text fragments effectively, paraphrase information accurately, and think critically.

The authentic information for the units has been sourced from different printed and electronic materials. A list of references is provided.

In developing this material we have enjoyed working with students, colleagues, specialist teachers and friends, and we are deeply grateful for their contributions, feedback and support. We hope you enjoy it as much as we did creating it.

Authors

Передмова

Навчальний посібник «Англійська мова професійного спрямування. Інформаційні технології та кібербезпека (частина І)» призначений для здобувачів першого (бакалаврського) рівня вищої освіти Навчально-наукового фізико-технічного інституту (спеціальності F5 «Кібербезпека та захист інформації» та F1 «Прикладна математика» галузі F «Інформаційні технології»).

Провідною метою навчального посібника є розвиток професійно орієнтованих англомовних комунікативних компетентностей в аудіюванні, говорінні, читанні і письмі на достатньому рівні володіння мовою (B2) у студентів – майбутніх ІТ-фахівців. Використання цього посібника сприяє оптимізації організації навчання іноземної мови в аудиторний і позааудиторний час, поглибленню фахових знань, посиленню самостійності й автономії студентів, розвитку вмінь творчого та критичного мислення у майбутніх ІТ-фахівців.

Специфікою цього навчального посібника є комплексне врахування індивідуальних особливостей майбутнього ІТ-фахівця, зокрема його рівня володіння іноземною мовою та навчального стилю. Це дозволяє забезпечити більш ефективний процес навчання, адаптуючи матеріал під потреби кожного студента та сприяючи кращому засвоєнню знань.

Навчальний посібник є першою частиною циклу й містить три розділи, кожен з яких охоплює по чотири підрозділи. Усі розділи безпосередньо пов’язані з тематикою ІТ-галузі. Так, у перший розділ увійшли підрозділи з такою тематикою: «Методи управління ІТ-проєктами», «Типи вебсайтів», «Вебдизайн та безпека вебсайтів», «Вебсервери та їх безпека». Теми другого розділу включають: «Класична криптографія. Шифри і коди», «Криптаналіз», «Стеганографія», «Цифрові водяні знаки». Третій розділ охоплює тематичні підрозділи: «Ідентифікація. Верифікація. Аутентифікація. Авторизація», «Паролі», «Біометрія», «Токени безпеки».

Використані автентичні тексти з вебсайтів, відео- та аудіоматеріали, фахові книги та статті. Усі підрозділи включають шість блоків («Розминка»; «Читання»; «Використання мови» (лексика, ідіоми та фразові дієслова, граматика); «Аудіювання»; «Говоріння»; «Письмо»; «Рефлексія та синтез»), що орієнтовані на розвиток професійно орієнтованих англомовних умінь аудіювання, читання, говоріння та письма. Блок «Рефлексія та синтез» передбачає практикування у синтезуванні і рефлексуванні засвоєної інформації на основі «хмарини слів» наприкінці кожного підрозділу.

Особливу увагу приділено розділу «Повторення», який пропонується наприкінці першого, другого та третього розділів навчального посібника. Він побудований таким чином, що студенти можуть не тільки повторити навчальний матеріал, а й виконати цікаві проєкти.

Комплекси вправ містять:

1) вправи однакові для всіх студентів групи («A. & B.»);
2) вправи для студентів з різним рівнем володіння іноземною мовою (вправа «A» відповідає рівню B1, вправа «B» відповідає рівню B2);
3) вправи для студентів з різним стилем навчання за модальністю: зорова, аудіальна, кінестетична та змішана модальності.

У вправах враховуються пріоритети студентів працювати самостійно, в парах чи в малих групах. Студент обирає вправи відповідно до домінуючого чи недомінуючого навчального стилю. Різноманітність та достатня кількість вправ дозволяють викладачу ефективно організувати аудиторну і позааудиторну роботу студентів.

До очевидних переваг пропонованого навчального посібника варто зарахувати його інтерактивність, що полягає у залученні покликань до додаткових джерел інформації, відеоматеріалів, словника, окремих завдань. До того ж формат презентації матеріалу передбачає безпосереднє заповнення студентами схем і таблиць, покликаних конструювати професійно орієнтовані англомовні знання, узагальнюючи власний фаховий досвід.

Доцільними і цікавими є вправи і завдання із залученням інструментів штучного інтелекту у різні блоки навчального посібника. Імплементація таких вправ і завдань дозволяє розвивати у студентів лексичні і граматичні навички, аналізувати запропоновані фрагменти тексту, перефразовувати надану інформацію, критично мислити. Виконуючи вправи, студенти вчаться застосовувати різні стратегії, що дозволяє їм бути гнучкими, організованими та швидко приймати рішення.

Навчальний посібник супроводжується низкою додатків: 1) міні-словничок до підрозділів, 2) граматичний банк з додатковими вправами, 3) скрипти аудіо- та відеозаписів, 4) психологічні тести, 5) методичні рекомендації для викладачів і студентів щодо використання цього навчального посібника. Автентичні матеріали, використані для ефективного навчання і викладання іноземної мови, було взято з різних друкованих та електронних джерел та подано перелік посилань.

Ми дякуємо усім студентам, колегам та друзям за участь, поради та коментарі в процесі розробки навчального посібника. Сподіваємось, що цей навчальний посібник не тільки сприятиме покращенню знань студентів з професійно орієнтованої англійської мови, а й принесе їм задоволення в освітньому процесі.

Автори

UNIT 1

UNIT	WARM UP	READING	USE OF ENGLISH	LISTENING	SPEAKING	WRITING	REFLECTION
1.1. IT Project Management Methods	Students' background knowledge about IT project management methods	Agile project management	Language use in terms of the topic. Present tenses	DevOps in 5 minutes	Speaking about IT management methods, their specifics, advantages, disadvantages	Writing definitions of terms; engaging in independent and AI paraphrasing; writing summary of the written text	Reflecting and synthesising
1.2. Types of Websites	Students' background knowledge about types of websites	Static and dynamic websites. Expanding vocabulary using AI	Language use in terms of the topic. Present tenses	Popular types of websites that you should know	Speaking about the specifics of different types of websites	Writing a paragraph; analysing the paragraph created by AI and simplifying it; writing a blog entry	Reflecting and synthesising
1.3. Website Design. Website Security	Students' background knowledge about website design	Web design basics	Language use in terms of the topic. Present tenses	How to perform a website security check	Speaking about the security of websites	Compressing information independently and using AI tools; writing summary of the audio text	Reflecting and synthesising
1.4. Web Servers. Security of Web Servers	Activating students' background knowledge about web servers	Web servers	Language use in terms of the topic; expanding vocabulary using AI. Present tenses	Demystifying web server hacking: techniques, vulnerabi-lities, and counter-measures	Speaking about security of web servers	Writing a paragraph; a blog entry	Reflecting and synthesising

1.1. IT PROJECT MANAGEMENT METHODS

WARM UP

1. **Using your background knowledge about different aspects of *IT Project Management,* do the tasks according to your learning style (dominant or non-dominant modality).**

1.1. ***Visual Modality***

Work individually and then in a small group. Define the specific categories of words and phrases related to the IT project. Describe the specifics of each category. Explore how they are interconnected within the context of the IT project.

purpose		**finance**	**changing goals**	**delays**	**cost**
time	**scope**	**people**	**unclear roles and resposibilities**	**incorrectly defined requirements**	**sponsors not involved**
		implementation			
risks			**lack of communication**	**skills gaps**	**insufficient resources**
IT Project Management					
	initiating		**user**	**product owner**	
planning			**product manager**		**tester**
	executing			**test analyst**	
		monitoring	**team lead**		**developer**
closing				**QA manager**	

1.2. *Auditory Modality*

Work in a small group. Discuss the following questions.

1. What is a project?
2. What is an IT project?
3. What is management? Why is it important for different fields of knowledge?
4. What does IT project management include?
5. There are specific phases within a project, which are unique to each project and represent the project life cycle. What are they?
6. What are the main functions of users, customers and stakeholders?
7. Who is running a project?
8. What is a requirement?
9. Have you ever participated in any IT Project? Tell about your experience.

1.3. *Kinesthetic Modality*

The role of a manager is essential in the IT project. He / She has to possess a mix of personal, project, and team traits. Choose one of the cards and outline the key traits of an effective IT project manager according to the suggested areas.

Card 1	**Card 2**	**Card 3**
Personal Area	**Project Area**	**Team Area**
is sociable ……. ……. ……. ……. …….	is able to develop IT project ……. ……. ……. ……. …….	is able to monitor the activity of the team members ……. ……. ……. ……. …….

READING

You are going to read an article about Agile project management.

2. **1. A. & B. Before reading, discuss the following quotation.**

"The important thing is not your process. The important thing is your process for improving your process."

Henrik Kniberg, Agile trainer and author

2. A. & B. Before reading, look at the following words and phrases, which have been taken from the text. In what context might they be mentioned? Use Merriam-Webster Dictionary if necessary.

Management, ad hoc, fledgling, sprint, software development, backlog, scrum, agile, stakeholders, misconceptions, requirements, discreet development, sustainable development, iterative.

3. **A. & B. Read the text "Agile Project Management". Answer the following questions.**

1. What is Agile project management? When was the "Agile Software Development Manifesto" developed?
2. What are the principles of the Agile manifesto? What are the values of the Agile manifesto?
3. What are common phases in the Agile methodology?
4. What do participants of the Agile project have to do at the first and second steps?
5. What is the difference between release plan and sprint planning?
6. What is the role of progress tracking?
7. What is the difference between sprint reviews and sprint retrospectives?
8. Why is continuous learning considered to be a requirement of Agile?

AGILE PROJECT MANAGEMENT

By C. Reaiche, S. Papavasiliou

Agile project management is defined as an iterative approach to managing projects, focused on continuous and incremental release of outputs. Within these incremental releases, clients and end users are able to provide feedback, and changes or updates are able to be made.

Within Agile project management there are four core values: individuals and interactions over processes and tools; working software over comprehensive documentation; customer collaboration over contract negotiation; responding to change over following a plan.

From these values flow agile governance, which follows the same principles of being iterative and flexible. Agile requires rapid decision-making, using minimum-effort governance processes and without the need for heavy front-end planning. There are identifiable governance points within the Agile process including authority, standard practices, metrics, and artifacts, which are part of the planning phase. Therefore, for Agile governance to occur, there needs to be: collaboration over conformance, enablement over inspection, continuous monitoring over quality gates, transparency over management reporting.

Collaboration, both within and outside the organisation, is a vital component of successful implementation of Agile. Stakeholders' commitment needs to be sought early on to promote transformation, adaptation and flexibility, and there must be alignment between organisational strategies and business plans.

Within the Agile Manifesto (2001), there are 12 key principles of Agile project management:

1. The number one priority is customer satisfaction through the early and continuous delivery of valuable outcomes.

2. Changing developments are welcome, even late in development. Agile processes harness change for the customer's competitive advantage.
3. Deliver working outputs frequently, from a couple of weeks to a couple of months, with a preference for the shorter timescale.
4. Businesspeople and developers must work together daily throughout the project.
5. Build projects around motivated individuals. Give them the environment and support they need and trust them to do the job.
6. The most efficient and effective method of conveying information to and within a development team is face-to-face conversation.
7. Working outputs are the primary measure of progress.
8. Agile processes promote sustainable development. The sponsors, developers, and users should be able to maintain a constant pace indefinitely.
9. Continuous attention to technical excellence and good design enhances agility.
10. Simplicity – the art of maximising the amount of work not done – is essential.
11. The best architectures, requirements, and designs emerge from self-organising teams.
12. At regular intervals, the team reflects on how to become more effective, then tunes and adjusts its behaviour accordingly.

The Agile methodology typically involves several common phases: 1) planning and discussion, 2) design, 3) implementation and testing, 4) release, and 5) feedback. There are seven steps that can be used to support the implementation of the Agile project management:

1. Document the project vision and scope during the planning meeting, involving key stakeholders to clarify target clients, needs, product details, and benefits.
2. Develop a high-level project roadmap translating planning outcomes into a timeline with goals, features, and metrics, supported by stakeholders.

3. Create a release plan outlining 3–5 sprints with proposed dates, updated quarterly in collaboration with the team.
4. Conduct sprint planning to define tasks, goals, and backlog items for each short iteration, usually lasting around 2 hours.
5. Track progress via daily 15-minute stand-ups where team members report on work completed, planned, and challenges.
6. Hold sprint reviews to showcase completed work and gather feedback for continuous improvement.
7. Perform sprint retrospectives to evaluate what worked, what didn't, and identify improvements, then restart the sprint planning cycle.

In sum, Agile methodologies are cyclical project management processes that support organisations, project managers, and teams. This approach supports projects which are unclear and require iterative outcomes. The Agile approach requires the project team to collaborate with clients and key stakeholders throughout. Through this approach, outcomes are supported, the team is goal oriented, and making incremental improvements. The following methodologies are part of the Agile family: Scrum, Kanban, Scrumban.

Borrowed and modified from: Reaiche, C., & Papavasiliou, S. (2022). Management methods for complex projects. James Cook University, https://jcu.pressbooks.pub/pmmethods

4. A. & B. Read the text again and do the following tasks.

4.1. Fill in the missing information in statements 1–8.

1. The term "agile" refers to an _____ approach.
2. According to the Agile methodology, it is not the _____ but the _____ that is an important element.
3. The most efficient method of sharing information is _____ conversation.

4. Agile processes _____ change for the customer's _____ advantage.
5. At regular intervals, the team _____ on how it can become more effective, and then _____ and adapts its behaviour appropriately.
6. The project team works with the _____, project manager and Scrum master to create the plan.
7. Each goal should include: date, name, _____, features, _____.
8. After each sprint a _____ is used to understand what worked and what requires improvement from the previous sprint.

4.2. Decide which statements are *true* and which are *false*.

1. Collaboration is an important component of successful implementation of Agile.
2. The primary measure of progress is the amount of time spent on a task, not the actual results produced from the work.
3. Agile requires rapid decision making with minimal governance processes. But it requires heavy front-end planning.
4. Agility is enhanced by a constant focus on technical excellence and good design.
5. At regular intervals, the team reflects on how to become more effective, and then adjusts and adapts its behaviour accordingly.
6. The first meeting for strategic planning requires the project team to consider the scope.
7. The release should document between 3 to 5 sprints.
8. Daily stand-ups allow you to monitor the team progress.

5. **A. & B. In pairs, select one word from the provided list. Student A asks the questions below, putting the chosen word into each question, while Student B responds using that word. You may skip any questions that do not apply. After completing the questions, switch roles and repeat the activity with a different word. See the example below.**

Agile, requeriment, project, development, stakeholder, customer, sustainable, sprint, iteration, team, collaboration, discreet, product, cycle, user, framework, technology, approach, management.

1. What does _____ mean?
2. What is the plural / singular of _____?
3. What is the synonym of _____?
4. What is the opposite of _____?
5. What is the noun for _____?
6. What is the verb for _____?
7. What is the adjective for _____?
8. What is the adverb for _____?
9. What collocations do you know with _____?
10. How to use _____ in a sentence?
11. What is the Ukrainian translation for _____?

For example:

The chosen word is "project".

Student A: "What does project mean?"

Student B: "Project" is a planned set of activities or tasks intended to achieve a specific goal.

Student A: "What is the plural of project?"

Student B: "Projects."

6. **A. & B. Make a list of the five most important things that you have to remember about the Agile project management. Compare your list to your partner's. Which three are the most popular among the class?**

USE OF ENGLISH

VOCABULARY

7. **Choose one of the exercises and do it.**

A. Match roles with responsibilities of the Agile project participants.

Writes code; serves as a link between the customer and the development team, manages the product backlog, sets the scope, approves releases; uses the digital product, identifies issues, provides feedback; develops test cases, reviews code, tests; participates in defining, starting and ending the project; realises project management.

Roles		Responsibilities
1	User	
2	Customer	
3	Product Owner	
4	Scrum Master	
5	Developer	
6	Tester	

B. Match the key terms (1–10) with their definitions (a–i).

1. Software development	6. Developer
2. Agile methodology	7. Software
3. Manifesto	8. Scrum master
4. Scrum	9. User story
5. Sprint	10. Requirement

a a framework that is focused on helping teams deliver complex projects in a collaborative manner.

b a project management approach that focuses on flexibility, collaboration, and staged development.

c a concise description of a requirement from an end user's perspective. It follows a simple template that includes a user persona, a goal, and the desired outcome.

d a collection of code / computer programs that is designed to perform specific tasks on a device.

e a process of developing apps to complete the specific requirement.

f a period (2–4 weeks), during which a development team works to complete a set of outlined tasks or goals.

g a person who is involved in the creation, designing, programming, testing, and maintenance of digital products.

h a public declaration of intentions written by a group or organisation to outline their goals.

i responsible for facilitating the framework and ensuring the team follows the agile principles.

8. **Choose one of the exercises and do it.**

A. Complete the sentences. Use: *framework, values, stakeholders, scrum master, incremental, requirements, iterative, change, team, priorities, artifacts, sprints*.

1. The Agile Manifesto is a document that contains four _____ and twelve principles. It was developed in 2001.
2. The Agile framework is considered as an _____ methodology.

3. Scrum uses three roles, three processes, and three _____ as the _____ for organising and performing work.
4. Scrum, as an Agile approach for small teams, includes _____ and is led by a _____ who is responsible for removing barriers while performing team members' daily tasks.
5. In Scrum the project managers are able to control all types of iterative and _____ processes.
6. A product backlog is an ordered list of tasks, functions, _____ and other elements that must be implemented within the project.
7. Agile approach uses _____ to benefit the customer's competitive edge.
8. Agile provides many opportunities to interact with _____ and the team – before, during and after each sprint.
9. By involving the client in the project development, a high degree of cooperation between the client and the _____ can be obtained, giving the group more opportunities to understand the final product.
10. Agile approach provides a unique opportunity for customers to participate in the IT project – to determine _____ and functions, plan iterations and reviews.

B. Complete the sentences.

1. People and communication are more important than relying solely on _____ and tools.
2. Functional software is more important than having extensive _____.
3. Working closely with _____ is more valuable than focusing only on terms.
4. Readiness for changes is more important than following the original _____.
5. The Agile method relies on dividing the planning and implementation of projects into _____ (sprints), which allows the project participans to continuously adapt and improve the plan, scope of work and structure throughout the entire project.

6. Teams often break Agile projects into sprints, or project intervals, lasting 1–4 weeks, each of which ends with a product _____.
7. Agile methodology is based on the belief that motivated, independent and highly qualified _____ are needed to achieve the best results and develop the best products.
8. Since your team regularly develops versions of the product and immediately receives customer _____, the risk of project failure is reduced to a minimum.
9. In the Agile methodology, changes are made with minimal _____, regardless of the stage of work.
10. _____ is the basis of the Agile method, allowing you to focus attention on the sprint goals or a specific result.

PHRASAL VERBS

9. **A. Fill in the correct particles. Then, explain the phrasal verbs. See Appendix 2, which contains a list of relevant phrasal verbs.**

1. The team decided to **carry** _____ with the project despite the difficulties.
2. We need to **carry** _____ the test phase before deploying the software in production.
3. The lessons we have learnt from this project will help us **carry** _____ improvements in future initiatives.
4. It is important to **carry** _____ our scheduled updates to maintain the security of the software.
5. We plan to **change** _____ to a new coding framework to improve the performance of our application.
6. After a review of the feedback, we will **change** _____ our development approach to be more responsive to user needs.

7. If the new tool dosn't work, we can easily **change** _____ to the previous project management software.
8. In response to feedback from the team, we will **change** _____ the time of the meeting.
9. The **change** _____ scope required us to rethink our schedule and resource planning.

B. Replace the words or phrases in bold with the correct form of a phrasal verb using *carry* and *change*. Then, create three interconnected sentences that include any phrasal verbs with "carry" and "change".

1. When the team decided **to move** to a new project management tool, they wanted to ensure that everyone was trained to take full advantage of it.
2. During the sprint planning meeting, the team decided **to alter** their approach to daily stand-ups to enhance communication.
3. In spite of the setbacks experienced in the last iteration, the team decided **to continue** and to push through in order to meet the upcoming deadline.
4. The Scrum Master instructed everyone **to perform** the tasks efficiently to keep the sprint on track.
5. The team decided **to return** to the previous system after realising that the new workflow wasn't delivering the desired results.
6. In response to the team's feedback, the project manager decided **to reorganise** the roles to make better use of everyone's strengths.
7. The lessons learned from the last retrospective will help us **to transfer** our successes to the next iteration.
8. It's important that we **follow through** on our plans from the sprint in order to maintain trust within the team.
9. We had to adapt our processes to ensure that everyone was working efficiently due to the recent **modification** of the team structure.

GRAMMAR

10. A. & B. Write a second sentence that has a similar meaning to the first. Use the word in brackets. Use present tenses in the sentences below.

1. She hasn't finished working on completing her project using the Agile methodology yet. ***(still)***
2. The team began work on the project in September and is still working. ***(has)***
3. Mary has been writing the user story. It is finished now. ***(written)***
4. My work in the project has lasted 2 months so far. ***(I)***
5. The computer has been mine for three years. ***(had)***
6. We've had a fifteen-minute meeting. ***(been)***
7. He started working for this IT company three years ago. ***(been)***
8. It is 5 o'clock but the project hasn't been finished yet. ***(Now I)***

A. Choose the correct answer.

1. Kanban is a method that _____ with Scrum practices to enhance productivity and efficiency.

   a) can be using b) can be used c) can use

2. Kanban helps teams visualise their work, limit work in progress, and focus on _____ tasks in a timely manner.

   a) complet b) completed c) completing

3. By _____ Kanban, Scrum teams can better prioritise tasks, identify bottlenecks, and improve overall workflow transparency.

   a) use b) used c) using

4. Scrum can provide teams with a more flexible and adaptive approach to managing their projects, allowing for continual improvement and _____ collaboration.

   a) increased b) increasing c) increase

5. Kanban, a visual management system, _____ in the 1940s in Toyota's manufacturing plants in Japan.

   a) has originated b) originates c) originated

6. Taiichi Ohno, an engineer at Toyota, developed the system _____ efficiency and productivity in their production processes.

   a) improve b) to improve c) improving

7. The word "kanban" _____ as "signboard" or "billboard" in Japanese.

   a) interpretes b) interpreted c) is interpreted

8. The system uses visual cues to signal the need for materials or work _____ progress.

   a) at b) in c) of

9. Over time, Kanban _____ and implemented in various industries outside of manufacturing to streamline workflows and improve communication.

   a) has been adapted b) has adapted c) adapted

10. Visualisation in the Kanban methodology is the main advantage, thanks _____ which each team member has a comprehensive view of the project, and the project manager can adjust it if necessary.

    a) of b) in c) to

B. Put the words into the correct form.

Scrum is closely **1) _____ (connect)** to the Agile methodology. It is a framework in IT project management that focuses on **2) _____ (iteration)** and **3) _____ (increment)** development. It involves frequent **4) _____ (collaborate)**, feedback, and **5) _____ (adapt)** among team members to deliver products **6) _____ (efficient)**. Scrum teams work in short sprints, **7) _____ (common)** 2-4 weeks long, where they plan, execute, and review

the progress. The Scrum framework consists of particular roles (Scrum Master, Product Owner), events (Sprint Planning, Daily Standups), and artifacts (the product backlog, sprint backlog) to ensure clarity and **8) _____ (success)** in project **9) _____ (deliver)**. Due to **10) _____ (flexible)** and continuous improvement, Scrum allows teams to **11) _____ (reacting)** quickly to changes and bring benefit to stakeholders constantly.

LISTENING

You are going to watch a video that explores the specifics of DevOps.

11. A. & B. Before watching a video, check if you know the meaning of the words. Use Merriam-Webster Dictionary if necessary.

Feedback, confusion, implementation, infinity, executable, bugs, deployment, integration, reducing, idle.

12. Watch the video "DevOps in 5 minutes". Do the tasks.

12.1. Decide which statements are *true* and which are *false*.

1. Development teams work independently without any feedback from the operations team.
2. The DevOps approach is associated with an infinity sign that represents continuous improvement and activity.
3. The DevOps culture aims to streamline communication and collaboration between development and operations teams.
4. Selenium is considered to be the most popular tool for automation testing.
5. Netflix introduced its online streaming service in 2014.

12.2. Fill in the missing information in statements 1–5.

1. The development team is responsible for developing the plan, designs, and building the system from _____.

2. The operations team gave the development team feedback on any _____ that needed fixing and any _____ required.
3. The _____ phase starts once the planning is finished.
4. Maven and Gradle are used in the _____ stage.
5. Simian Army continuously created _____ (bugs) in the environment without _____ the users.

13. A. & B. Watch the video again. Answer the questions.

1. What benefits does the DevOps approach offer in terms of collaboration between development and operations teams?
2. What does the infinity symbol of DevOps symbolise?
3. What specific phases are involved in the implementation of the DevOps approach?
4. How is version control achieved within the DevOps approach?
5. What tools are used in different phases of the DevOps lifecycle?

SPEAKING

14. A. To deepen your understanding of the Lean Methodology, conduct online research. Then in discussion with your groupmate who is familiar with this methodology, clarify information about the specifics further. Use information provided in the table. Your conversation should include at least 5–6 exchanges per each participant. Be creative! Remember to keep the tone respectful!

Student A	Student B
1. I know that you developed software using the Lean management methodology two months ago. What are the main principles of the Lean methodology?	1. ……

Student A	Student B
2. …….	2. Taiichi Ohno outlined the original Lean wastes. Among them: defects, overproduction, waiting, transportation, motion, inventory, over processing.
3. What mistakes do people have when implementing Lean?	3. ……..
4. …….	4. PDSA, Kanban Boards, Gemba Walks, Daily Huddle Meetings
5. What are the main advantages of Lean methodology?	5. ……
6. …..	6. ……

B. Begin by researching the Six Sigma and PRiSM methodologies online. Then discuss with your groupmate the advantages of each methodology. Your dialogue should include at least 7–8 exchanges per each participant. Be creative! Remember to keep the tone respectful!

15. **A. Work in small groups. The current Agile Methodologies Workshop aims to familiarise participants with different project management methods such as Waterfall, Agile, Scrum, and others. Carry out an internet survey to understand the difference between methods used in the IT field. Fill in the table with your findings, focusing on specifics, advantages and diadvantages of different methods. Use information from both your survey and the provided text (Ex. 3). Then create a three-minute monologue to present your findings to your groupmates, encouraging questions and discussion at the end.**

Methods	Specifics	Advantages	Disadvantages
1. Waterfall			
2. Agile			

Methods	Specifics	Advantages	Disadvantages
3. Scrum			
4. Kanban			
5. Lean			
6. Critical Path Method (CPM)			
7. Critical Chain Management (CCM)			
8. Projects in Controlled Environments (PRINCE2)			
9. Project Management Body of Knowledge (PMBOK)			
10. PRiSM			
11. Six Sigma			
12. Extreme Project Management (XPM)			

B. You have decided to participate in the scientific conference. Your supervisor suggested you the list of topics. Choose one of the topics and prepare a presentation (up to 9–10 slides). Answer the questions after or during your presentation.

1. Agile vs. Waterfall methodologies.
2. Risk management strategies in IT projects.
3. Team management in IT projects.
4. The role of project management tools in enhancing IT project success.
5. Incorporating quality assurance and testing in IT project management.
6. Factors influencing successful project planning and execution in IT projects.
7. Future trends in the field of IT project management.

WRITING

16. **The current Agile Methodologies Training Session aims to introduce and reinforce the understanding of essential Agile terminology among team members, thereby enhancing effectiveness in our projects. Write definitions for the terms listed in the box below. Make sure that your definitions are clear and can be easily understood by team members who may be new to Agile practices. Give an example or context for how each term is used within Agile frameworks, if possible.**

Agile, stakeholders, scrum, requirements, iteration, team, sprint, user story.

17. **1. A. & B. Work with AI. Give your own paraphrasing in the second column. Then use any AI tool to paraphrase the collocations in the third column.**

Collocation	Student's paraphrasing	AI paraphrasing
1. *Agile project management is defined as …*	*Agile project management is determined / considered / described as …*	*The definition of agile project management is …*
2. *Within Agile project management there are 4 core values …*		
3. *From these values flow agile governance …*		
4. *Agile requires rapid decision-making …*		
5. *Collaboration, both within and outside the organisation, is an important component of Agile.*		

Collocation	Student's paraphrasing	AI paraphrasing
6. *Within the Agile Manifesto, there are 12 key principles …*		
7. *There are 7 steps that can be used to support …*		
8. *In sum, Agile methodologies are cyclical project management processes …*		

2. A. & B. For the research, you need to write a concise summary of the text in Ex. 3.

A. Write a 150–160 word summary.

B. Write a 180–200 word summary.

Use a five-key-step list:

1. **Read the text.**
2. **Split it into parts.**
3. **Define the key points in each part.**
4. **Create a summary.**
5. **Compare the summary with the article.**

REFLECTION AND SYNTHESIS

18. **You have completed this unit. This word cloud can help you to reflect on and synthesise the key concepts from the topic. Focus on the most important terms and ideas that stood out to you. Using the word cloud as a visual tool, you have to illustrate your understanding.**

1.2. TYPES OF WEBSITES

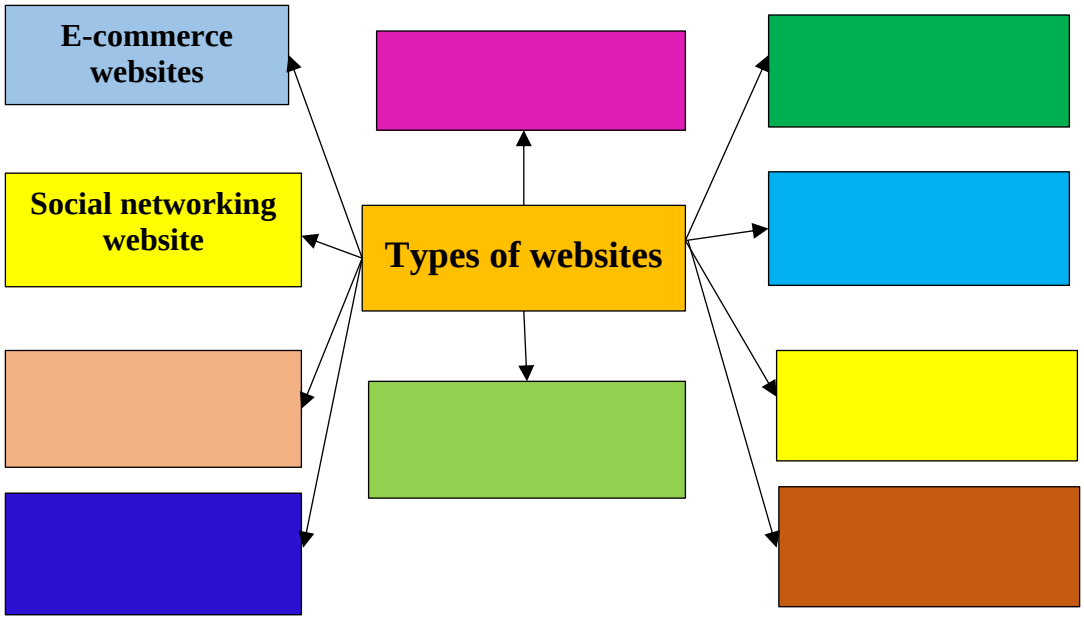
WARM UP

1. Using your background knowledge about different types of websites, do the tasks according to your learning style (dominant or non-dominant modality).

1.1. *Visual Modality*

Work individually and then in small groups. Create a mind map "Types of Websites". Specify the types of websites and give examples of the different types of websites as in the example.

E-commerce websites serve as online platforms that enable businesses and consumers to buy and sell products or services over the internet. The examples of e-commerce websites include Amazon, eBay, and Alibaba.



1.2. *Auditory Modality*

Work in small groups. Talk about website classification using the following categories:

- **owner** (*for example, personal websites − owned by an individual to share personal experiences, or interests, ……..*);
- **users' permission to view the website;**
- **objectives;**
- **access;**
- **used technologies;**
- **monetisation.**

1.3. *Kinesthetic Modality*

Conduct a survey about website usage within your group. Analyse the data to define the main trends. Then prepare a report summarising your findings.

1. What types of websites do you visit frequently?
    a) Social media platforms
    b) News websites
    c) Entertainment websites
    d) E-commerce websites
    e) Educational websites
    f) Your answer:
2. What types of websites do you avoid?
    a) Gaming websites
    b) Political websites
    c) Adult content websites
    d) Health-related websites
    e) Your answer:

3. How do you usually discover new websites to visit?
    a) Through search engines
    b) Recommendations from friends or family
    c) Advertisements
    d) Random browsing
    e) Your answer:
4. Do you have any concerns about online security or privacy while browsing different types of websites?
    a) Yes
    b) No
    c) Sometimes
5. What types of websites would you like to visit more in the future?
    a) Travel websites
    b) Fitness and health websites
    c) Environmental websites
    d) Career development websites
    e) Your answer:

READING

You are going to read an article about types of websites.

2. **1. A. & B. Before reading, discuss the quotations about websites.**

1. "A successful website does three things:
   It attracts the right kinds of visitors.
   Guides them to the main services or product you offer.
   Collect Contact details for future ongoing relation."

   Mohamed Saad
2. "Websites promote you 24/7: No employee will do that."

   Paul Cookson

2. A. & B. Before reading, look at the following words and phrases, which have been taken from the text. In what context might they be mentioned? Use Merriam-Webster Dictionary if necessary.

Static, dynamic, server, website, web page, navigation, content, non-interactive, to update, hosting, to monitor, to store, search request, to regenerate.

3. A. & B. Read the text "Static and Dynamic Websites". Then complete the table outlining the advantages and disadvantages of static and dynamic websites.

Static website

Advantages of static website	Disadvantages of static website
…….	…….
…….	…….
…….	…….
…….	…….
…….	…….

Dynamic website

Advantages of dynamic website	Disadvantages of dynamic website
…….	…….
…….	…….
…….	…….
…….	…….
…….	…….

STATIC AND DYNAMIC WEBSITES

A **website** (also written as a web site) is a collection of web pages and related content that is identified by a common domain name and published on at least one web server. Websites are typically dedicated to a particular topic or purpose, such as news, education, commerce, entertainment, or social media.

Hyperlinking between web pages guides the navigation of the site, which often starts with a home page. The most-visited sites are Google, YouTube, and Facebook.

STATIC WEBSITE

A static website is one that has Web pages stored on the server in the format that is sent to a client Web browser. It is built with fixed Hypertext Markup Language (HTML), Cascading Style Sheets (CSS) and JavaScript files that are pre-designed and do not change based on user interactions.

The static website is typically simpler in structure and functionality compared to a dynamic website, as it does not rely on server-side processing or databases to generate content. Images are commonly used to create the desired appearance and as part of the main content. Audio or video might also be considered “static” content if it plays automatically or is generally non-interactive. This type of website usually displays the same information to all visitors. Similar to handing out a printed brochure to customers or clients, a static website will generally provide consistent, standard information for an extended period of time.

Although the website owner may make updates periodically, it is a manual process to edit the text, photos, and other content and may require basic website design skills and software. Simple forms or marketing examples of websites, such as a classic website, a five-page website or a brochure website are often static websites, because they present pre-defined, static information to the user. This may include information about a company and its products and services through text, photos, animations, audio / video, and navigation menus.

The static website may still use server side includes (SSI) as an editing convenience, such as sharing a common menu bar across many pages. As the site's behavior to the reader is still static, this is not considered a dynamic site.

The static website may lack interactive features, personalised content, and scalability, making it less suitable for complex or interactive web projects. Hosting a static website is straightforward, and it offers fast loading speeds and enhanced security due to its static nature.

DYNAMIC WEBSITE

A dynamic website is one that changes or customises itself frequently and automatically. Server-side dynamic pages are generated "on the fly" by computer code that produces the HTML (CSS are responsible for appearance and thus, are static files). There are a wide range of software systems, such as CGI, Java Servlets and Java Server Pages (JSP), Active Server Pages and ColdFusion (CFML) that are available to generate dynamic Web systems and dynamic sites. Various Web application frameworks and Web template systems are available for general-use programming languages like Perl, PHP, Python and Ruby to make it faster and easier to create complex dynamic websites.

A site can display the current state of a dialogue between users, monitor a changing situation, or provide information in some way personalised to the requirements of the individual user.

For example, when the front page of a news site is requested, the code running on the webserver might combine stored HTML fragments with news stories retrieved from a database or another website via RSS to produce a page that includes the latest information.

Dynamic sites can be interactive by using HTML forms, storing and reading back browser cookies, or by creating a series of pages that reflect the previous history of clicks. Another example of dynamic content is when a retail website with a database of media products allows a user to input a search request, e.g. for the keyword Beatles. In response, the content of the Web page will spontaneously change the way it looked before, and will then display a list of Beatles products like CDs, DVDs, and books.

Dynamic HTML uses JavaScript code to instruct the Web browser how to interactively modify the page contents. One way to simulate a certain type of dynamic website while avoiding the performance loss of initiating the dynamic engine on a per-user or per-connection basis, is to periodically automatically regenerate a large series of static pages.

Borrowed and modified from: https://en.wikipedia.org/wiki/Website

4. Read the text again and do the tasks.

4.1. Fill in the missing information in statements 1–7.

1. A website is a collection of web pages and related content identified by a common _____ and published on at least one web server.
2. Hyperlinking between web pages guides the navigation of the site, which often starts with a _____ _____.
3. The most-visited sites are _____, YouTube, and Facebook.
4. The static website is typically simpler in structure and _____.
5. The static website may lack _____ features.
6. A dynamic website is one that changes or customises itself frequently and _____.
7. Dynamic sites can be interactive by using _____ forms.

4.2. Match websites with their characteristics.

Static website	**a**	personalised
	b	slower
	c	simple
	d	fixed content
Dynamic website	**e**	complex
	f	faster
	g	fewer updates
	h	Portfolio website
	i	Social media website
	j	updates regularly

5. **A. & B. Work with AI to give synonyms for the words in italics in the table. Provide your own synonyms in the second column, and use any AI tool to fill in the third column. After that, create two sentences using synonyms from different columns.**

Words	Synonyms generated by students	Synonyms generated by AI
1) *navigation* of the website		
2) to *store* information		
3) *dynamic* website		
4) to *modify* website		
5) *static* website		
6) *scalability* of website		
7) to *generate* information		

Words	Synonyms generated by students	Synonyms generated by AI
8) to *provide* information		
9) *on the fly*		
10) *general-use* programming languages		
11) *the current* state		
12) to be *dedicated* to a topic		
13) to *display* the same information		

6. **A. & B. Make a list of the five most important things that you have to know about static and dynamic websites. Compare your list to your partner's. Which three are the most popular among the class?**

USE OF ENGLISH

VOCABULARY

7. **A. & B. Match the types of websites with their descriptions.**

1	Archive website	**a**	A website developed to create online diaries.
2	Malware website	**b**	A website developed to present background information about a company, organisation or service.
3	Blog	**c**	A website created to publish fake news to deceive users and make profit from ad.
4	Celebrity website	**d**	A website created by state, department of a country.

5	Corporate website	**e**	A website developed to preserve information on webpages from the past.
6	Click-to-donate site	**f**	A website about an individual or a small group.
7	Government website	**g**	A website that contains information about a public figure.
8	Fake news website	**h**	A website where users can donate to a charity.
9	Personal website	**i**	A website created by educational institution with the aim of publishing information about structure, organisations, educational opportunities, current news etc.
10	University website	**j**	A website developed to attack users' computers when they first visit a website by downloading a file.

A. Complete the sentences. Use: services, communication, websites, platforms, goals, functionality, static, updated, audience, dynamic, tools, user.

Websites are virtual **1)** _____ accessible through the internet that provide various types of information, **2)** _____, and resources to users. They can be **3)** _____, showing fixed content, or **4)** _____, with content that is regularly **5)** _____. Websites can serve as a means of **6)** _____, e-commerce, entertainment, education, and much more. The design and **7)** _____ of websites play a crucial role in a **8)** _____ experience, engagement, and overall success. With the continuous growth of the internet, **9)** _____ have become essential **10)** _____ for individuals, businesses, and institutions to reach a wider **11)** _____ and achieve their **12)** _____ .

B. Complete the sentences.

The term “web page” is a virtual representation of a traditional physical book, where separate **1)** _____ are linked **2)** _____ to form a cohesive online entity. Web pages are considered to be the essential units of WWW (the World Wide Web), comprising a set of interlinked **3)** _____ documents that are stored on **4)** _____ servers and accessed through a web **5)** _____. The first web page was created by T. Berners-Lee at CERN in **6)** _____.

Web pages usually contain information presented in text, images, videos, and audio **7)** _____. They are created using **8)** _____, CSS, and JavaScript. Web pages can be **9)** _____, with fixed content that does not change, or **10)** _____, with content that is updated regularly. Also, web pages can be designed for providing information, on-line transactions, or communication with users, and are viewed on various devices like **11)** _____, smartphones, and tablets, using responsive design to adjust to different screen **12)** _____.

Users can interact with web pages by **13)** _____ on links, filling out forms, or watching videos. Most web pages incorporate such elements as forms, buttons, and menus, allowing **14)** _____ to interact with the content and provide **15)** _____. Furthermore, web pages can be **16)** _____ through HTTPS (Hypertext Transfer Protocol Secure) encryption to ensure **17)** _____ of user data and prevent cyber attacks.

IDIOMS

8. **A. Match the idioms in bold to their equivalents. Have you got any similar idioms in your language?**

A warning sign, a goldmine, in the same, taking on more than they could handle, a mixed blessing, share similar ideas, initiating conversation.

1. Students and teachers are all **in the same boat** when it comes to navigating the new online educational platform for distance learning.
2. When I saw a lot of pop-ups and download prompts, I knew this site was **a red flag** for malware.
3. While news websites keep us informed what is happening in the world, they can also be **a double-edged sword**, as they can spread misinformation just as easily.
4. The Community Forum was great for **breaking the ice** among like-minded individuals.
5. The Educational website is **a treasure trove** of resources, with free courses and articles for learners of all ages to use.
6. The niche blog attracts readers who are **on the same wavelength**. They discuss everything from sustainable living to eco-friendly products.
7. The website's homepage was overloaded with so much information that it felt like they were **biting off more than they could chew**, making it difficult for users to find what they needed.

B. Fill in the blanks using the idioms below. Each sentence requires a combination of two idioms. Change the forms of the verbs if necessary.

In the same boat, a double-edged sword, breaking the ice, a treasure trove, on the same wavelength.

1. A university website is _____ of academic papers and resources for students and professors who are _____ regarding their research interests.
2. Creating a personal website is a great way of _____ with potential employers, but it can be _____ if you share too much private information.
3. The mission statement on a corporate website aims to get clients _____, especially when businesses and customers are _____ during a global economic shift.
4. A travel blog often starts by _____ with relatable stories, eventually becoming _____ of tips for people planning their own adventures.
5. When new tax laws are launched, the government website provides guidance for all citizens because they are all _____ and need to be _____ with the new regulations.
6. A fake news website is _____; it might offer _____ of catchy headlines that get clicks, but it ultimately destroys the user's ability to trust the media.
7. An archive website acts as _____ for historians who, despite living in different eras, are _____ when it comes to the struggle of preserving human knowledge.

Borrowed and modified from: https://gemini.google.com/

GRAMMAR

9. **A. & B. Correct the mistakes related to the usage of present tenses in a given text.**

1. Sam is an experienced software developer who is developing websites. **2.** Currently, he works on the creation of a website for an online shop that will sell digital devices. **3.** He spend two months developing this website and is still in the process of creating it. **4.** Since October, he is working on this project, but he has not yet finished developing the website. **5.** Sam collaborates closely with his team throughout the development process. **6.** They are sharing ideas and tackling challenges together, which has significantly improved their efficiency. **7.** Additionally, Sam mentors some junior developers since he started the project, helping them grow their skills and understand the project's requirements better. **8.** The team is communicating for the past two months, ensuring everyone stays motivated.

10. **A. The underlined parts of the sentences may contain mistakes. Some underlined parts are correct. Write out parts that contain a mistake and correct it.**

1. A website **(a)** **consists** of multiple individual web **(b)** **pages**, each with **(c)** **it's** own content and purpose.
2. A static website remains **(a)** **unchanging** and is served as **(b)** **is**, with no **(c)** **on-the-fly** updates.
3. A dynamic website creates and updates content in real-time, often **(a)** **using** databases and coding languages **(b)** **offer** **(c)** **customised** experiences.
4. **(a)** **An** education site is a website that **(b)** **provides** educational information to students, teachers, or the general public, focusing **(c)** **for** courses, tutorials, study guides, and research materials.

5. Non-profit sites **(a) <u>are owned</u>** by non-profit organisations and are aimed **(b) <u>to</u> (c) <u>rise</u>** awareness, fundraise, or provide services related to their specific mission or purpose.
6. Malware websites are websites that **(a) <u>intentional</u> (b) <u>spread</u>** malicious software, such as viruses, Trojans, and spyware, to **(c) <u>unsuspecting</u>** users.
7. Malware websites **(a) <u>use often</u>** deceptive tactics **(b) <u>to attract</u>** visitors to download or install malware, such as fake updates, free software, or **(c) <u>misleading</u>** advertisements.
8. Malware websites **(a) <u>can be</u>** masked as legitimate websites, **(b) <u>made</u>** them difficult **(c) <u>for users</u>** to detect.
9. Malicious websites can also spread malware through **(a) <u>accidental</u>** downloads, where **(b) <u>a user</u>** simply visits a website and malware **(c) <u>are downloaded</u>** without his / her consent.
10. When infected, the malware **(a) <u>can</u>** compromise sensitive information, **(b) <u>steal</u>** login credentials, and even gain control of the **(c) <u>user</u>** device.

B. Correct the grammar mistakes.

1. Archive.org, known as the Internet Archive, is a non-profit digital library co-founding in 1996 by B. Kahle and B. Gilliat.
2. The site is focused on preserved and provided access to the world's digital cultural heritage, including websites, books, music, and films.
3. The primary objective of the Internet Archive is archive and preserve the content of the Internet, providing its accessibility for future generations.
4. By search through the website's huge collections, users can get valuable insights into the past, present, and future of human achievements.
5. The Internet Archive has enable new forms of digital science, allowing scholars to study and analyse the evolution of the internet over time.

6. The Internet Archive website works to libraries and book scanners to digitise physical books, making them free to read and download online.
7. A portfolio website presents the creative profession as an expert in his / her field.
8. A portfolio website increases visibility and expands the range potential clients and collaborators.
9. A blog enables talented people exchange their thoughts, experiences and insights about certain field of knowlege.
10. A simple and intuitive navigation system allows visitors to easily explore the website. A simple and user-friendly navigation system allows visitors to easily navigation the site.

LISTENING

You are going to watch a video that explores different websites.

11. **A. & B. Before watching a video, check if you know the meaning of the words / phrases. Use Merriam-Webster Dictionary if necessary.**

To boost, to store, link, catch their eye, captivating descriptions, to appeal, an awesome way, affiliate, to really expand your reach, a customised domain, display, insights into your personality, a one-stop hub, to showcase, landing pages, non-gated pages, membership websites, nonprofit, a diverse group, in-depth knowledge, consulting, festivities.

12. **A. & B. Watch the video "Popular Types of Websites That You Should Know". Then name popular websites; enumerate the things you have to know before creating a website; name the purposes of different websites mentioned in the video.**

13. Watch the video again and do the following tasks.

13.1. Fill in the missing information in statements 1–12.

1. _____ _____ give your customers a seamless shopping experience and make it really easy for them to explore, select, and purchase.
2. It can help build your brand, spread your messaging and connect with your _____ audience.
3. A _____ helps you to show your interests through written, visual, and digital content.
4. _____ _____ are focused on your skills and they help to attract potential employers or clients.
5. A _____ _____ is a space where you can truly express yourself.
6. _____ pages are open to anyone, whereas _____ pages require users to fill in their details for access, like a name and email address.
7. _____ _____ give you the ability to create a personalised experience and offer exclusive content and valuable resources in a password-protected area.
8. A wildlife protection organisation might be looking to raise awareness, while a food bank might be looking to recruit _____ or _____.
9. _____ are usually made up of different discussion threads, which make it easy for users to find the specific subject they want to focus on.
10. _____ _____ are a great place for people looking for in-depth knowledge on a specific topic, service, or product.
11. Starting a _____ _____, you can create a place that fosters trust, engagement, and a sense of belonging among your members.
12. If you're an expert in a certain field, you should consider creating a _____ _____ to share your knowledge and even monetise it.

13.2. Put the types of websites (1–16) in order they appear in the video presentation.

A	Portfolio websites	
B	Business websites	
C	Personal websites	
D	eCommerce websites	
E	Booking websites	
F	Blog websites	
G	Event websites	
H	Landing pages	
I	Online forums	
J	Community websites	
K	Membership websites	
L	Wedding websites	
M	Nonprofit websites	
N	School websites	
O	Consulting websites	
P	Informational websites	

2. A. & B. Discuss. What factors contribute to the popularity of websites?

SPEAKING

14. **A. With your partner, discuss the features of the website "Cybersecurity Hub". Create an engaging dialogue using the provided information. Your dialogue should include at least 5-6 exchanges per each participant. Be creative! Remember to keep the tone respectful!**

Student A	Student B
1. Hi, have you heard about the latest website that has been gaining popularity in the cybersecurity community since May?	1. ……
2. It's called Cybersecurity Hub. ……	2. ……
3. ……	3. That's really cool. I've been trying to learn more about cybersecurity since my future speciality is related to it. So it would be really helpful. Do they have any tutorials or training materials?
4. Yes, they have ……	4. ……
5. I think it's really important for ……	5. …….

B. Work in pairs. You want to share some information about professional websites with your groupmates. Create a dialogue discussing several professional websites you often visit. Highlight the unique features and specific functions of these sites. Your dialogue should include at least 7–8 exchanges per each participant. Be creative! Remember to keep the tone respectful!

15. **A. Work independently. You often visit the website "WIRED". You would like to share some information about it with your groupmates. Use the link of this website: https://www.wired.com/. Structure your presentation into three clear parts: introduction, main body and conclusions.**

B. Work independently. You often visit some professional websites. Choose some of them and define the specifics of these sites. Then share information with your groupmates. Structure your presentation into three clear parts: introduction, main body and conclusions.

WRITING

16. **1. A. & B. Work with AI. Analyse the AI-generated paragraph about university websites.**

What indicates that the paragraph was written by AI?

"University websites serve as vital resources for students, faculty, and prospective applicants, offering a wide array of information and services. These platforms typically feature details about academic programs, admission procedures, campus events, and financial aid options, making them essential for navigating higher education. Additionally, they provide access to online resources such as course materials, library databases, and academic calendars, fostering a supportive learning environment. A well-designed university website also enhances communication by integrating tools for students to interact with faculty, apply for scholarships, and register for classes. As institutions increasingly embrace digital transformation, university websites play a crucial role in reflecting the university's brand and mission, while ensuring accessibility and engagement within the academic community".

Created by AI Text Generator: https://deepai.org/chat/text-generator

Re-write the paragraph in a style that is more natural to a human being.

2. A. & B. You are asked to write a paragraph (5–6 sentences) about one of the professional websites.

Follow these recommendations.

A paragraph contains a single unit of an idea, and usually involves:

a) a topic sentence that sets the tone for the paragraph;

b) supporting details or evidence that develop the idea;

c) explanation of the information;

d) a conclusion that ties the paragraph together.

17. **A. Write a blog entry on the topic "Types of websites". Create information about different types of websites (not less than five sentences per one website).**

1. **Portfolio websites.**
2. **Business websites.**
3. **Personal websites.**

B. Write a blog entry on the topic "Types of websites". Create information about different types of websites (not less than five sentences per one website).

1. **Business websites.**
2. **Petition websites.**
3. **University website.**
4. **News website.**

REFLECTION AND SYNTHESIS

18. **You have completed this unit. This word cloud can help you to reflect on and synthesise the key concepts from the topic. Focus on the most important terms and ideas that stood out to you. Using the word cloud as a visual tool, you have to illustrate your understanding.**

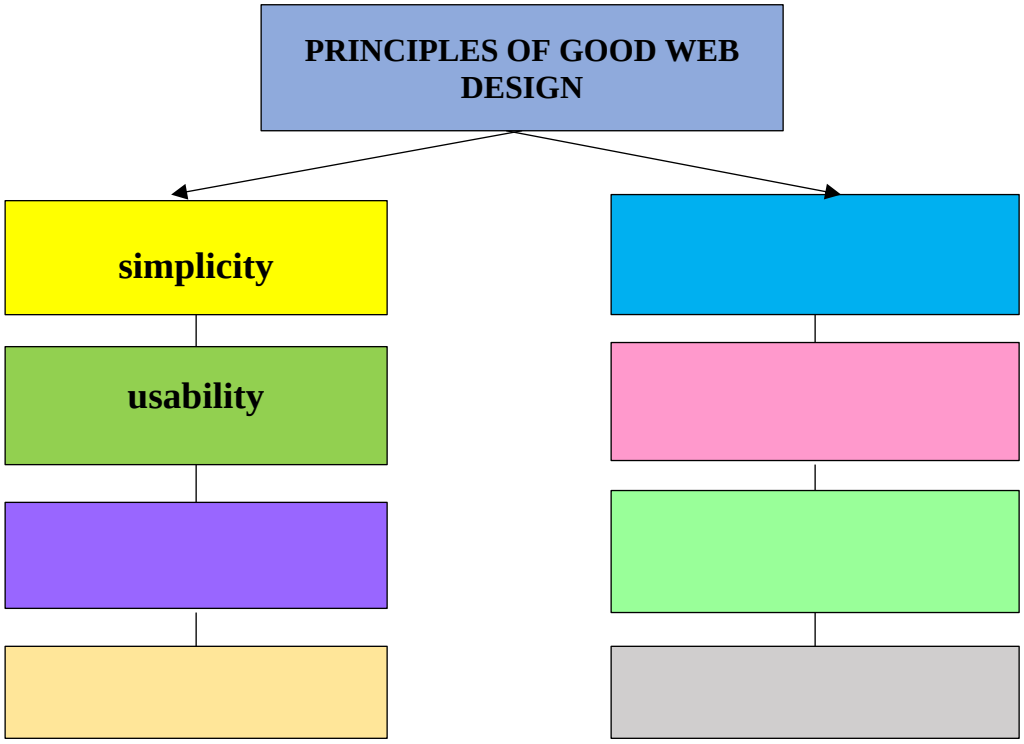
1.3. WEBSITE DESIGN. SECURITY OF WEBSITES

WARM UP

1. **A. & B. Using your background knowledge about website design, do the tasks according to your learning style (dominant or non-dominant modality).**

1.1. ***Visual Modality***

Work individually, then in small groups. Create a mind map that visually represents the principles of good web design. Explain each principle during your group discussion as in the example. Share your points of view.



One of the principles of good web design is simplicity. It involves a simple design that avoids mess and concentrates on the most important content.

1.2. *Auditory Modality*

Create a list of frequently asked questions about website design. Then, in pairs, take turns asking and answering these questions.

1. What does web design stand for?
2. What is the difference between web development and web design?
3. How much can a new website cost? Is it always expensive?
4. How important is web design?
5. Who deals with web design?
6. …….
7. …….
8. …….
9. …….
10. …….

1.3. *Kinesthetic Modality*

Research the importance of a web designer and web developer in website creation process. Choose one of the cards and write about the goals, types and skills of a web designer and a web developer. Then explain the difference between the roles of a web designer and a web developer. Show how their skills and responsibilities complement each other in creating effective websites.

Card 1: Web Designer			**Card 2: Web Developer**		
Goals	**Types**	**Skills**	**Goals**	**Types**	**Skills**
To make sure that the website is user friendly	*Visual Designers*	*HTML and CSS knowledge*	*To maintain the core structure of a website*	*Frontend Web Developers*	*Testing and debugging*

READING

You are going to read an article about web design.

2. **1. A. & B. Before reading, discuss the following quotations.**

1. "Great web design without functionality is like a sports car with no engine."

Paul Cookson

2. "Web design is not just about creating pretty layouts. It's about understanding the marketing challenge behind your business."

Mohamed Saad

3. "Digital design is like painting, except the paint never dries."

Neville Brody

2. A. & B. Before reading, look at the following words and phrases, which have been taken from the text. In what context might they be mentioned? Use Merriam-Webster Dictionary if necessary.

Accessibility, visual design, to incorporate, website development, navigation, search engines, increase readership, start your web design process with researching and sketching, consistency, technique, hierarchy, adaptability, menu, banner or logo, navigation bar, contact information, social network icons.

3. **A. & B. Read the text about web design basics. Six paragraphs have been removed. Choose which of the paragraphs fit into the gaps.**

A	Use a consistent color palette to guide visitors' attention without overwhelming them, and avoid relying on color alone to signal important info by incorporating bold or larger fonts. Ensure sufficient contrast for readability with tools like WebAIM's Color Contrast Checker, and consider using color palette generators like Palletton for cohesive design.

B	Yogi Berra said, "If you don't know where you are going, you'll end up someplace else". Before designing your educational website, **identify its purpose** by considering who your visitors will be (e.g., students, parents, colleagues) and what you want them to do on the site (e.g., access assignments, view student work, learn about your teaching).
C	When designing your website's navigation, prioritize simplicity and clarity to meet your site's purpose. Start with your homepage, but remember visitors may need to navigate elsewhere for what they seek; if they can't find it easily, they'll leave. **Navigation** acts like a table of contents, mainly through menus that should be well-organised and easy to access. Keep in mind the "serial position effect", where visitors focus on the first and last items, so place key links at the top of menus.
D	**Adaptability.** Ensure your website works on all devices – desktop, laptop, tablet, or mobile – without losing its purpose. Use responsive templates from tools like Wix or WordPress, and verify that text is legible, key information is visible without scrolling, and buttons are easy to press. Test your site across major browsers (Chrome, Edge, Firefox, Opera, Safari) on multiple devices, checking all links and functions, then fix any issues.
E	**Planning** is essential to avoid frustration when building a website. Start by researching and sketching: explore similar sites, noting those that are easy to use or memorable, and jot down features you like. You don't need to include everything immediately – just keep notes and add features gradually.
F	**Within-page linking** helps navigate long content by using headings and a clickable table of contents at the top, allowing users to jump to sections instead of scrolling. Be sure to include a "back to top" link at the bottom of each section for easy return to the menu.

WEB DESIGN BASICS

T. Trust, J. Haugsjaahabink

Today's user-friendly web platforms like Wix, Google Sites, Weebly, and WordPress make website creation easy, but not all sites are valuable or educational. To engage viewers, websites must be accessible, well-designed, easy to navigate, and simple to scan, or they risk losing visitors quickly.

1. _____

Creating an educational website differs from other types, often serving to inform students about daily classroom activities or provide online resources. Focusing on a single purpose initially can simplify the design process, even if the site later serves multiple functions.

2. _____

Next, sketch your website's layout and design on paper using a pencil. It's easier to rearrange or adjust your layout with post-it notes or paper drafts early on.

A **website layout** determines the placement of key elements like the **menu, logo, navigation bar, contact information, and social icons**. It involves decisions about item positions, image and text sizes, and visual placement. Popular sites like Google, Amazon, and National Geographic typically place menus, logos, and navigation bars at the top, while contact info and social icons are often at the bottom or upper right corner. Visitors are accustomed to familiar website layouts, such as clicking the header to return to the home page. Following this tradition will make your site easier to navigate. The website should have a consistent layout across all pages, with the menu, header, and search bar in the same place, making navigation easier for users.

When designing your site layout, consider what appears "above the fold", a term from newspaper design referring to the visible part of the page before scrolling. On websites, this is the part of the screen visible without scrolling, which varies by device. To quickly engage visitors, place key content like a short video, compelling headline, or striking visuals above the fold, as users decide within seconds whether to stay.

3. _____

Search engines are a popular navigation tool, and many web design tools like WordPress allow embedding one on every page for consistency. Ensure your pages contain a relevant text and images with the alternative text, including key search terms. For example, if students search for "homework" but your page is titled "after-school work", the search engine won't be helpful.

4. _____

Accordions are a useful navigation method that let users view multiple headings at once and open sections as needed. Tip: When linking to external sites, open them in a new window or tab so users can easily return to your site.

Visual design is important, but it shouldn't distract or confuse visitors. Instead, it should guide users to key content through visual hierarchy. Platforms like Google Sites, Wix, Weebly, and WordPress offer templates that help manage these design choices.

Guidelines for typical visual design elements:

1. Text. Use easy-to-read text, ideally at least 16-point font, with larger sizes for titles and headings. Stick to no more than three fonts for consistency, and avoid overly decorative fonts to ensure readability and accessibility.

2. Color & Contrast. **5. _____**

3. White Space. It helps reduce clutter, clarify visual flow, and make it easier for users to find what they need.

4. Icons. Use standard icons and shapes, like a question mark for "help" and a house for "home".

Accessibility. Educational websites should be accessible to all, including users with disabilities. A study of over 6,000 school websites found most are not fully accessible. Use the Accessibility Statement Generator to improve your site's accessibility and show your commitment to inclusivity.

6. _____

4. Read the text again and do the tasks.

4.1. Fill in the missing information in statements 1–10.

1. Building a website without some degree of _____ can lead to frustration.
2. The _____ involves decisions about the position of each item on the page, the size of images and text, and placement of visuals.
3. "_____ _____" is a term from newspaper design that refers to the part of the page that is visible before scrolling.
4. Most web design tools, like Wordpress, allow you to embed a _____ within your site.
5. Most browsers default to a _____ size to ensure readability and accessibility.
6. It is good practice to limit yourself to no more than _____ and maintain _____ in font style from page to page.
7. It may be tempting to use lots of colour on your website, however too many colours can be _____ .
8. Use white space on your page to reduce _____, make the visual path clear to your user and allow them to find what they are looking for efficiently.
9. Some of your users may have disabilities and your website needs to allow them to _____ the information you have presented.
10. Make sure to _____ your website across multiple devices and browsers.

4.2. Decide whether these sentences are *true* or *false*.

1. Identifying your target audience is one of the first steps in designing your website.
2. It is beneficial to research similar websites while planning your own.
3. Contact information is usually found at the top of websites.
4. Consistency in layout across pages enhances user navigation.
5. The term "above the fold" refers to the lower half of a webpage.
6. The navigation of a website should be designed based on its purpose to facilitate user goals.
7. The "serial position effect" suggests that visitors typically remember the middle items in a list best.
8. Accordions allow users to view only one section of content at a time.
9. Using many colours on a website is an effective way to make it visually appealing and easy to navigate.
10. White space is important for reducing visual clutter and enhancing user navigation.

5. **A. & B. In pairs, select one word from the provided list. Student A asks the questions below, putting the chosen word into each question, while Student B responds using that word. You may skip any questions that do not apply. After completing the questions, switch roles and repeat the activity with a different word. See the example below.**

Accessibility, adaptability, layout, content, design, network, icon, valuable, enrich, engine, hierarchy, development, click, accordion, space, visual, clutter, browser, consistency.

1. What does _____ mean?
2. What is the plural / singular of _____?

3. What is the synonym of _____?
4. What is the opposite of _____?
5. What is the noun for _____?
6. What is the verb for _____?
7. What is the adjective for _____?
8. What is the adverb for _____?
9. What collocations do you know with _____?
10. How to use _____ in a sentence?
11. What is the Ukrainian translation for _____?

For example:

The chosen word is "project".

Student A: "What does project mean?"

Student B: "Project" is a planned set of activities or tasks intended to achieve a specific goal.

Student A: "What is the plural of project?"

Student B: "Projects."

6. **A. & B. Discuss the questions.**

1. What are the main requirements for the websites? What things do you need to consider to identify the purpose of a website?
2. What should you do at the beginning of the web design process? How can researching other websites help you in the web design process? What is an advantage of sketching out your website's layout on paper?
3. What is included in a website's layout? What are some key considerations involved in the layout process? Where are typical items usually located on a website? Why is consistency in layout important for a website?

4. Why is it important to capture attention and present information above the fold on a website? What are some examples of how to capture attention and present interesting information above the fold?
5. Why is it important to make navigation easy for users? What is the main technique used in all navigation schemes? Can search engines be used as a navigation tool? If so, how should they be implemented?
6. What is the "serial position effect"? How can it be used in navigation design? What is within-page linking? How can it be used to improve navigation? What is the benefit of having a "back to top" link at the bottom of each section?
7. What is an accordion? How can it be used for navigation?
8. Why is it important to keep visual design simple? What is the purpose of visual hierarchy in website design? What are some guidelines for typical visual design elements?
9. Why is it important for educational websites to be accessible? What are some tips for making a website adaptable across different devices and browsers?

USE OF ENGLISH

VOCABULARY

7. **A. Group the following words into pairs of synonyms.**

Accessible, significant, simplify, flexibility, incorporate, moving, valuable, ***available***, hierarchy, audience, adaptability, clarify, navigation, establish, scrolling, integrate, set up, guidance, readership, grading.

B. Categorise the provided synonyms into two groups: "strong matches", which contain synonyms that have nearly identical meanings, and "weak matches", which include synonyms that share a similar meaning but may differ in context, or usage.

Use: *to determine, to look up and down, to press, to create, to draw, to lessen, to make up, to include, to recognise, to minimise, arrange, to investigate, to develop, structure, to select, to divide … into, various, to split, several, to integrate.*

Phrases	Strong matches	Weak matches
1) to *design* your educational website		
2) to *identify* the purpose		
3) to *reduce* potential frustration		
4) to *explore* various websites		
5) to *sketch out* your website organisation and visual design		
6) the *layout* of a website		
7) to *click* the header		
8) to *break up* the content by headings		
9) test your website across *multiple* devices		
10) the free website building programs *incorporate* a design		

PHRASAL VERBS

8. **A. Fill in the correct particles. Then explain the phrasal verbs. See Appendix 2, which contains a list of relevant phrasal verbs.**

1. During the meeting, I am planning **to bring** _____ the idea of including a dark mode feature to make it more accessibility.
2. We need **to bring** _____ our design and development teams to create a cohesive user experience.
3. To make the landing page more interactive, let's **bring** _____ some new animation techniques.
4. It's important **to break** _____ the user journey to see where visitors might be dropping off on our site.
5. Our team wants **to break** _____ traditional design barriers by using more engaging experiences.
6. We can't be scared to **break** _____ from standard templates if we want to create something really unique.
7. We should **build** _____ our content strategy before launching the new website to ensure it attracts the appropriate audience.
8. We want to **build** _____ the feedback we received from our beta testers and continue to refine the website further.
9. As your audience grows, you should **build** _____ additional resources and support pages on the website.

B. Replace the words or phrases in bold with the correct form of a phrasal verb using *bring*, *break*, and *build*. Then, create three interconnected sentences that include any phrasal verbs with "bring", "break", and "build".

1. As we redesign the homepage, I would like to **raise** the issue of user feedback from our last survey.

2. Let's **simplify** the wireframe so that we can clearly see the purpose of each feature.
3. We could really **add** some new ideas by consulting with a design agency.
4. If you want to stand out, you need to **get away** from using stock images and create unique visuals.
5. We need to **enhance** our online presence by optimising the website for search engines.
6. To create a consistent design, we should **combine** input from both the marketing and design teams.
7. We can **extent** the success of our previous campaign by ensuring our website reflects the same branding.
8. This new software could help us **achieve** the goals we have.
9. Once the new site is up, we should plan to **create** an FAQ section to help users.

GRAMMAR

9. **A. & B. Put the words into the correct present tense.**

Jill **1)** _____ **(to be)** a talented web designer who **2)** _____ **(to create)** amasing websites for different clients. Every day, she **3)** _____ **(to brainstorm)** new ideas and **4)** _____ **(to design)** layouts that **5)** _____ **(to capture)** the essence of her clients' brands. Jill often **6)** _____ **(to collaborate)** with graphic designers and developers to make sure that the websites work perfectly.

Since September, she **6)** _____ **(to work)** on a project for a local bakery, designing a colourful and user-friendly website to promote the delicious cakes and pastries. During this time, Jill **7)** _____ **(to develop)** several initial prototypes and presented them to the bakery owners for feedback. At this moment she **8)** _____ **(to collaborate)** with graphic designers and developers to ensure that the websites work perfectly. Jill **9)** _____

(to receive) also positive feedback from the owners, who **10) _____ (to be)** excited about the direction of the project. Furthermore, she **11) _____ (to implement)** several innovative features that enhance the overall user experience.

A. Choose the correct option.

KNOW YOUR AUDIENCE

According **1) _____ (to / of)** the University of Maryland Baltimore Website Manual, "Most users visit a web page **2) _____ (in / for)** 10–15 seconds. In that brief time, 80 percent will skim the page **3) _____ (of / for)** keywords they already have in mind. Therefore, before you create content, it's important **4) _____ (to understand / understand)** your audience and anticipate what content and keywords they're trying to find."

Are you creating a website for your students? Parents? Colleagues? Administrators? Which words or phrases **5) _____ (appealing / appeal)** to each of these groups? What type of tone and language do you use when communicating with each of these groups? You will want to keep this **6) _____ (to mind / in mind)** when **7) _____ (selecting / selection)** the word choice and writing style for your website.

Use language that appeals to your audience. For example, if you **8) _____ (are designing / are designed)** a website for your students, consider what language you use to capture their attention or give directions, and use this same style of language when creating your website content. Also, use a readability checker **9) _____ (ensuring / to ensure)** your content **10) _____ (writes / is written)** at a level that is accessible by your audience. By **11) _____ (paying / played)** close attention to your language usage when designing your website and ensuring it will captivate your audience, you will keep them **12) _____ (engaged / engage)** in your content for longer.

Borrowed and modified from: "Web Design Basics for Educators" by Torrey Trust, 2019, https://edtechbooks.org/webdesign/writingfortheweb.

B. Choose the correct option.

WRITING FOR A SUBJECT-SPECIFIC WEBSITE

If you are designing a website to present your students with information and resources **1) _____ (relating / related)** to one or more subject areas, here **2) _____ (is / are)** a few additional tips to engage your learners with the text on your site.

Keep it Simple and Organised: Limit **3) _____ (the number / the amount)** of information on your website so that your students don't feel overwhelmed when they visit. Chunk information and resources for sub-topics into separate sub-pages rather **4) _____ (trying / tried)** to feature everything the student needs to learn about a topic **on** a single page.

Keep Your Content Up to Date: **5) _____ (Do you ever scrolled / Have you ever scrolled)** to the bottom of a website to see its copyright date (e.g., Copyright 2013) and then question the credibility of the information on the site since it **6) _____ (hasn't updated / hasn't been updated)** in many years? Your students will do the same thing! **7) _____ (Making sure / Make sure)** you spend time at least once every few months **8) _____ (modifying / modified)** your site by revising information, adding or removing resources, and featuring related news. By presenting new content for your subject area, you can **9) _____ (hook students in / hook students on)** and have them **10) _____ (stay in / stay on)** your site longer. For example, if you're designing a social studies website, instead of presenting the same facts about American historical figures, you can add content that usually **11) _____ (get skipped / gets skipped)** over or left out of history textbooks such as LGBTQ history and notable African-American history. By **12) _____**

(incorporating / incorporated) interesting new content that appeals to your students, you will be increasing student motivation and engagement.

***Create Content that is "Made To Stick"*:** Heath and Heath (2007) developed a set of guiding principles, called the Made to Stick principles, that **13) _____ (can use / can be used)** to create content that is **14) _____ ("sticky" / "stick")** (i.e., hard to forget). The acronym SUCCESS can help you remember the principles:

***Simple*:** As **15) _____ (mentioning / mentioned)** previously, don't overwhelm the reader. **16) _____ (Focus on / Focus in)** one key point per paragraph. Omit extra words. Write in a concise and clear manner.

***Unexpected*:** Present information that surprises the reader.

***Concrete*:** Make it easy **17) _____ (for / to)** the reader to see how the content is relevant **18) _____ (in / to)** their life.

***Credible*:** Ensure the information you present is current, accurate, and reliable.

***Emotion*:** Present content in a way that makes the readers **19) _____ (to feel / feel)** something (e.g., joy, frustration, anger, excitement).

***Story*:** Tell a story. Storytelling is one of **20) _____ (the powerfulest / the most powerful)** techniques for communicating information since people who are reading or listening to a story mentally put themselves in the story, thus making it more memorable.

10. A. Choose the correct option.

1. The most important thing to remember is that _____ for the web is different _____ academic or print writing.

   a) write, on b) writing, from c) written, from

2. You should use “half the word count (or less) than conventional writing” _____ a webpage.

    a) of b) in c) on

3. With _____ words to communicate the information you want _____ on your website, you need to ensure that every word that you use, the tone that you take, and the style of writing you employ, increase the readability of your page.

    a) fewer, to present b) less, present c) fewer, presenting

4. Ultimately, the language you choose to use can _____ whether a reader explores the content on your site or makes an immediate exit.

    a) influencing b) to influence c) influence

5. Subheadings give the reader _____ roadmap of your website and are critical _____ accessibility and screen readers.

    a) a, for b) the, to c) a, to

6. _____ subheadings helps chunk, or compartmentalise, ideas and concepts, while also _____ the hierarchy of information.

    a) Used, reinforcing b) Using, reinforcing c) Using, reinforce

7. For example, if you _____ a website heading for “atoms”, and subheadings for “protons”, “neutrons”, and “electrons”, the subheadings reinforce that they are the parts of _____ atom.

    a) will have, the b) have, an c) will have, a

8. It’s important _____ the size of font when making headings.

    a) considering b) consider c) to consider

9. It is worth _____ that certain web design platforms (such as Wix, Weebly and Google Sites) _____ set the page title to Heading 1, but you will want to check the settings to confirm this.

    a) noting, automatically
    b) to note, automatical
    c) noted, automatically

10. Using the "_____ pyramid" concept is another technique to captivate _____ attention of website visitors.

a) inverting, a b) inverted, the c) inverted, the

11. The idea behind the _____ pyramid is to have the most important information "on top" (within your first paragraph), with the details _____ in the subsequent paragraphs.

a) inverted, coming b) inverting, coming c) invert, coming

12. Readers often _____ pages for information, so by putting the big takeaways _____ on, you will increase the chances the readers learn the information they need.

a) scan, early b) scans, early c) scans, earlier

Borrowed and modified from: https://edtechbooks.org/webdesign/writingfortheweb

B. Complete the sentences using the words in bold. Use two to five words.

1. It was the first time they had created a website.

   never They _____ a website before.

2. I started creating websites five years ago.

   been I _____ a website for five years.

3. They haven't finished creating a website yet.

   still They _____ a website.

4. We had never visited Google company before.

   first It _____ we had ever visited before.

5. When did T. Berners-Lee propose to create a global hypertext project, which later became known as the World Wide Web?

   ago How long _____ to create a global hypertext project, which later became known as the World Wide Web?

6. A text on a webpage needs breaking up into smaller paragraphs.

   broken A text on a webpage needs _____ up into smaller paragraphs.

7. This website is so expensive for me that I can't afford it.

   too This website is _____ to afford.

8. The teacher made us read the text about the specifics of websites.

   made We _____ the text about the specifics of websites.

9. Using different words for the same subject is not allowed when designing the website.

   use Nobody _____ different words for the same subject when designing the website.

10. Tom didn't begin designing a website until he had gathered all the necessary information about the target audience.

    before Tom had gathered all the necessary information about the target audience _____ designing a website.

LISTENING

You are going to watch a video that explores the specifics of website security check.

11. A. & B. Before watching a video, check if you know the meaning of the words and phrases. Use Merriam-Webster Dictionary if necessary.

Malware, vulnerabilities, spam, digging, pinpointing, plugins, sensitive changes, brute forcing programs, arduous, a long tangled string of random characters, inappropriate permissions, restricting user permissions, the expired certificate, innocuous, breaking into a site.

12. **Watch the video "How to Perform a Website Security Check".**

Do the following tasks.

12.1. Decide whether these sentences are *true* or *false*.

1. Online scanners are the most effective way to detect malware and vulnerabilities on a website.
2. According to the text, Sucuri SiteCheck does not suggest the ways to help you resist attacks.
3. All WordPress plugins can remove malware automatically.
4. According to the text, one of the unexplained challenges that you may notice on your website is sudden disappearance of important data or files.
5. It is recommended that you take two crucial steps before making changes to the website that could potentially cause harm or damage: backing up the website and understanding the code.
6. According to the text, using a weak password on your main account can put the website and its security at risk, making it vulnerable to brute forcing programs that can easily guess the password and gain administrator access.
7. A visible WordPress version in your frontend tells hackers exactly what vulnerabilities your site has, especially if you are using an obsolete version of WordPress.
8. Keeping PHP up to date is important for security.
9. SSL certificates are only important for e-commerce sites.
10. SQL injections are a common way of breaking into a site.

12.2. Put the key recommendations in the order they appear in the text.

Letter	Recommendation	Number
A	Look for strange changes on your site, such as new links, articles, or pages that you did not create.	
B	Check your SSL certificate regularly to ensure it is up-to-date and secure.	
C	Use strong and unique passwords for all accounts, and consider using a password manager.	
D	Scan your website with a WordPress plugin like All in One WP Security and Firewall or Wordfence Security.	
E	Back up your site and understand its code before making any changes.	
F	Make sure everything is up to date, including WordPress, plugins, and themes.	
G	Remove any unnecessary plugins and themes to reduce the attack surface.	
H	Review user accounts and remove any unknown or unauthorised users.	
I	Use an online tool like Sucuri SiteCheck to scan your site for malware and vulnerabilities.	
J	Regularly scan your site's files and directories for malware and viruses.	

13. **Answer the questions.**

1. Do you follow the recommendations presented in the video?
2. What tools do you use to check a website security?

SPEAKING

14. **A. Work in pairs. As the head of the IT company, you have a discussion with a cyber security expert about recent website security incidents. Act out a dialogue about website security covering the following information:**

1) **a few incidents recently that the customers have reported;**
2) **the outdated encryption;**
3) **the last update about two years ago;**
4) **expecting damage, serious consequences;**
5) **the plan to fix the problem;**
6) **timeline for fixing the problem.**

Your dialogue should include at least 5–6 exchanges per each participant. Be creative! Remember to keep the tone respectful!

Complete the table and role play the dialogue below.

A: a head of the company	B: a specialist in cyber security
1. Tom, I'm becoming increasingly concerned about the security of our website. We've had a couple of incidents recently where our customers have reported that their logins have been compromised. What's the problem?	I'm afraid it's a common problem. Our website uses outdated encryption. ….
2. ……	Last updated was about two years ago. …….
3. What kind of damage can we …?	……..
4. …….	If we're lucky, …. It'll just be a nuisance. But if we're unlucky, ….

A: a head of the company	B: a specialist in cyber security
5. What's your plan to fix this?	I recommend we implement …
6. …….	…….

B. In preparation for a class on "Website security", your teacher has given you the task to make up a list of frequently asked questions about the security of websites. Then, in pairs, discuss these questions, sharing your opinions.

15. **A. Work in groups. You are asked to prepare the information about 10 essential principles of user-centered design for website success. Each member should choose two principles and inform about the significance and specifics of these principles.**

Principle 1: Empathy and understanding.

Principle 2: Define the aim.

Principle 3: Know the audience.

Principle 4: Keep it simple and intuitive.

Principle 5: Make it easy to navigate.

Principle 6: Prioritise feedback.

Principle 7: Use consistency.

Principle 8: Design for error prevention.

Principle 9: Make it responsive.

Principle 10: Iterate and refine.

B. In preparation for an ESP lesson, you are asked to choose one of the topics for a presentation below. Prepare a three-minute presentation. Follow a structure: introduction, main body, and conclusions.

1. The evolution of web design: trends, best practices, and future.
2. The art of typography on the web: best practices for choosing fonts, colours, and text layout.

3. The role of storytelling and emotional design in web design.
4. How to make your website inclusive and usable for all people.
5. The power of minimalism in web design.
6. The role of colour in web design.

WRITING

16. A. & B. Reduce the information in the sentences independently and using the AI tools. Then compare the results.

To reduce information in the sentence, you need:

1) to eliminate unnecessary words;

2) to combine ideas concisely;

3) to use simpler phrases;

4) to avoid redundancy;

5) to replace long phrases with shorter alternatives.

Statement	Information reduction by a student	Information reduction by AI
1. While a complicated password can be arduous to remember making logging in less convenient, it is even more inconvenient to have to your site from a hack.		A complicated password is hard to remember, but it is even harder to recover from a hack. (Created by *https://deepai.org/chat/text-generator*)
2. You should back up your site and have an understanding of the code before making any sensitive changes.		
3. If your site is infected periodically with malware and you can't find any cause in the files, the issue may be with your server or another site on your server.		

Statement	Information reduction by a student	Information reduction by AI
4. In the best case scenario, your password would be a long tangled string of random characters.		
5. We strongly recommend you use a password manager.		
6. While you are on the user's page, take a look at all your users and make sure there is no one there who you do not recognise or has inappropriate permissions.		
7. You can also use an SSL certificate checker to scan your site to make sure your certificate is not expired, and there are no vulnerabilities present in your SSL protocol.		

17. **For your research, you need to write a summary of the audio text. Watch the video presentation "How to Perform a Website Security Check".**

A. Write a 150–160 word summary.

B. Write a 170–180 word summary.

Use a five-key-step list.

1. **Read the text.**
2. **Split it into parts.**
3. **Define the key points in each part.**
4. **Create a summary.**

REFLECTION AND SYNTHESIS

18. **You have completed this unit. This word cloud can help you to reflect on and synthesise the key concepts from the topic. Focus on the most important terms and ideas that stood out to you. Using the word cloud as a visual tool, you have to illustrate your understanding.**

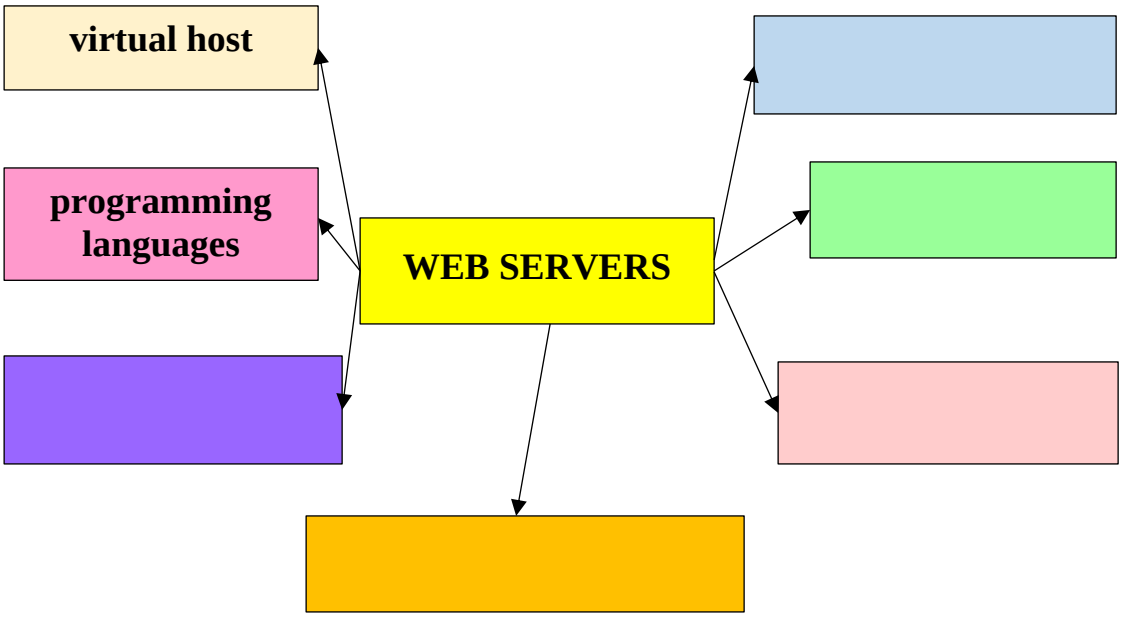
1.4. WEB SERVERS. SECURITY OF WEB SERVERS

WARM UP

1. A. & B. Using your background knowledge about web servers, do the tasks according to your learning style (dominant or non-dominant modality).

1.1. *Visual Modality*

Work individually and then in small groups. Create a mind map focusing on the concept of *web servers*, including key terms and ideas related to the topic. Briefly explain how they relate to the central concept.



1.2. *Auditory Modality*

Work in small groups. Answer the questions.

1. What is a web server?
2. What are the main types of web servers?
3. What are the main features of web servers?
4. What is the difference between web servers and application servers?
5. What is the difference between a web browser and a web server?

1.3. *Kinesthetic Modality*

Work in small groups. Conduct a survey to assess background knowledge of web servers. Extend the provided questionnaire by adding questions 4–5. Once the survey is completed, report the results.

1. What is the primary purpose of a web server?
   - A To store and manage databases
   - B To serve static files to clients
   - C To execute server-side scripts and programs
   - D To handle email communications
2. Which of the following protocols is used to secure communication between a client and a web server?
   - A HTTP
   - B HTTPS
   - C FTPS
   - D SFTP
3. What is the term for the process of temporarily storing frequently accessed files or data in memory to improve performance?
   - A Caching
   - B Clustering
   - C Load balancing
   - D Content Delivery Network (CDN)
4. …….
5. …….

READING

You are going to read an article about web servers.

2. **1. A. & B. Before reading, discuss the following quotations.**

"The right server for the right job."

Bob Muglia

2. A. & B. Before reading, look at the following words and phrases, which have been taken from the text. In what context might they be mentioned? Use Merriam-Webster Dictionary if necessary.

Scripting language, hardware, software, to extend, hosting provider, to invoke, accurate, portrayal, conjured, backup, retention, LAMP, WAMP, databases.

3. **Read the text about web servers and fill in the gaps (A–F).**

	Sentences
1	A number of companies, including Google, Yahoo, and Facebook, are looking to reinvent this concept.
2	The balance adds the capability for interactivity and for the information to change based on the result of user interactions.
3	We will utilise Linux, the predominant choice.
4	Hardware, an operating system, and an HTTP server comprise the bare necessities.
5	In a web server, Apache serves as the HTTP component, which compiles the results from scripting languages, databases, and HTML files to generate content that is sent to the user.
6	Among the plethora of combinations, the use of LAMP prevails as the catch-all reference to a server with these types of services.

WEB SERVERS

While we could simply focus on how to create web pages and websites, none of this is possible without the underlying hardware and software components that support the pages we create. Examining what these components are and how they interact helps us understand what our server is capable of. The diagram represents the basic elements of a web server. **A _____**. The addition of a database and scripting language extend a server's capabilities and are utilised in most servers as well.

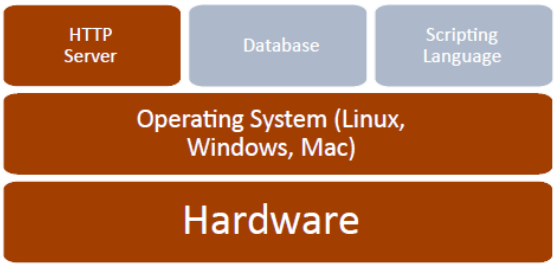


Figure 1. *Web Server Software Structure*

Hardware

The mention of phrases like the *data center*, *hosting provider*, or even big name companies like *Microsoft* and *Google* can invoke mental images of large, sterile rooms full of tall racks of hardware with blinking lights and a maze of wires. Those more familiar with such rooms will also know the chill resulting from the heavily air-conditioned atmosphere and droning whir of fans that typically accompany them. This, however, is not a requirement nor an accurate portrayal of a great deal of servers connected to the Internet. With the addition of the right software, the device you are using to read this with could become an internet connected server. While it would not sustain the demands made of domains like Amazon.com or MSN.com, you would be able to perform the basic actions of a server with most of today's devices.

Even though we have reached this point, it is difficult to forget the mental picture conjured by the thoughts of the data center. In the current "traditional" model, thin, physically compact servers are stacked vertically. These are referred to as rack mount hardware. Many rack mount systems today contain hardware similar to what we have on our desktops, despite the difference in appearance.

B _____. Google, for instance, has already used custom-built servers in parts of its network in an effort to improve efficiency and reduce costs. One implementation they have tried proved so efficient that they were able to eliminate large power backup units by placing a 9-volt battery in each server – giving it enough emergency power to keep running until the building's backup power source could kick in. They have also experimented with alternative cooling methods like using water from retention ponds or placing datacenters where they can take advantage of natural resources like sea water for cooling or wind and solar for energy.

Even small, low powered devices are finding demand as servers in part to enable the Internet of Things. These small, "just-enough-power" devices are used to connect data from the environment or other devices to the Internet, leaving the data center behind and living instead at the source of the data itself.

Software

A typical web server today contains four elements in addition to the physical hardware. These are the operating system, web server, a database and a scripting language. One of the most popular combinations of these systems has been abbreviated to the LAMP, standing for Linux, Apache, MySQL, and PHP, named in the same order. There are many combinations of solutions that meet these features, resulting in a number of variations of the acronym, such as WAMP for Windows, Apache, MySQL, PHP or MAMP, identical with exception of Mac (or, rightfully, a Macintosh developed operating system). **C _____**.

All that is ultimately required to convey static pages to an end user are the operating system and HTTP server, the first half of the WAMP acronym. **D _____**.

Operating System – Linux

Your operating system is what allows you to interact with the applications and hardware that make up your computer. It facilitates resource allocation to your applications and communication between hardware and software. Typically, operating systems for servers fall under three categories: Linux-based, Windows-based, and Mac-based. Within each of these categories are more options, such as a various version of Mac and Windows operating systems, and the wide variety of Linux operating systems. **E _____**.

Developed by Linus Torvalds in the early 1990s while he was a student, Linux was created so that Linus could have access to UNIX systems at his university without the need for an operating system. As his project became more robust, he decided to share it with others, seeking input but believing it would remain a more personal endeavor. What he could not have predicted was the community that would come together and participate in helping shape it into what is today. As the basis of a large number of Linux-based operating systems (or "flavors" of Linux), the Linux core can be found around the world, even in the server rooms of its competitors like Microsoft.

HTTP Server – Apache

Apache is an open source web server originally developed for UNIX systems. Now supported on most platforms including UNIX, Linux, Windows, and Mac, Apache is one of the most utilised server applications. First developed in 1995, Apache follows a similar open source approach as Linux, allowing users to expand on the software and contribute to the community of users. The user group around Apache developed The Apache Foundation, which maintains a library of solutions for web services.

F _____. Apache (or any web service) will track which files on the server do and do not belong to the website, and also controls what options are available to the end user through its configuration files.

Apache and other HTTP servers allow us to share our web pages, scripts, and files with our end users. Any output from our database and scripting languages is turned into HTML output that the client's browser displays as our webpage. While we can view HTML and JavaScript files on a computer that is not a web server, we need an HTTP server to view them as a destination on a network.

Borrowed and modified from:
https://eng.libretexts.org/Bookshelves/Computer_Science/Web_Design_and_Development/Book%3A_Web_Development_and_Programming_(Mendez)/01%3A_Web_Development/1.03%3A_Web_Servers

Modified by https://deepai.org/chat/text-generator

4. Read the text again and do the following tasks.

4.1. Fill in the missing information in statements 1–8.

1. The bare necessities are made up of three things: _____, an operating system and an HTTP server.
2. In the "traditional" model, thin, physically compact servers are _____ on top of each other.
3. A typical web server contains an _____, web server, database and _____.
4. LAMP is an acronym that stands for Linux, Apache, _____ and _____, in that order.
5. Operating systems for servers typically _____ three categories: Linux-based, _____ and Mac-based.
6. In the early 1990s, Linus could access _____ at the university without relying on an _____.
7. Apache is an open _____ web server that was originally developed for _____ systems.
8. While we can view HTML and JavaScript files on a computer that is not a _____, we need an HTTP server to view them as a _____ on a network.

4.2. Decide which statements are *true* and which are *false*.

1. A web server relies on hardware, an operating system, and an HTTP server as its core components, with databases and scripting languages enhancing its functionality.
2. Many companies like Google, Yahoo, and Facebook are innovating with server design to improve efficiency, such as Google using custom-built servers and alternative cooling methods.
3. All data centers require a heavily air-conditioned environment with a maze of wires and blinking lights.

4. The LAMP stack includes Windows, Apache, MySQL, and Python, which is the most common configuration for web servers.
5. Linux was created by Linus Torvalds in the early 1990s while he was a student.
6. Linux is the basis for many different Linux-based operating systems and can be found in various server environments worldwide.
7. Apache was initially developed in 1995 as a proprietary software before becoming open source.
8. Apache is supported on most platforms including UNIX, Linux, Windows, and Mac.

5. **A. & B. Work with AI tools. Fill in the gaps with synonyms and antonyms for the words in italics in the table, idependently and using AI tools. Give two examples of sentences using the generated phrases.**

Synonyms

Phrases with words in italics	Synonyms suggested by students	Synonyms generated by AI
to *focus* on		
to *create* web pages and websites		
examining what these components are		
to *comprise* the bare necessities		
it would not sustain the *demands*		
custom-*built* servers		
to *eliminate* large power backup units		
to *stand for* Linux, Apache, MySQL, and PHP		

Phrases with words in italics	Synonyms suggested by students	Synonyms generated by AI
to *fall under* three categories		
to become more *robust*		
the client's browser *displays* as our webpage		

Antonyms

Phrases with words in italics	Antonyms suggested by students	Antonyms generated by AI
to improve *efficiency*		
to *reduce* costs		
to take *advantage* of natural resources		
the *wide* variety of		
any *output*		
those more *familiar*		

6. Read the text again and answer the questions.

1. What are the three main components of a web server, and how do they interact with each other?
2. How does Google's approach to server design differ from traditional methods, and what benefits has it achieved?
3. What is the LAMP acronym? What does it mean in the context of web servers?
4. What is Linux? Who developed Linux? How did it come to be the predominant choice for server operating systems?
5. What is Apache? What role does it play in a web server, besides serving as an HTTP component?

USE OF ENGLISH

VOCABULARY

7. **A. Fill in the gaps using the words below.**

Settings, credentials, system, http.conf, server, operating system, delimiter, configuration files, plain text format file, scripts, files, pound sign.

When we create a new **1)** _____, settings may not be exactly as we want them, or the time may come where we want to add, remove, or change something about our **2)** _____. To do this, we will need to edit the **3)** _____ that control the different pieces of our system. Our actual web server config file is called **4)** _____. For PHP **5)** _____, we need to refer to php.ini, and for MySQL, we refer to my.cnf. These files may be located in different places depending on the **6)** _____, and the version in use, so it is best to use your system's file search tools to find where they are on your machine. Configuration (or setting) files are typically a **7)** _____ with one set on each line with comments near each value describing the setting's use. These files will also use the same commenting **8)** _____ for their notes to enable or disable individual settings. Typically, the delimiter used is a semicolon, or **9)** _____ #.

If you want to change settings on your server itself such as the port it listens on, what folder it looks for **10)** _____ in, its name, or other related features, look to the httpd.conf file. From the php.in file, you can control elements like which modules are installed and enabled for your system, how much data **11)** _____ are allowed to consume, and more. Similarly, your MySQL config file determines what port it listens on, which user it runs as on your server, what your admin account's **12)** _____ are, and more.

Borrowed and modified from:
https://eng.libretexts.org/Bookshelves/Computer_Science/Web_Design_and_Development/Book%3A_Web_Development_and_Programming_(Mendez)/01%3A_Web_Development/1.03%3A_Web_Servers

B. Fill in the gaps.

Changes to these files typically require you to restart your **1)** _____ (in our case, for Apache or PHP changes), or at least the service that you are changing (in our case, MySQL changes). This can be done using the control panel if you are using a combination program like Wamp 2, or by using your operating system's **2)** _____ tools or by using system **3)** _____ at a command prompt. Restarting Wamp 2 in a GUI operating system like Windows can be done by right-clicking on Wamp's **4)** _____ in the tray. In a CentOS server, the same effect can be achieved by typing "service httpd **5)** _____". If all else fails, you can always physically restart the machine (referred to as "bouncing"), but this is something you will want to avoid on a live **6)** _____ as it will cause a much longer period of downtime.

If you use installer **7)** _____ or a combo installer like Wamp 2, you will probably get by initially without making any changes to these files. Binary installers, however, will not know where or how to make changes to **8)** _____ files and you will need to follow the instructions to **9)** _____ these files by hand to integrate all of your elements.

Borrowed and modified from:
https://eng.libretexts.org/Bookshelves/Computer_Science/Web_Design_and_Development/Book%3A_Web_Development_and_Programming_(Mendez)/01%3A_Web_Development/1.03%3A_Web_Servers

IDIOMS

8. **A. Match the idioms in bold to their equivalents. Have you got any similar idioms in your native language?**

To hope for the best, an indication of a more significant underlying problem, to face the difficult situation, to work late, to start our tasks immediately, it's your responsibility, to handle that issue when we encounter it.

1. We need **to bite the bullet** and upgrade our web server hardware. The current setup simply can't handle the amount of traffic.

2. Once we've received approval, we'll **hit the ground running** with the new web server deployment to meet our launch deadline.
3. Our team had **to burn the midnight oil** last night to fix the server downtime before our next major release.
4. We have done our part to prepare the system; now **the ball is in your court** to complete the server configurations.
5. We've made all the necessary updates. Let's **keep our fingers crossed** that the server will perform well during peak hours.
6. We can worry about scaling for international users later. For now, we'll **cross that bridge when we come to it.**
7. The slow loading times could just be **the tip of the iceberg**. We may need to examine the server logs for deeper problems.

B. Fill in the blanks using the idioms below. Each sentence requires a combination of two idioms. Change the forms of the verbs if necessary.

Bite the bullet, keep our fingers crossed, cross that bridge when we come to it, the tip of the iceberg.

1. When the main server crashed during peak hours, I had to _____ and pay for the expensive emergency migration while _____ that the backup data wasn't corrupted.
2. We know the current hardware won't handle next year's traffic, but we've decided to _____ and just _____ that we don't hit those numbers early.
3. The slow page load times are just _____ regarding our database issues, so we might as well _____ now and rewrite the entire backend architecture.
4. I'm _____ that the security patch works, though I suspect these minor glitches are only _____ for our outdated server software.

5. Instead of worrying about a total system failure that might never happen, let's _____ and simply _____ by upgrading our RAM today.
6. The specialist decided to _____ and switch to a cloud provider, _____ that the hidden migration costs wouldn't exceed the budget.
7. Realising the minor latency spike was just _____, the team prepared to _____ by drafting a full disaster recovery plan.

Borrowed and modified from: https://gemini.google.com/

GRAMMAR

9. A. & B. Put the verbs into the correct form. Use present tenses in the sentences below.

1. The web server _____ **(receive)** thousands of requests every hour.
2. As a web server administrator, I _____ **(maintain)** the servers that host websites and web applications for 5 years.
3. My friend, an admin in the IT company, _____ **(have)** the overall control of a server since the beginning of this company.
4. Google, Microsoft, and Facebook _____ **(have)** their servers for many years.
5. The IT team _____ **(upgrade)** the web server's memory to improve its performance now.
6. Hewlett Packard Enterprise (HPE) is a global server company. The company _____ **(be)** in the server market for many years and _____ **(be)** always an important player in the sector.
7. The web server _____ **(host)** the company's website for three years now.
8. The website _____ **(be)** available 24/7 on the web server.
9. Many developers _____ **(work)** on updating the server's software for weeks.

10. The web server _____ **(process)** data efficiently and quickly.
11. The company's IT team _____ **(monitor)** the server's performance for hours to identify any issues.
12. Some people _____ **(try)** to hack into the server for several weeks. But they haven't achieved their aim.
13. The server _____ **(experience)** technical difficulties since the morning.
14. The developers _____ **(test)** the new web server software to ensure it's bug-free.
15. The experts _____ **(work)** all day to fix the problem with the web server.

10. **A. Choose the correct answer.**

1. A web server is a computer that hosts a web site and makes its content available ***with / to*** clients, usually over the Internet.
2. A web server is a powerful machine that ***stores / retains*** and manages the site's files, databases and applications, and makes these ***accessible / reasonable*** via unique domain / IP addresses.
3. When a user requests a web page, the web server retrieves the ***requesting / requested*** data from its storage.
4. Then, the web server sends the data it ***is retrieving / has retrieved*** back to the user's browser, allowing the user to view the content.
5. Web servers can be configured ***processing / to process*** different types of requests, for example, HTTP requests for web pages, FTP requests for file transfer, or email requests for email service.
6. Various technologies and techniques such as load balancing, caching and SSL encryption ***must be used / can be used*** to optimise performance, security and scalability.
7. Web servers can also run ***in / on*** a variety of operating systems, including Linux, Windows and MacOS.

8. They can be managed ***use / using*** a range of tools and software, including Apache, Nginx and Microsoft IIS.
9. Some web servers ***are also designed / also design*** for specific uses, like specialised e-commerce servers for online shopping platforms or cloud-based servers for scalable infrastructure.
10. Overall, web servers play an important role in ***delivered / delivering*** websites and online services to users worldwide.

B. There is an odd word in some of the lines. Find it and write in the space provided.

A web server plays a vital role in the function of the Internet,	1 √
being serving as the foundation of online communication. Its main	2
function is in the storage and management of web pages, so that	3
when users access a web page via their with web browser,	4
they are presented with the information they require.	5
The web server has fetches the requested data from its memory,	6
is prepares the data for the user, if necessary, before sending the data	7
back. The web server also authenticates users, before handles	8
requests for specific resources, and facilitates if communication	9
between different others systems and applications.	10

LISTENING

You are going to watch a video about demystifying web server hacking (techniques, vulnerabilities, and countermeasures).

11. A. & B. Before watching a video, check if you know the meaning of the words and phrases. Use Merriam-Webster Dictionary if necessary.

Dedicated machine, run on, a static web page, vulnerabilities, configuration, intrusion, compromised, defaults, maintenance, consequences, defaced, open-source web server architecture, malicious intent, providing default documents, authentication, certificate mapping, authentication of credentials.

12. Watch the video "Demystifying Web Server Hacking: Techniques, Vulnerabilities, and Countermeasures".

Do the following tasks.

12.1. Choose the correct answer.

1. What is a web server?
    a. A cloud-based service that hosts websites.
    b. A software application that runs on a user's device.
    c. A dedicated machine or virtual machine running a web service.
2. Why are web servers more vulnerable to attacks?
    a. Because they are constantly interacting with users.
    b. Because they are less secure and easily accessible via the internet.
    c. Because they are more complex than other types of servers.
3. The hierarchy of web servers involves seven stacks. One of them is:
    a. Database
    b. Files
    c. Certificates

4. What is one way, web servers can be compromised?
    a. By not having a certificates
    b. By not setting proper permissions for files or directories
    c. By not having a firewall
5. According to the text, one of the consequences of web server attacks is:
    a. defacement of websites
    b. increased traffic
    c. absence of internet connection
6. What is the name of the web server component in the LAMP stack?
    a. IIS
    b. Apache
    c. Svchost.exe
7. What is the purpose of Svchost.exe in the IIS architecture?
    a. To provide authentication and certificate mapping
    b. To assist network processes
    c. To cache HTTP requests

12.2. Match 1–6 with a–j.

1	Web server definition	**a**	Attackers target vulnerabilities / configuration errors in software.
2	Security issues with web servers	**b**	Conflicts with security due to business ease-of-use.
		c	The web server itself is Apache.
		d	A web server is a software / hardware combination that hosts websites.
3	Why are Web Servers Compromised?	**e**	Compromising user accounts.

4	Consequences of Web Server Attacks	**f**	A web server is a dedicated machine or virtual machine running a web service.
		g	It's got little modules that do things like authentication, certificate mapping, providing default documents, caching http, providing errors and logging.
5	Open-Source Web Server Architecture	**h**	Improper authentication for external systems
		i	There are many web services. For example, Apache, IIS and JINX.
6	IIS Web Server Architecture	**j**	Bugs in O/S.

13. A. & B. Watch the video again and talk about the issues below.

1. Security issues with web servers.
2. The reasons why web servers are compromised.
3. Consequences of web server attacks.

Then express your opinion about the methodology, the attack tools, and the attack countermeasures.

SPEAKING

14. A. Work in pairs. In the forum, you and a partner discuss some web server issues: different top web server software and security practices. Using information from the table, act out a dialogue below. Your dialogue should include at least 5–6 exchanges per each participant. Be creative! Remember to keep the tone respectful!

A	B
1. Hi …, I've been reading about different web server software. I am wondering what you think about Nginx. Is it as good as Apache?	**1.** Yes, Nginx is actually a popular choice for many websites. It's known for ….
2. What about Microsoft IIS? …..	**2.** Yes, IIS is definitely a popular choice for …. But …
3. That's true. Security is a big concern for … What …..	**3.** Well, first, I make sure to keep my software up to date and ….
4. ….. any recommendations …	**4.** Definitely! ……
5. ……	**5.** ….
6. ….	**6.** …..

B. Work in pairs. For your ESP lesson, make up a list of questions about web servers. Then role play a dialogue using these questions. Your dialogue should include at least 7–8 exchanges per each participant. Be creative! Remember to keep the tone respectful!

15. **A. For the ESP lesson, prepare some information about web servers. Use the plan.**

1. Definition.
2. How does web server work?
3. Examples of web server uses.
4. Dynamic vs. static web servers.
5. Top web servers on the market.
6. Web server security.

B. You are going to participate in the conference "Web servers and their security". Create a presentation on one of the topics below.

1. Web server vulnerabilities and how to mitigate them.
2. Implementing SSL / TLS certificates for secure communication.
3. Managing authentication and authorisation for web servers.
4. Detecting and responding to web server-based attacks.
5. Best practices for securing web server configuration files and code.
6. Using Intrusion Detection Systems (IDS) to monitor web server security.
7. Securing web server data with encryption and hashing.

WRITING

16. **A. & B. For your research, write a paragraph about one of the web servers: Apache Web Server, IIS Web Server, Nginx Web Server, LiteSpeed Web Server, Node.js.**

A paragraph involves:

a) a topic sentence that sets the tone for the paragraph;
b) supporting details or evidence that develop the idea;
c) explanation of the information;
d) a conclusion that ties the paragraph together.

17. **A. For your website, write a blog entry of 150–160 words on the topic "The role of cloud computing in web server management". Use key words: *cloud computing, web server management, scalability, flexibility, cost-effectiveness, reliability, security.* Structure your blog entry with an introduction, main body, and conclusion. Focus on clarity and coherence.**

B. For your website, write a blog entry of 180–200 words on one of the following topics. Ensure that your writing is structured with an introduction, a main body, and a conclusion. Remember to focus on clarity.

1. Common web server attacks: types and techniques.
2. DDoS attacks on web servers: mechanisms and mitigation strategies.
3. SQL injection and cross-site scripting: threats to web servers and their mitigation.
4. Impact of zero-day vulnerabilities on web server security.
5. Practices for securing web servers: defence strategies.

REFLECTION AND SYNTHESIS

18. **You have completed this unit. This word cloud can help you to reflect on and synthesise the key concepts from the topic. Focus on the most important terms and ideas that stood out to you. Using the word cloud as a visual tool, you have to illustrate your understanding.**

1.5. UNIT 1. REVISION 1

WARM UP

1. **A. & B. Decide whether these sentences are *true* or *false*.**

1. Agile is a methodology that promotes flexible and iterative project management.
2. Product owner realises project management.
3. The main purpose of website security is to protect sensitive data and prevent unauthorised access.
4. A typical web server today contains four elements in addition to the physical hardware.
5. Cross-site scripting is a common web security vulnerability where attackers inject malicious scripts into web pages.
6. Static websites cannot be updated without altering the underlying code.
7. All types of websites require the same level of security measures, regardless of their purpose.
8. In Agile methodology, the project scope is strictly defined at the start of the project and cannot change.
9. Website accessibility ensures that people with disabilities can use and navigate the site effectively.
10. The use of extensive animation and graphics always enhances the user experience on a website.
11. The term “above the fold” originated from the design of newspapers.
12. Most browsers default to a 14-point font size to ensure readability and accessibility.

READING

2. **Read the text and do the following tasks.**

2.1. Decide if the statements are *true* or *false*.

1. Transparency, inspectation and frequency are key pillars.
2. A client can be responsible for prioritising work.
3. A sprint is a fixed time period (1–4 weeks) during which a development team works to complete a set of tasks.
4. During the sprint, the backlog can be changed.
5. In Step 2, the roles in Scrum teams are assigned: the Product Owner, Scrum Master and development / project team members.

2.2. Fill in the missing information in statements 1–5.

1. There are three key pillars of Scrum: transparency, inspection, _____ .
2. _____ are maintained by the Product Owner.
3. At the end of the sprint, the team will share their completed work with the key _____ and _____ .
4. _____ is responsible for the process and advocates for the team.
5. _____ are visible information documentation, including burn down charts of tasks and the task status board.

SCRUM

The Scrum method involves working within a team, led by a Scrum Master. The role of the Scrum Master is to complete work required, remove any obstacles impacting project outcomes and collaborate to meet the desired end-state. Similar to the Agile method, work is completed within short cycles or sprints. Within these sprints the team will meet daily, holding stand-ups where they discuss current work on hand, support required and roadblocks.

There are three key pillars of Scrum: transparency, inspection, adaption.

To use Scrum, the project must start with a clear purpose which is either provided by or to the business, and a set of requirements which are prioritised. There are several key terms and components which make up Scrum:

Features: these requirements are created by the client and / or organisation.

Backlog: storage document which outlines all features which are yet to be started. Backlogs are maintained by the Product Owner.

Product Owner: the client or representative who is responsible for prioritising work.

Sprints: short or set periods of time which the team is allocated to complete selected work or features. These can be between 1 and 4 weeks. The length should be consistent throughout the project life cycle.

The Scrum Guide outlines a number of elements that need to be completed or considered during the course of a project:

- Team members select requirements from the backlog, and they identify requirements which are achievable in the time-frame.
- A sprint backlog is created to document requirements and tasks that need to be discussed as part of the sprint planning meeting.
- As the team commits to the sprint backlog, work begins on key tasks and requirements.
- During the sprint, teams are protected from interruptions and their focus is on meeting outcomes.
- During the sprint, no changes are made to the backlog.
- The backlog requirements and priorities can be shifted in preparation for the next sprint.
- Daily stand-ups occur each day (15-minute meetings). Team members share what they completed yesterday, plan for today and discuss any blockers.

- At the end of the sprint, the team will share their completed work with the key stakeholders and clients. This will be used to obtain feedback to support future work. Reflection sessions (also called retrospectives) are used to support improvements.

Within the Scrum Guide there are 3 primary roles:

Scrum Master: responsible for the process and advocates for the team. They are responsible for removing obstacles or blockers, supporting team communications through discussion and mediation, negotiates resources and negotiates with the external team. They are primarily there to support the team.

Product Owner: responsible for representing the client's voice and making decisions regarding the project priorities. They are the owners of the backlog, communicate the stakeholder's vision, and works with the team daily to answer questions and provide guidance and support.

Project Team: the team is comprised of 7 members (plus or minus 2), who are responsible for project delivery. They are responsible for the estimations, committing to tasks, and daily status reports. The team should also be self-organising, requiring no specific structure.

Applying Scrum. Figure 1 shows the key phases within the Scrum process. It highlights that there are several different components within Scrum, including multiple meetings. These ceremonies include sprint planning meetings, daily stand-ups, review sessions and retrospectives. There are several reporting requirements and steps within Scrum, including:

Step 1. Familiarisation with the Scrum guidelines: understand the steps required to use Scrum within a project.

Step 2. Assign roles within Scrum teams: identify the Product Owner, Scrum Master and development / project team members.

Step 3. Create backlog: identify the breakdown of the different tasks and activities required.

Step 4. Sprint planning meeting and daily stand-ups: held on the first day of each sprint. All members should attend. Within this meeting:

Product Owner presents the next priorities that need to be completed.

Project team determines how these priorities will be addressed, including estimating how long items will take and what the project team can commit to.

Daily stand-up allows team members to provide updates on their progress.

Step 5. Determine sprint start and end dates: ensure that each project team member is aware of the length of a sprint, when they start and when they finish.

Step 6. Review and reflect: at the end of each sprint, run a reflection session to understand what worked and what did not, while ensuring performance is reviewed.

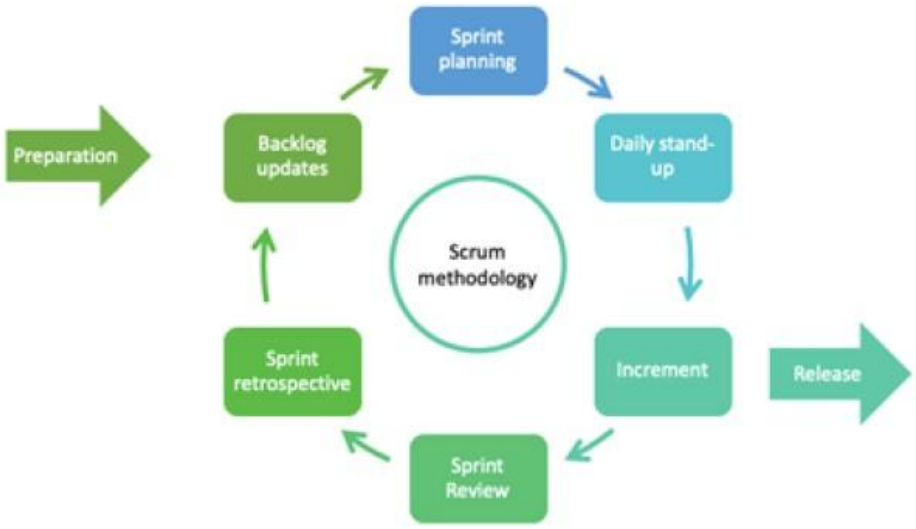


Figure 1. *Scrum process example, by Carmen Reaiche and Samantha Papavasiliou, licensed under CC BY (Attribution) 4.0*

Additionally, the project team needs to track their progress. Once work has commenced, progress is tracked through “radiators”. Radiators are visible information documentation, including burn down charts of tasks and the task status board.

The radiators are organised into five columns: *Story* (the client's requirements), *To Do* (tasks yet to be started), *In Process* (tasks currently being worked on), *To Verify* (tasks requiring testing or verification), and *Done* (completed tasks). This representation enables the project team to easily monitor their progress and identify areas that need attention.

In sum, Scrum is a common form of Agile project management. This framework supports team members to collaborate with one another, clients, and stakeholders to support achieving the goals and outcomes of the project. Due to its iterative and incremental nature, Scrum is a flexible process which is aimed at satisfying the client's expectations.

3. Find words and phrases in the text that match definitions 1–7.

1. _____ is a facilitator who makes sure that the Scrum framework is followed and helps the team to improve its processes.
2. _____ is a priority list of tasks to be completed, often consisting of the product backlog and sprint backlog.
3. _____ is a fixed time iteration, typically lasting 1–4 weeks, during which the development team works on selected backlog items.
4. _____ are short meetings where team members share progress and identify any obstacles.
5. _____ is responsible for maximising the value of the product by managing the backlog and ensuring that it reflects stakeholder needs.
6. _____ are visual tools, such as charts or boards, that provide transparency about the team's progress and the challenges.
7. _____ is an Agile framework that promotes iterative development and team collaboration to deliver quality products incrementally.

4. **Answer the questions.**

1. What is Scrum?
2. What key pillars are mentioned in the text?
3. What key terms and components make up Scrum?
4. What three roles are important for Scrum?
5. What key phases are involed in Scrum?

USE OF ENGLISH

5. **A. Fill in with *portfolio websites, dynamic website, iterative, visual elements, web page, collaboration, white space, static website, personal website, operating systems*.**

1. The Agile framework is considered as an _____ methodology.
2. _____ , both within and outside the organisation, is a vital component of successful implementation of Agile.
3. The _____ may lack interactive features, personalised content, and scalability.
4. A _____ is one that changes itself frequently and automatically.
5. The term "_____" is a virtual representation of a physical book, where separate pages are linked together to form a cohesive online entity.
6. _____ are focused on your skills and they help to attract potential employers or clients.
7. A _____ is a space where you can truly express yourself.
8. The _____ should help lead the user to the key items on your website.
9. Use _____ on your page to reduce visual clutter.
10. Traditionally, _____ for servers fall under three categories: Linux-based, Windows-based, and Mac-based.

B. Complete the sentences.

1) _____ was developed in the early **2) _____** by Linus Torvalds, a student who wanted to **3) _____** the UNIX systems at his university without relying on existing **4) _____** systems. As the project evolved and gained strength, Linus decided to share it with others, initially presenting it as a **5) _____** project and inviting feedback. However, he could not predict the vibrant community that would make Linux into what it is **6) _____** . The Linux **7) _____** has become the foundation for numerous Linux-based operating systems, often referred to as "**8) _____** ", and it is used globally, even in the **9) _____** rooms of competitors like Microsoft.

6. **A. Put the verbs in brackets into the correct present tense.**

1. Does the project manager _____ **(reviewing)** the timelines for the IT project every morning?
2. Now the team _____ **(design)** a new user-friendly interface for the website.
3. We _____ **(launch)** the new website ahead of schedule.
4. The developers _____ **(work)** on optimising the website's load speed right now.
5. Our security software _____ **(protect)** the site from multiple attacks this month.
6. The team members often _____ **(talking)** about potential improvements in website security.
7. I _____ **(test)** the web server for any vulnerabilities today.
8. We _____ **(implement)** new security measures to enhance the website's protection.
9. The project stakeholders _____ **(attending)** weekly meetings to discuss progress and challenges.

10. Our designers _____ **(update)** the website design to keep it modern and appealing.
11. _____ you ever **(develop)** _____ the website?

B. Complete the sentences using the words in bold. Use two to five words.

1. Tom keeps interrupting me at this sprint planning meeting.
   Tom **is** …….
2. What is the meaning of the word "agile"?
   What **does** ……?
3. Developing a website is new to me.
   …….. **before**.
4. What's your opinion of this website?
   ……. **think** …….?
5. I started developing this website in October. I'm still developing it.
   …… **been** …….
6. I am on the fifteenth page of the Scrum Guide I am reading.
   So far I …. ……..
7. Agile teams are still enhancing their skills through Agile training sessions. They started last month.
   ……. **been** ……...
8. Many organisations keep adopting Agile practices to enhance their productivity currently.
   ……. **are** ……..
9. I find working on this project enjoyable.
   ……. **enjoying** ……...
10. Team members keep engaging in daily stand-ups to synchronise their efforts.
    …… **engaging** ……...

SPEAKING

7. Work in groups. Choose one of the rubrics and discuss the questions.

1. IT Project Management

1. What are the main phases of IT project management? What key activities occur in each phase?
2. Can you compare and contrast two project management methodologies: Agile and Waterfall, Scrum / Kanban, Lean / Scrum?
3. What are the roles and responsibilities of a project manager in an IT project?
4. How can stakeholder engagement impact the success of an IT project?

2. Types of Websites

5. What are the main differences between an e-commerce website and a portfolio website?
6. Name at least three types of websites and describe their target audiences.
7. How does blogging differ from corporate websites?
8. What are the differences between a static web site and a dynamic web site?

3. Website Design

9. What are the key principles of effective website design?
10. Why is user experience critical in the design of a website?
11. How can responsive design affect website usability across different devices?
12. What essential elements should be included in a website's navigation menu?

4. Security of Websites

13. What are common website security threats?
14. Why is the website encryption important?
15. What measures can be implemented to prevent SQL injection attacks on websites?
16. How does regular software updating contribute to website security?

5. Web Servers and Security of Web Servers

17. What is the function of a web server? How does it serve web content to users?
18. What is the difference between shared hosting and dedicated hosting?
19. What are some common security practices for protecting web servers?
20. What role does it play in a web server, besides serving as an HTTP component?

8. Work in groups. Choose one of the activity and do the task.

1. IT Project Management

A. A project manager notices low team motivation as deadlines approach. What steps can he / she take to manage team dynamics and maintain productivity while meeting project deadlines?

B. A software development startup is launching a new app but is having with changing priorities and scope creep. Discuss the causes of these problems and propose strategies to improve project management processes.

2. Types of Websites

A. Are personal blogs still relevant in today's digital world, or have social media platforms replaced them? Discuss the benefits and limitations of both.

B. Analyse how the shift to mobile devices has affected the types of websites being created. What implications does this have for future web development?

3. Website Design

A. As a web designer, you present your design to a client who prefers flashy designs but has a target audience that appreciates simplicity. Discuss how you would persuade him / her to put user experience before aesthetics.

B. In groups, create a design for a non-profit organisation's website that focuses on user accessibility and engagement. What key features should be included?

4. Security of Websites

A. A company's website experiences a data leakage due to a poor password policy. Discuss the immediate actions that the company should take as well as preventive measures for the future.

B. A developer discovers vulnerabilities in a partner's website. Should they disclose these vulnerabilities, and if so, how? What are the implications for both parties?

WRITING

9. **You are asked to write a paragraph (120–150 words) on one of the topics given below.**

Use any five phrasal verbs: ***carry on, carry out, carry forward, carry through, change over, change up, change back, change around, change in, bring up, bring together, bring in, break down, break through, break away, build up, build on, build out.***

1. **IT project management.**
2. **Website security.**
3. **Types of websites.**
4. **Website design.**
5. **Website security.**
6. **Web servers and their security.**

10. **To participate in the *Opinion Essay Contest,* you need to write an essay (180–200 words) on one of the topics given below. Your essay should follow a clear structure, consisting of an introduction, main body, and conclusion. Additionally, you must incorporate the idioms: *in the same boat, a double-edged sword, breaking the ice, a treasure trove, on the same wavelength, to bite the bullet, to keep our fingers crossed, to cross that bridge when we come to it, the tip of the iceberg, to hit the ground running, to burn the midnight oil, the ball is in your court.***

A. Use at least seven idioms.

B. Use at least ten idioms.

Topics:

1. **IT project management.**
2. **Website security.**
3. **Types of websites.**
4. **Website design.**
5. **Website security.**
6. **Web servers and their security.**

PROJECT

11. **Work in small groups. Your university administration has been asked to create a community platform for students. The platform will serve different purposes:**

- ✓ **event scheduling,**
- ✓ **local news distribution,**
- ✓ **forum discussions,**
- ✓ **networking opportunities,**

- ✓ **academic resources,**
- ✓ **volunteer service,**
- ✓ **student feedback and polls,**
- ✓ **a marketplace for local artisans.**

As a team, you are tasked to develop the project plan and the initial design for this website. You need to explain how the following concepts relate to your project's framework:

1. **IT Project Management. Plan the project timeline, resources needed, and roles within the team.**
2. **Types of Websites. Identify what type(s) of website this project will encompass (e.g., an informational site, a forum, an e-commerce section, etc.).**
3. **Website Design. Develop a design brief that includes user-friendly navigation, appealing aesthetics, and accessibility features.**
4. **Security of Websites. Discuss the necessary security measures to ensure user data protection, especially in the marketplace and forum sections.**
5. **Web Servers. Decide whether you will use cloud hosting or traditional hosting services for the platform.**
6. **Security of Web Servers. Plan how to secure the web server environment, including firewalls and regular security audits.**

Demonstrate your understanding of how each component is important to the final goal of developing a secure, functional, and appealing community engagement platform.

UNIT 2

UNIT	WARM UP	READING	USE OF ENGLISH	LISTENING	SPEAKING	WRITING	REFLECTION
2.1. Classical Crypto-graphy. Ciphers and Codes	Students' background knowledge about classical cryptography, ciphers and codes. Analysing the statements about cryptography generated by AI	Classical cryptography. Ciphers and codes	Language use in terms of the topic. Past tenses	Secret codes: a history of cryptography	Speaking about the difference between codes and ciphers, their specifics	Writing a definition, an informative report	Reflecting and synthesising
2.2. Crypt-analysis	Students' background knowledge about cryptanalysis	Cryptanalysis. Cryptanalysis Attacks	Language use in terms of the topic; expanding vocabulary using AI. Past tenses	What is cryptanalysis? The science of codes: an intro to cryptography	Speaking about the difference between linear and differential cryptanalysis, cryptanalysis tools, attacks	Writing a summary of the audio text	Reflecting and synthesising
2.3. Stegano-graphy	Students' background knowledge about steganography	Steganography	Language use in terms of the topic. Past tenses	How to hide data inside images (stegano-graphy)	Speaking about types of steganography, history of steganography, steganography vs. cryptography	Analysing the for and against essay written by AI. Writing a for and against essay	Reflecting and synthesising
2.4. Digital water-marking	Activating students' background knowledge about digital watermarking	Digital watermarking	Language use in terms of the topic; expanding vocabulary using AI. Past tenses	Digital watermarking	Speaking about the specifics of watermarking	Writing a summary of the written and / or the audio text	Reflecting and synthesising

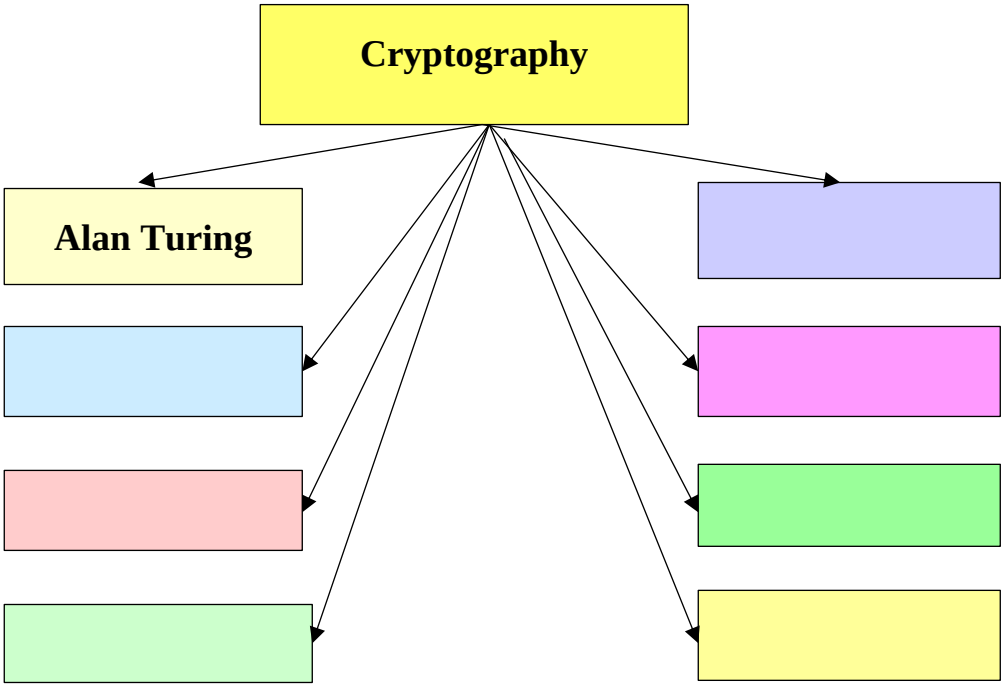
2.1. CLASSICAL CRYPTOGRAPHY. CIPHERS AND CODES

WARM UP

1. **Using your background knowledge about classical cryptography, do the tasks according to your learning style (dominant or non-dominant modality).**

1.1. ***Visual Modality***

Individually, think about the names of famous cryptographers. Then in small groups create a mind map, share and discuss the findings. Each group member should take turns explaining the contributions of the cryptographers.



1.2. *Auditory Modality*

Work in a small group. The AI Text Generator has generated the statements about cryptography. Some of these statements may be considered controversial, while others are not. Differentiate these statements into two groups: *Controversial (C)* and *Non-controversial (N)*. Then give a short explanation for each group, explaining why you have grouped the statements as you have.

1. The widespread use of encryption in messaging apps has enabled terrorists and other malicious actors to communicate undetected, allowing them to plan and execute attacks.
2. A digital signature is a type of encryption that proves the authenticity of a message without revealing its contents.
3. Backdoors in encryption algorithms, intentionally inserted by government agencies, are necessary to allow law enforcement to access encrypted communications in cases of national security.
4. End-to-end encryption, which is used by popular messaging apps like WhatsApp and Signal, is a flawed concept that prioritises privacy over public safety and can be used to conceal illegal activities.
5. Hash functions are used to create a digital fingerprint of data, which can detect any changes to the data.
6. The creation of quantum-resistant encryption algorithms is a waste of time and resources, as the development of practical quantum computers is still years away.
7. Public-key cryptography uses a pair of keys: a public key for encryption and a private key for decryption.
8. The use of homomorphic encryption, which allows computations to be performed on encrypted data without decrypting it first, is a security risk that

could lead to significant vulnerabilities in critical infrastructure.

9. Encryption scrambles data into a code that can only be deciphered with the correct decryption key.
10. Symmetric encryption is faster and more efficient than asymmetric encryption, but it requires both parties to share the same secret key.

Generated by AI Text Generator: https://deepai.org/chat/text-generator

1.3. *Kinesthetic Modality*

Fill in the table below. Define the terms "cryptology", "cryptography", "cryptographer", "cryptologist". Analyse and compare the differences between these concepts. Then explain the roles and contributions of both a cryptographer and a cryptologist in the field of cybersecurity.

Term	Explanations
Cryptology	……
Cryptography	……
Cryptologist	……
Cryptographer	……
Differences between concepts:	……
Roles and Contributions of both a cryptographer and a cryptologist in Cybersecurity:	……

READING

You are going to read an article about classical cryptography.

2.

1. A. & B. Before reading, discuss the following quotations.

1. "Cryptography is typically bypassed, not penetrated."

Adi Shamir

2. "Cryptography is the ultimate form of non-violent direct action."

Julian Assange

3. "Cryptography shifts the balance of power from those with a monopoly on violence to those who comprehend mathematics and security design."

Jacob Appelbaum

2. A. & B. Before reading, look at the following words and phrases, which have been taken from the text. In what context might they be mentioned? Use Merriam-Webster Dictionary if necessary.

Encryption, ciphertext, cipher, principle, eavesdropper, algorithms, indecipherable, circumstances, concentrated, interpret, encipherment, auxiliary, crypto variable, public / private key.

3.

A. & B. Read the text about classical cryptography. Four paragraphs have been removed. Choose which of the paragraphs fit into the gaps.

A	Codes generally substitute different length strings of characters in the output, while ciphers generally substitute the same number of characters as are input. A code maps one meaning with another. Words and phrases can be coded as letters or numbers. Codes typically have direct meaning from input to key. Codes primarily function to save time. Ciphers are algorithmic. The given input must follow the cipher's process to be solved. Ciphers are commonly used to encrypt written information.

B	We assume *Eve*, the **eavesdropper**, may observe the ciphertext, so the goal is for it to be meaningful to *Bob* but meaningless to *Eve*. An eavesdropper is someone who secretly listens to conversations, originally referring to someone who hung from a building's eaves to overhear inside talks.
C	Most modern ciphers are categorised by whether they operate on fixed-size blocks (**block ciphers**) or continuous streams (**stream ciphers**), and whether they use the same key for both encryption and decryption (**symmetric**) or different keys (**asymmetric**). Symmetric keys must be shared secretly, while asymmetric algorithms use a public / private key pair, allowing one key to be public without compromising security.
D	If the algorithms themselves are not secret, then there must be some other secret information in the system. That information is called the **(secret) key**. The key is just an extra piece of information given to both the *Enc* and *Dec* algorithms. Another way to interpret Kerckhoffs' principle is that *all of the security of the system should be concentrated in the secrecy of the key*, not the secrecy of the algorithms. If a secret key gets compromised, you only need to choose a new one, not reinvent an entirely new encryption algorithm. Multiple users can all safely use the same encryption algorithm but with independently chosen secret keys.

CLASSICAL CRYPTOGRAPHY

Cryptography is the mathematical basis for secure systems, focusing on safe storage, transmission, and processing of information, while cryptology includes both cryptography and cryptanalysis.

Encryption Basics & Terminology

Let's formalise the scenario (fig. 1): *Alice* has a message m (the **plaintext**) she wants to send privately to *Bob*. She transforms m into **ciphertext** c using

Encryption (Enc). When *Bob* receives c, he uses **Decryption** (Dec) to recover the original message m.

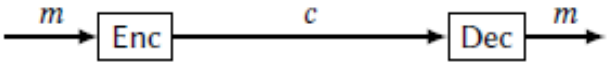


Figure 1. *Encryption*

1. _____

Secrets & Kerckhoffs' Principle

Something important is missing from this picture. If we want Bob to be able to decrypt *c*, but Eve to not be able to decrypt c, then Bob must have some information that Eve doesn't have. Something has to be kept secret from Eve.

You might suggest to make the details of the *Enc* and *Dec* algorithms secret. This is how cryptography was done throughout most of the last 2000 years, but it has major drawbacks. If the attacker does eventually learn the details of *Enc* and *Dec*, then the only way to recover security is to invent new algorithms. If you have a system with many users, then the only way to prevent everyone from reading everyone else's messages is to invent new algorithms for each pair of users. Inventing even one good encryption method is already hard enough!

The first person to articulate this problem was Auguste Kerckhoffs. In 1883 he formulated a set of **cryptographic design principles**. They are:

1. The system must be practically, if not mathematically, indecipherable.

2. It should not require secrecy, and it should not be a problem if it falls into enemy hands.

3. It must be possible to communicate and remember the key without using written notes, and correspondents must be able to change or modify it at will.

4. It must be applicable to telegraph communications.

5. It must be portable, and should not require several persons to handle or operate.

6. Lastly, given the circumstances in which it is to be used, the system must be easy to use and should not be stressful to use or require its users to know and comply with a long list of rules.

Some are no longer relevant given the ability of computers to perform complex encryption. The second principle, now known as **Kerckhoffs's principle**, is still critically important.

2. _____

The process of choosing a secret key is called **Key Generation** (fig. 2), and we write KeyGen to refer to the (randomised) key generation algorithm. We call the collection of three algorithms (Enc, Dec, KeyGen) an **encryption scheme**. Kerckhoffs' principle says that we should assume that an attacker knows the details of the KeyGen algorithm. Knowing the details (i.e., source code) of a randomised algorithm doesn't mean you know the *specific output* it gave when the algorithm was executed.

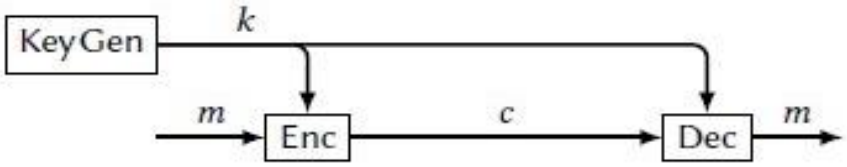


Figure 2. *Encryption scheme*

Ciphers & Codes

In cryptography, a **cipher** (or cypher) is an algorithm for performing encryption or decryption – a series of well-defined steps that can be followed as a procedure. An alternative, less common term is **encipherment**. To encipher or encode is to convert information into cipher or **code**. In common parlance, "cipher" is synonymous with "code", as they are both a set of steps that encrypt a message; however, the concepts are distinct in cryptography, especially classical cryptography.

3. _____

Codes use a codebook to substitute words or phrases with random strings of characters or numbers, like “UQJHSE” for “Proceed to the following coordinates”. Ciphers encrypt plaintext into ciphertext, which contains all the original information but is unreadable without the proper decryption.

The operation of a cipher usually depends on a piece of auxiliary information, called a key (or, in traditional NSA parlance, a cryptovariable). The encrypting procedure is varied depending on the key, which changes the detailed operation of the algorithm. A key must be selected before using a cipher to encrypt a message. Without knowledge of the key, it should be extremely difficult, if not impossible, to decrypt the resulting ciphertext into readable plaintext.

4. _____

Borrowed and modified from: Rosulek M. The Joy of Cryptography. School of Electrical Engineering & Computer Science Oregon State University, Corvallis, Oregon, USA, https://open.umn.edu/opentextbooks/textbooks/897
Trevisan L. Cryptography. Lecture Notes from CS276, Spring 2009, Stanford University, https://lucatrevisan.github.io/books/crypto.pdf
Kerckhoffs’s principle, https://en.wikipedia.org/wiki/Kerckhoffs%27s_principle
Cipher, https://en.wikipedia.org/wiki/Cipher
Modified by https://deepai.org/chat/text-generator

4. A. & B. Read the text again and do the following tasks.

4.1. Decide whether these sentences are *true* or *false*.

1. Kerckhoffs’ principle states that all security should be concentrated in the secrecy of the algorithms.
2. The key is a piece of information given to both the encryption and decryption algorithms.
3. Kerckhoffs’ principle is no longer relevant given modern computer capabilities.
4. Codes substitute different length strings of characters, while ciphers substitute the same number of characters as are input.

5. Asymmetric key algorithms use the same key for both encryption and decryption.
6. The operation of a cipher does not depend on a piece of auxiliary information, called a key.

4.2. Fill in the missing information in statements 1–6.

1. Cryptography studies ways of securely storing, transmitting, and _____ _____ .
2. The term "_____" refers to a person who secretly listens to a conversation between other people.
3. The system must be practically, if not mathematically, _____ .
4. _____ generally substitute different length strings of characters in the output, while _____ generally substitute the same number of characters as are input.
5. A key must be selected before using a cipher to _____ a message.
6. If the algorithm is _____, the key must be known to the recipient and sender and to no one else.

5. **A. & B. In pairs, select one word from the provided list. Student A asks the questions below, putting the chosen word into each question, while Student B responds using that word. You may skip any questions that do not apply. After completing the questions, switch roles and repeat the activity with a different word. See the example below.**

Cipher, drawback, principle, encryption, secret, prevent, substitute, characters, algorithm, private, public, eavesdropper, ciphertext, cryptography, decrypt, encrypt.

1. What does _____ mean?
2. What is the plural / singular of _____?

3. What is the synonym of _____?
4. What is the opposite of _____?
5. What is the noun for _____?
6. What is the verb for _____?
7. What is the adjective for _____?
8. What is the adverb for _____?
9. Can you give _____ collocations?
10. How to use _____ in a sentence?
11. What is the translation for _____?

For example:

The chosen word is "project".

Student A: "What does project mean?"

Student B: "Project" is a planned set of activities or tasks intended to achieve a specific goal.

Student A: "What is the plural of project?"

Student B: "Projects."

6. **A. & B. Make a list of the five most important things that you have to remember about classical cryptography. Compare your list to your partner's. Which three are the most popular among the class?**

USE OF ENGLISH

VOCABULARY

7. **A. & B. Match the words / phrases with their meanings.**

1	code	**a**	scrambling a message with a code
2	cipher	**b**	unscrambling an enciphered message
3	encipher	**c**	replacement at the level of the words
4	encode	**d**	scrambling of both codes and ciphers.
5	decipher	**e**	unscrambling an encoded message
6	decode	**f**	replacement at the level of the letters
7	encrypt	**g**	unscrambling of both codes and ciphers
8	decrypt	**h**	scrambling a message with a cipher
9	public key	**i**	for dencrypting the data
10	private key	**j**	the practice of making and breaking of secure data
11	cryptography	**k**	for encrypting the data
12	cryptology	**l**	the practice of making data secure

8. **Choose one of the exercises and do it.**

A. Complete the sentences. Use: *plaintext, one-time pad, specify, attacker, Eve, reveal, eavesdropper's, ciphertext, key, encrypts, algorithm, security*.

Suppose Alice and Bob are using **1)** _____ but are concerned that an **2)** _____ sees their ciphertext. They can't presume what an attacker will do after seeing the **3)** _____. But they would like to say something like, "because of the specific way the ciphertext was generated, it doesn't **4)** _____ any information about the **5)** _____ to the attacker, no matter what the attacker does with the ciphertext".

We must first precisely **6)** _____ how the ciphertext is generated. The Enc **7)** _____ already describes the process, but it is written from the point of view of Alice and Bob. When talking about **8)** _____, we have to think about what Alice and Bob do, but from the **9)** _____ point of view! From Eve's point of view, Alice uses a **10)** _____ that was chosen in a specific way (uniformly at random), she **11)** _____ a plaintext with that key using OTP, and finally reveals only the resulting ciphertext (and not the key) to **12)** _____.

B. Complete the sentences.

Edgar Allan Poe was not only an **1)** _____, but **2)** _____ a cryptography enthusiast. He once wrote, in a discussion on the state of the art in **3)** _____: "Human ingenuity cannot concoct a **4)** _____ which human ingenuity cannot resolve."

This was an accurate assessment of the **5)** _____ that existed **6)** _____ 1841. Whenever someone would come up with an **7)** _____ method, someone else would inevitably find a way to **8)** _____ it, and the cat-and-mouse game would repeat again and **9)** _____ .

Modern 21st-century cryptography, **10)** _____, is different. There are many schemes whose security we can prove **11)** _____ a very specific sense. The codemakers can win against the code-**12)** _____.

PHRASAL VERBS

9. **A. Fill in the correct particles. Then explain the phrasal verbs. See Appendix 2, which contains a list of relevant phrasal verbs.**

1. While researching old encryption methods, I **came** _____ a very interesting example of the Vigenère cipher.
2. When using asymmetric encryption, the choice of public and private keys **comes** _____ significantly for security.
3. In our secure communication system, we need to **deal** _____ unique key shares to all those involved to ensure confidentiality.
4. After evaluation of the vulnerabilities, we **decided** _____ the use of the outdated Caesar cipher for our project.
5. Before deployment, we need to **decide** _____ the encryption protocol that strikes the right balance between security and performance.
6. Experts from different fields need to **come** _____ to develop a strong cryptographic framework.
7. We will need to **deal** _____ the weaknesses in our encryption algorithm before we launch the system to guarantee the security of the data.

B. Replace the words or phrases in bold with the correct form of a phrasal verb using *come, deal,* and *decide*. Then, create three interconnected sentences that include any phrasal verbs with "come", "deal", and "decide".

1. While researching ancient texts, I **found by chance** an interesting manuscript describing early methods of cryptography.
2. In modern digital security, encryption protocols really **become relevant** to protect sensitive information from hackers.

3. During the international conference, experts from different fields **united** to discuss the future of cryptographic technologies.
4. The teacher decided to **distribute** the tasks in such a way that each student received a project related to cryptography.
5. To improve security, it is important for companies to **manage** vulnerabilities in their systems in a timely manner.
6. After careful consideration, the committee **chose not to use** outdated encryption methods that lack resilience.
7. They had to **make a choice** after the consideration of the most effective algorithm before incorporating it into their new software solution.

GRAMMAR

10. A. & B. Put the verbs into the correct past tense.

1. I _____ **(study)** different methods of encryption before I _____ **(decide)** to specialise in digital security.
2. My brother _____ **(study)** contemporary cipher techniques, while I _____ **(work)** on my paper.
3. By the time they _____ **(launch)** their project, the team _____ **(test)** their encryption software against a wide range of attacks.
4. She _____ **(prepare)** her presentation on decoding techniques for two hours before the conference began.
5. As they _____ **(decode)** the encrypted messages, they discovered hidden patterns that revealed important information.
6. Sam _____ **(decipher)** the message for two hours before he completed the task.

7. As Ann _____ **(review)** the historical codes, she realised that many of them had influenced modern cryptographic methods.
8. In 1883 Auguste Kerckhoffs _____ **(formulate)** a set of cryptographic design principles.
9. He said that they _____ **(encrypt)** the message.
10. The team _____ **(develop)** a sophisticated encryption algorithm for months before it was finally ready for testing.

A. Choose the correct answer.

1. The task of encoding a message _____ privacy is called encryption.
   a) preserve b) to preserve c) preserved
2. Methods for symmetric-key encryption _____ for literally thousands of years.
   a) have studied b) study c) have been studied
3. The process of _____ the message is known as decryption.
   a) decode b) decoding c) decoded
4. Understanding what cryptographic primitives can do and how they can be combined _____ to build secure systems, but it is not sufficient.
   a) is required b) requires c) require
5. The obvious weakness of such substitution ciphers _____ the very limited number of possible keys, so an adversary can easily try them all.
   a) is b) are c) are being
6. During the Second World War, the German Enigma machines used complex encryption techniques _____ multiple permutations and variable shifts to produce a unique coded message.
   a) involved b) involving c) involve
7. Most classic methods suffer _____ the problem of being deterministic

encryption schemes.

a) in b) of c) from

8. If the same message is sent twice, the encryptions _____ the same.

a) would be b) will be c) was

9. The disadvantage of the one-time pad is that Alice and Bob need to agree _____ advance on a key that is as large as the total length of all the messages they will ever exchange.

a) of b) on c) in

10. Your laptop cannot use one-time pad _____ with your base station.

a) to communicate b) communicate c) communication

B. Choose the correct answer.

1. Different substitution ciphers _____ in cultures with alphabetic _____ systems. The secret key is a permutation of the letters of the alphabet.
   a) was invented, written
   b) were invented, write
   c) were invented, writing
2. Encryption is performed by applying the permutation to _____ letter of the message, and decryption is performed by using _____ inverse permutation.
   a) every, a
   b) each, the
   c) every, ---
3. The Atbash cipher, _____ for encrypting Hebrew text, in which the first letter of the alphabet _____ by the last, the second letter by the second-last, and so on.
   a) used, is replaced
   b) using, replace
   c) use, is replaced

4. This technique _____ in _____ book of Jeremiah.
    a) famously employ, the
    b) is famously employed, the
    c) is employed famously, a
5. The Caesar cipher, attributed to Julius Caesar, is _____ simple encryption technique in which each letter is shifted three positions forward in the alphabet, _____ a subtle substitution of the original text.
    a) ---, producing
    b) a, produced
    c) a, producing
6. Substitution codes in which the permutation is allowed to _____ arbitrary were _____ throughout the Middle Ages and into modern times.
    a) being, used
    b) be, use
    c) be, used
7. With _____ alphabet, the number of keys is 26!, which is too large _____ a brute-force attack.
    a) a 26-letters, for
    b) a 26-letters, of
    c) a 26-letter, for
8. However, such systems are easily broken due to the fact that different letters _____ with different frequencies in any _____ language, so Eve _____ immediately guess what the encryptions of the most common letters are, and work out the whole code with some trial and error.
    a) occurs, gave, must
    b) occur, given, can
    c) occured, give, could

9. _____ The Arab scholar al-Kindy noticed this in _____ 9th century AD.

   a) The, the
   b) ---, the
   c) The, a

10. _____ "The Adventure of the Dancing Men", Sherlock Holmes _____ a substitution cipher.

   a) On, breaking
   b) In, break
   c) In, breaks

Borrowed and modified from: Trevisan L. Cryptography. Lecture Notes from CS276, Spring 2009 Stanford University. 154 p. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License.

LISTENING

You are going to watch a video that explores the secret codes during the history of cryptography.

11. A. & B. Before watching a video, check if you know the meaning of the words and phrases. Use Merriam-Webster Dictionary if necessary.

Hiding writing, transposition, substitution, skytale, rod, flaws, scramblings, rearranged, interceptor, to replace, shift, a wannabe code breaker, monoalphabetic, ingenious, treatise, occurring letter, deciphering, wrench, likelihood, mishmash, constantly bickering, burgeoning industry, misspell, encrypted message, a cunning and intelligent code breaker.

12. **A. & B. Watch the video "Secret Codes: A History of Cryptography (Part 1)". Decide whether these sentences are *true* or *false*.**

1. Herodotus' technique of hidden writing was used during the war with Persia in the 5th century BC.
2. The disadvantage of transposition ciphers is that a short message has limited scrambling.
3. The Caesar cipher is an example of transposition ciphers.
4. The Islamic Golden Age was a time of war and conflict in the Middle East.
5. The text states that the best method for the study of the Quran and the Hadiths was linguistic technique.
6. Al-Kindi was skilled in many fields, from mathematics to music, medicine and cryptanalysis.
7. Frequency analysis was only used in cryptography for encrypting messages.
8. The Dark Ages is a term the author generally dislikes. However, when it comes to cryptography, it is appropriate.
9. The Renaissance marked a renewed interest in cryptography in Europe.
10. By the 15th century, almost every court in Europe had a cryptographer's office and every ambassador had a cryptographer's secretary.
11. Nomenclatures were considered as a mix of ciphers.
12. The failure of Mary Queen of Scots' cipher to protect her secret communications ultimately led to her downfall and execution.

13. **A. Watch the video again and talk about the issues below.**

1. What cryptographic inventions from the Ancient World are discussed in the article? Please provide specific examples and their significance.

2. What was the contribution of the Islamic codebreakers to the development of cryptography?
3. What term is used to describe the period in European history when cryptography was not a priority? Why?
4. Why did cryptography become a growing industry during the Renaissance?
5. Who is credited with developing a better cryptographic system in the 16th century?

B. Watch the video again and summarise information in the video.

SPEAKING

14. A. Work in pairs. In the forum, you and a partner discuss some issues about codes and ciphers: the difference between codes and ciphers in cryptography, advantages and disadvantages of codes and ciphers. Use information from the table. Complete the table and role play the dialogue below. Your dialogue should include at least 5–6 exchanges per each participant. Be creative! Remember to keep the tone respectful!

A	B
1. I always confuse about the difference between codes and ciphers. Can you explain it to me?	Well, a code is ….., whereas a cipher is …….
2. So, a code is more like a word substitution game?	Well, codes can be more straightforward to create and use, but they're often less secure because …. Ciphers, on the other hand, are more secure because …
3. ……. advantages and disadvantages ….	

A	B
4. I've heard that Caesar Ciphers.	……
5. …….	……
6. …….	……

B. Work in pairs. For your ESP lesson, make up a list of ciphers and their specifics. Then, role play a dialogue using information about these ciphers. Your dialogue should include at least 7–8 exchanges per each participant. Be creative! Remember to keep the tone respectful!

15. **A. For the ESP lesson, you are asked to prepare a three-minute presentation about:**

1. Substitution ciphers. Transposition ciphers.
2. Polygraphic ciphers. Permutation ciphers.
3. Unsolved ciphers and codes you can't break.
4. Famous cryptographers and their contribution to science.

Choose one of the topics. Organise your presentation according to the structure:

1. Introduction.
2. Main body.
3. Conclusions.

B. You are asked to explain the quotations below.

1. "Cryptography is typically bypassed, not penetrated."

Adi Shamir

2. “There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files.”

Bruce Schneier

3. “Computers had their origin in military cryptography.”

Austin Grossman

WRITING

16. **A. & B. Work in small groups. For the research, you need to write a definition of the following ciphers:**

- **substitution ciphers,**
- **transposition ciphers,**
- **polygraphic ciphers,**
- **permutation ciphers.**

Choose one of the tasks and do it.

A. Create definitions that are appropriate for individuals with no background in cryptography. Your definitions should use simple language and relatable examples.

B. Create definitions for your groupmates within your graduate programme. These definitions have to be more technical and include specific terminology relevant to your field of study.

After writing the definitions, pair up with another group. Share your definitions and discuss how each definition meets the specific needs of your target audience. Consider aspects such as complexity, terminology, and the use of examples that are relevant to each group’s background.

17. **A. & B. For your ESP lesson, write an informative report on the topic "The role of cryptography in cyber security", with the length of 200 to 250 words.**

Follow the steps:

1. Begin with an introduction (outline the importance of cyber security in the digital world).
2. In the main body, explain the key concepts, discuss various cryptographic techniques and their applications; analyse examples where cryptography has played a critical role.
3. In conclusion, outline the future of cryptography.
4. Then, ensure your report is well-structured, clearly written, and properly referenced using reliable sources.

REFLECTION AND SYNTHESIS

18. **You have completed this unit. This word cloud can help you to reflect on and synthesise the key concepts from the topic. Focus on the most important terms and ideas that stood out to you. Using the word cloud as a visual tool, you have to illustrate your understanding.**

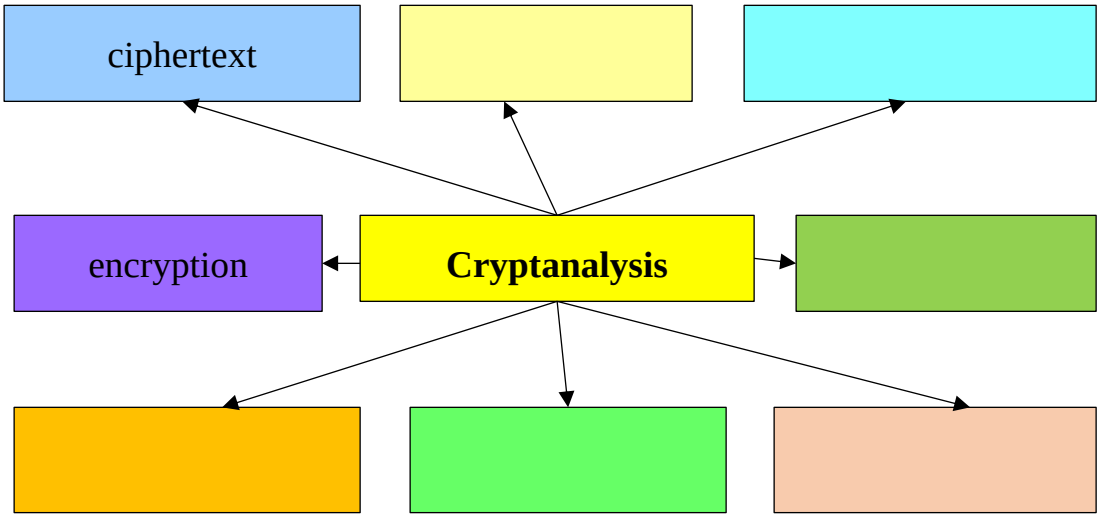
2.2. CRYPTANALYSIS

WARM UP

1. A. & B. Using your background knowledge about cryptanalysis, do the tasks according to your learning style (dominant or non-dominant modality).

1.1. *Visual Modality*

Work individually, then in a small group. Create a mind map with a central concept of *cryptanalysis*. Start by brainstorming relevant terms related to cryptanalysis. Clearly illustrate how each term relates to the central concept.



1.2. *Auditory Modality*

Discuss the questions.

1. What is cryptanalysis?
2. What is the aim of cryptanalysis?
3. How does cryptanalysis work?
4. Who uses cryptanalysis?
5. What do you know about cryptanalysis tools?
6. What is frequency analysis?
7. What is differential cryptanalysis / linear cryptanalysis?

1.3. *Kinesthetic Modality*

Searching the internet, fill in the table to answer the question:

What are the requirements and responsibilities of a cryptanalyst?

1	Protecting sensitive information from interception, copying, modification or deletion.
2	…….
3	…….
4	…….
5	…….
6	…….
7	…….

READING

You are going to read an article about cryptanalysis and cryptanalysis attacks.

2.

1. A. & B. Before reading, discuss the following quotation.

"Security is a process, not a product."

Bruce Schneier

2. A. & B. Before reading, look at the following words and phrases, which have been taken from the text. In what context might they be mentioned? Use Merriam-Webster Dictionary if necessary.

Accessing, insecurity, subversion, misconception, adversary, to compromise, assumed, ciphertext, unbreakable, brute-force, intercepted, nonrandom, arbitrary, to disclose, keylogger, unauthorised person, plaintext, vulnerability.

3. **Read the text about cryptanalysis and cryptanalyses attacks. Six sentences have been removed. Choose which of the sentences fit into the gaps.**

A	tries every possible key until the correct one is found, making all ciphers vulnerable except unbreakable ones like the one-time pad.
B	a cryptanalysis technique where the attacker can choose plaintexts to be encrypted and then observe the corresponding ciphertexts, with the ability to adapt their choices based on previous results, in order to gather information and eventually break the encryption scheme.
C	However, it can serve both ethical and malicious purposes: black hat hackers use it for cybercrime, while white hat hackers conduct security tests for organisations.
D	For example, a maid with access to her employer's computer, might insert a thumb drive containing malware that installs a keylogger that transmits keystrokes to an enemy agent.
E	Any cipher except a one-time pad can be broken with enough computational effort (by brute force attack if nothing else), but the amount of effort needed to break a cipher may be exponentially dependent on the key size, as compared to the effort needed to use the cipher.
F	refers to a security breach where an attacker exploits the time when a system is less monitored or staffed, such as during lunch hours or late at night, to perform unauthorised access or attacks without detection.

CRYPTANALYSIS. CRYPTANALYSIS ATTACKS

Cryptanalysis is the practice, art, and science of defeating the methods devised by cryptography. In other words, it's the technique of accessing the plaintext content of a communication whithout the decryption key. The goal is to find some weakness that allow subversion of the cryptographic scheme.

Cryptanalysts examine ciphers, cryptosystems, and ciphertext to understand how they work and to find ways to weaken or defeat them. **1.** _____.

Malicious attackers attempt to subvert a system. This is an essential part of communications intelligence and some computer security attacks. Often the goal of the attacker is to read material that the users of the cryptosystem intend to keep secret.

It is a common misconception that any encryption method can be broken. During World War II at Bell Labs, Claude Shannon proved that the one-time pad cipher is unbreakable, provided the key material is truly random, never reused, kept secret from all possible attackers, and of equal or greater length than the message. This means that an adversary who intercepts an encrypted message has no better chance of guessing the contents than an adversary who only knows the length of the message. Even using the keys twice can lead to compromise.

2. _____. In such cases, effective security can still be achieved if some conditions (e.g., key size) are such that the effort ("work factor" in Shannon's terms) is beyond the ability of any adversary.

Cryptanalysis attacks come in many different forms:

Ciphertext-only attack assumes the cryptanalyst only has access to the ciphertext without any plaintext, making it the most common but weakest form of cryptanalysis due to limited information. Modern ciphers are designed to resist such attacks, which typically require the cryptanalyst to have some knowledge of the plaintext, such as its language, distribution, or standard patterns.

A brute force attack (or exhaustive key search) **3.** _____. Its difficulty depends solely on key length: with N bits, there are 2N keys, requiring up to 2N attempts in the worst case and about 2N-1 on average. This method is used as a benchmark for other attacks and can work in ciphertext-only scenarios if enough plaintext information (at least N bits) is available to identify the correct key.

Known-plaintext attack. In this type of attack, it is assumed that the cryptanalyst has access to at least a limited number of pairs of plaintext and the corresponding enciphered text. During World War II, the Allies used such methods, called “cribs”, to break the Enigma cipher – initially through stolen plaintext and intercepted ciphertext, but later mostly through educated guesses. These later guesses are technically ciphertext-only attacks, which are more difficult to execute.

A chosen-plaintext attack allows a cryptanalyst to select plaintexts, obtain their ciphertexts, and exploit patterns or vulnerabilities, especially since public-key systems make the encryption key publicly available, enabling attackers to generate ciphertexts for any plaintext. Therefore, public-key algorithms must defend against such attacks.

An adaptive chosen-plaintext attack is **4.** _____.

Chosen-ciphertext attack. In this attack the analyst can choose an arbitrary ciphertext and have access to plaintext decrypted from it. In a real-world case, this would require the analyst to have access to the communication channel and the recipient end.

A *Lunchtime attack* or *midnight attack* **5.** _____.

Adaptive chosen-ciphertext attack. In this attack, the analyst can choose a series of ciphertexts and see the resulting plaintexts, with the opportunity at each step to analyse the previous ciphertext-plaintext pairs before choosing the next ciphertext.

Open key model attacks. In this type of attack, the attacker has some knowledge about the key for the cipher being attacked.

A *related-key attack* is a cryptanalytic technique where the attacker analyses the encryption under multiple keys that have a known, related relationship, aiming to uncover secret information or keys by exploiting these relationships.

Known-key distinguishing attack and chosen-key distinguishing attack, where an attacker can distinguish ciphertext from random along with the knowledge or ability to choose the key.

Side-channel attack. This is not strictly speaking a cryptanalytic attack, and does not depend on the strength of the cipher. It refers to using other data about the encryption or decryption process to gain information about the message, such as electronic noise produced by encryption machines, sound produced by keystrokes as the plaintext is typed, or measuring how much time various computations take to perform.

Evil maid attack. This is also not a cryptanalytic attack. It refers to an unauthorised person such as a maid getting physical access to the encryption equipment, and modifying it to disclose the plaintext or key when it is used. **6.** _____.

Borrowed and modified from: Attack model https://en.wikipedia.org/wiki/Attack_model, Cryptanalysis https://en.citizendium.org/wiki/Cryptanalysis, all written content is available under the Creative Commons-Attribution-ShareAlike 3.0 Unported license
Modified by https://deepai.org/chat/text-generator

4. **A. & B. Read the text again. Do the following tasks.**

4.1. Fill in the missing information in statements 1–10.

1. Cryptanalysis is considered to be the practice, art, and science of _____ the methods devised by _____ .
2. Malicious attackers attempt to _____ a system.
3. Effective security can be achieved if some conditions (e.g., key size) are such that the effort is beyond the ability of any _____.

4. A brute force attack tries every possible key until the correct one is found, making all ciphers _____ except unbreakable ones like the one-time pad.
5. In a known-plaintext attack, the cryptanalyst is assumed to have access to a limited number of pairs of _____ and the corresponding _____ text.
6. In a chosen-ciphertext attack, an analyst can select an arbitrary _____ and access the plaintext that has been _____ from it.
7. In an open key model attack, the attacker knows the _____ for the cipher being attacked.
8. A _____ is not, strictly speaking, a cryptanalytic attack and does not depend on the strength of the cipher.
9. A maid with access to her employer's computer, might insert a thumb drive containing malware that installs a _____ that transmits keystrokes to an enemy agent.
10. A _____ is a cryptanalytic technique where the attacker analyses the encryption under multiple keys that have a known, related relationship, aiming to uncover secret information or keys by exploiting these relationships.

4.2. Decide whether these statements are *true* or *false*.

1. Black hat hackers use cryptanalysis for penetration testing.
2. The one-time pad cipher is breakable if the key material is reused.
3. Any cipher can be broken with enough computational effort, regardless of key size.
4. Ciphertext-only attacks assume that the cryptanalyst has access only to the ciphertext and no access to the plaintext.
5. Known-plaintext attacks were used by the Allies during World War II to cryptanalyse the Enigma machine cipher.
6. Chosen-plaintext attacks are only possible in public-key cryptosystems.

7. Adaptive chosen-plaintext attacks allow the analyst to analyse the results of previous plaintexts before choosing the next plaintext.
8. A known-key distinguishing attack can be used to distinguish ciphertext from random without knowing the key.
9. A side-channel attack is a type of cryptanalytic attack that relies on the strength of the cipher.
10. An evil maid attack is a type of cryptanalytic attack that involves modifying encryption equipment to disclose the plaintext or key.

5. **A. & B. Work with AI to give synonyms for the words in italics in the table. Provide your own synonyms in the second column, and use any AI tool to fill in the third column. After that, create two sentences using synonyms from different columns.**

Expressions	Synonyms suggested by students	Synonyms generated by AI
1) the cryptosystem intends to keep secret		
2) it is a common misconception		
3) an adversary who intercepts a message		
4) to be very resistant to this type of attack		
5) to break a cipher		
6) intercepted ciphertext		
7) to provide direct access to the plaintext		
8) to exploit vulnerabilities		

Expressions	Synonyms suggested by students	Synonyms generated by AI
9) to choose an arbitrary ciphertext		
10) temporary access		
11) to distinguish ciphertext		
12) the strength of the cipher		
13) an unauthorised person		
14) to disclose the plaintext or key		

6. **A. & B. Make a list of the five most important things that you have to remember about cryptanalysis and cryptanalysis attacks. Compare your list to your partner's. Which three are the most popular among the class?**

USE OF ENGLISH

VOCABULARY

7. **A. & B. Match the phrases with definitions.**

1	Ciphertext-only attack	**a**	the attacker can get the ciphertexts (plaintexts) which correspond to an arbitrary set of plaintexts (ciphertexts) of their own choosing
2	Known-plaintext attack	**b**	similar to a chosen-plaintext attack, except that the attacker can get ciphertexts encrypted under two different keys. The keys are not known, but the relationship between them is known
3	Chosen-plaintext attack	**c**	the cryptanalyst is only allowed to access a collection of ciphertexts

4	Adaptive chosen-plaintext attack	**d**	similar to a chosen-plaintext attack, except that the attacker can choose succeeding plaintexts on the basis of information learned from prior encryptions
5	Related-key attack	**e**	the attacker has a range of ciphertexts to which they know the relevant plaintext

IDIOMS

8. **A. Match the idioms in bold to their equivalents. Have you got any similar idioms / phrases in your language?**

The most vulnerable point in a security system, to decipher hidden meanings, easily understood, to keep secret, the ongoing struggle, to reveal confidential information, forefront.

1. The hackers managed to **spill the beans** on the organisation's sensitive data through a sophisticated cryptanalysis attack.
2. Many secure systems are designed to keep data **under lock and key**.
3. Skilled cryptanalysts can sometimes **read between the lines** to find weaknesses.
4. In some cases, the methods used in contemporary cryptography appear to be **an open book** to those who know where to look.
5. As technology advances, tools and techniques for cryptanalysis remain on the **cutting edge**, constantly challenging established protocols.
6. Unfortunately, even the most secure systems can have **the weakest link**, often found in human factors such as poor password management.
7. As a result, the battle between cryptographers and hackers becomes a game of **playing cat and mouse**, with each side adapting to outsmart the other.

B. Fill in the blanks using the idioms from the list below. You may need to change the verb tense.

Spill the beans, under lock and key, read between the lines, an open book, cutting edge, the weakest link, playing cat and mouse.

In the highly competitive world of cryptanalysis, the battle between code-makers and code-breakers is a perpetual game of **1)** _____. On one side, engineers develop **2)** _____ encryption algorithms designed to keep state secrets **3)** _____, buried beneath layers of complex mathematical functions. They operate under the assumption that their math is airtight, but a seasoned cryptanalyst knows that the algorithm itself is rarely the problem.

Instead, they look for **4)** _____ in the security chain – which is almost always the human element. An analyst doesn't just look at the raw data; they **5)** _____ of communication metadata to find patterns in timing or frequency. If a tired operator makes a mistake or a disgruntled employee decides to **6)** _____ to a journalist, the most "unbreakable" system can suddenly become **7)** _____ to those who know how to interpret the fragments.

Borrowed and modified from: https://gemini.google.com/

GRAMMAR

9. **A. & B. Put the verbs into the correct past tense.**

1. The cryptanalysts _____ **(discover)** a flaw in the encryption algorithm last year.
2. While they _____ **(analyse)** the ciphertext, they _____ **(realise)** that the substitution method had been poorly implemented.
3. The experts _____ **(work)** on breaking the code for months before they finally succeeded.

4. The attackers carried out their plan just as the organisation _____ **(enhance)** its security measures.
5. They _____ **(compromise)** already several systems before the IT department _____ **(detect)** the intrusion.
6. The cryptographer _____ **(complete)** his report on the vulnerabilities of the algorithm before the security conference _____ **(start)**.
7. By the time the meeting _____ **(start)**, the analysts _____ **(share)** their findings with the team.
8. While the attackers _____ **(plan)** their next move, the victim organisation _____ **(upgrade)** its defences.
9. Before implementing the new security protocols, the cryptanalysts _____ **(conduct)** already several tests.
10. The team _____ **(test)** different decryption techniques when they _____ **(come)** up with a breakthrough method.

A. Choose the correct answer.

A cryptosystem which is Vigen`ere where there are **1)** _____ **(as many keys as / as much keys as)** letters in the cleartext is called a one-time pad cryptosystem, and the pad in this cryptosystem is the name **2)** _____ **(to use / used)** for the collection of all of those Vigen`ere keys.

It is a very important thing when **3)** _____ **(using / used)** a one-time pad never to reuse the pad – that's why it's called a one-time pad – **4)** _____ **(because / because of)** if Eve guesses that the pad **5)** _____ **(has reused / has been reused)**, she can crack all of the messages which **6)** _____ **(sent / were sent)** with that pad. We will not discuss here how that attack **7)** _____ **(in / on)** encryption with a reused one-time pad **8)** _____ **(work / works)**, but suffice it to say that the attack is based, again, on frequency analysis.

One final note about one-time pads: **9) _____ (typically / typical)**, when using a one-time pad, the keys **10) _____ (are picked / picked)** purely randomly. The advantage of doing that is that there is no way Eve can predict what the keys in the pad might be, even if she **11) _____ (will know / knows)** Alice and Bob very well. With a randomly **12) _____ (choosing / chosen)** one-time pad, this cryptosystem is called information **13) _____ (theoretical / theoretically)** secure, meaning that is secure no matter **14) _____ (how many / how much)** computation power Eve can throw at the problem.

Borrowed and modified from: OpenWorkbook of Cryptology. A project-based introduction to crypto in Python. This work under a Creative Commons Attribution-ShareAlike 4.0 International license.

B. Put the words into the correct form.

The attack on the Caesar cipher which we discussed **1) _____ (was based / based / basing)** on *frequency analysis*. There is actually some interesting history here: As was mentioned above, the Caesar cipher **2) _____ (used / was used / uses)** by Julius and his nephew in **3) _____ (a / the / ---)** first century BCE. The approach of frequency analysis was first described **4) _____ (near / nearest / nearly)** a thousand years later, in a book *Manuscript on* **5) _____ (Deciphering / Decipher Deciphered)** *Cryptographic Messages* by the Muslim philosopher, mathematician, physician, and general polymath Al-Kindi. Like the mathematician and astronomer Al-Khwarizmi, Al-Kindi worked at one of the **6) _____ (great / greater / greatest)** centers of scholarship in the world in the 8th century CE, the House of Wisdom in Bagdad under the Abbasid Caliphate. Al-Kindi and Al-Khwarizmi seem to have both been involved in **7) _____ (brought / bring / bringing)** an Indian system for writing numbers **8) _____ (using / used / to use)** positional notation to **9) _____ (--- / an / the)** Arab world. This notation

later spread to Christian Europe in the early 13th century through a book called Liber Abaci **10) _____ (to write / writing / written)** by a man Leonardo of Pisa ... whom we know today as Fibonacci. Some have claimed that Fibonacci's notation helped bring about the Renaissance in Europe, since without good numerical notation, it would have been very hard to do double-entry bookkeeping, which **11) _____ (use / used / was used)** by great trading houses like the Medici, who then had the funds **12) _____ (support / to support / supporting)** the tremendous flowering of the arts which **13) _____ (were / was / is)** the Renaissance...

Borrowed and modified from OpenWorkbook of Cryptology. A project-based introduction to crypto in Python. This work under a Creative Commons Attribution-ShareAlike 4.0 International license

10. A. Choose the correct option.

1. The cryptanalyst _____ the encrypted message since 8 p.m.
    a) has been analysing
    b) were analysing
    c) had analysed
2. By using frequency analysis, the cryptanalyst _____ the most common letter in the encryption two hours ago.
    a) finds
    b) found
    c) will find
3. The encryption algorithm is so secure that only the best cryptanalyst _____ to crack it.
    a) can
    b) was able
    c) could

4. Before starting the decryption process, the team _____ all the possible keys.
    a) had examined
    b) examines
    c) examine
5. By the time we cracked the code, we _____ all the available data.
    a) already analysed
    b) were already analysing
    c) had already analysed
6. The cryptanalyst _____ to solve the puzzle at 7 o'clock yesterday.
    a) tried
    b) had been trying
    c) was trying
7. The encrypted message _____ in a way that made it difficult to decipher.
    a) was encoded
    b) encoded
    c) encodes
8. He _____ as a cryptanalyst for 5 years before he retired.
    a) worked
    b) had been working
    c) was working
9. The decryption process _____ several hours to complete yesterday.
    a) took
    b) takes
    c) taking
10. By the time we _____ the code, we _____ on it for three hours without a break.
    a) crack, had been working
    b) cracked, had been working
    c) cracked, were working

B. Complete the sentences using the words in bold. Use two to five words.

1. It was the first time the team had broken a code.

   never The team _____ a code before.

2. This text needs to be encrypted as soon as possible.

   encrypting This text needs _____ as soon as possible.

3. He had never seen such a complex encryption before.

   first It _____ he had ever seen such a complex encryption before.

4. When did the Caesar cipher become a well-known example of a simple substitution cipher?

   ago How long _____ a well-known example of a simple substitution cipher?

5. It was the first time they had attempted to break a 256-bit key.

   never They _____ to break a 256-bit key before.

6. The professor made us study the intricacies of cryptographic protocols.

   made We _____ the intricacies of cryptographic protocols.

7. They haven't finished cracking the encryption yet.

   still They _____ the encryption.

8. Using different encryption techniques for the same dataset without permission from the cryptography team is not allowed.

   use Nobody _____ different encryption techniques for the same dataset without explicit permission from the cryptography team.

9. The complexity of the encryption algorithm is so high to crack it without a massive computational power and advanced cryptanalysis techniques.

   too The complexity of the encryption algorithm is _____ to crack it without a massive computational power and advanced cryptanalysis techniques.

10. Alisa hasn't finished decrypting the message yet.

still Alisa _____ the message.

LISTENING

You are going to watch a video about cryptanalysis.

11. A. & B. Before watching a video, check if you know the meaning of the words. Use Merriam-Webster Dictionary if necessary.

Weaknesses, cipher, substitution, frequency, to identify, ciphertext, hacking, distribution, to infer.

12. Watch the video "What is cryptanalysis?".

Answer the questions.

1. What is the goal of cryptanalysis, according to the text?
2. What type of substitution cipher is used in the example mentioned in the text?
3. What technique is used to identify patterns in the ciphertext in order to infer the key?
4. What is the most common letter in the English language, according to the text?
5. What is the plain text message that was revealed through cryptanalysis in the example?

13. A. & B. Watch the video again and do the following tasks.

13.1. Fill in the missing information in statements 1–5.

1. Cryptanalysis is the process of analysing and decrypting _____ without knowing the key or the algorithm used to encrypt the message.
2. The main goal of cryptanalysis is to find _____ systems.

3. A Caesar Cipher is a type of _____ where each letter in the plain text is shifted _____ of positions down the alphabet.
4. Frequency analysis involves analysing the _____ of letters in the cipher text.
5. The plain text message is "_____".

13.2. Decide whether these statements are *true or false*.

1. Cryptanalysis involves decrypting messages without the need for the encryption key or algorithm.
2. The goal of cryptanalysis is to strengthen cryptographic systems by identifying their weaknesses.
3. A Caesar Cipher is a type of substitution cipher that shifts letters a fixed number of positions in the alphabet.
4. In the example, the letter "E" is suggested to correspond to the letter "L" in the ciphertext.
5. The plain text message revealed at the end of the example is "ethical hacking".

SPEAKING

14. A. Work in pairs. In your ESP class, you'll explore the differences between Linear Cryptanalysis and Differential Cryptanalysis. Conduct research online to understand both concepts, and then create a dialogue.

You may use this link: https://www.geeksforgeeks.org/differential-and-linear-cryptanalysis/

Your dialogue should include at least 5–6 exchanges per each participant. Be creative! Remember to keep the tone respectful!

A	B
1. I'm having trouble understanding the difference between linear cryptanalysis and differential cryptanalysis. Can you explain it to me?	1. Sure thing! Linear cryptanalysis is a type of attack that involves finding a linear relationship between the plaintext and ciphertext bits.
2. …….	2. …….
3. …….	3. …….
4. …….	4. ……
5. …….	5. ……
6. …….	6. …….

B. Work in pairs. Act out a dialogue about cryptanalysis attacks. Your dialogue should include at least 7–8 exchanges per each participant. Be creative! Remember to keep the tone respectful!

15. **A. You are asked to choose one of the topics and prepare a brief talk about one of the topics. Use information from the text.**

1. What is cryptanalysis?
2. Who uses cryptanalysis?
3. Cryptanalysis attacks.
4. Cryptanalysis tools.
5. Forms of cryptanalysis.
6. The cryptanalyst's requirements and responsibilities.

B. You are asked to prepare a presentation on one of the topics.

1. Linear cryptanalysis: theory and applications

- the basics of linear cryptanalysis;
- historical context and significance of linear cryptanalysis;
- examples of attacks using linear cryptanalysis;
- countermeasures against linear cryptanalysis.

2. **Differential cryptanalysis: a powerful attack on block ciphers**
   - introduction to differential cryptanalysis and its history;
   - the basics of differential cryptanalysis (finding differentials, using them to attack the cipher);
   - examples of attacks using differential cryptanalysis;
   - countermeasures against differential cryptanalysis.
3. **Cryptanalytic tools and techniques**
   - overview of popular cryptanalytic tools and software;
   - basic techniques for performing cryptanalysis (e.g. frequency analysis, differential analysis);
   - advanced techniques for performing cryptanalysis.
4. **Quantum cryptanalysis: threats and mitigations**
   - introduction to quantum computing and its implications for cryptography;
   - the basics of quantum cryptanalysis;
   - examples of quantum attacks on classical cryptographic algorithms;
   - mitigations against quantum attacks.
5. **Difference between frequency analysis and differential cryptanalysis**
   - overview of cryptanalysis and its importance in cryptography; definition of frequency analysis and differential cryptanalysis;
   - frequency analysis (explanation of how frequency analysis works; limitations);
   - differential cryptanalysis (explanation of how differential cryptanalysis works; the limitations of differential cryptanalysis);
   - comparison of frequency and differential cryptanalysis.

WRITING

16. **A. For the research, you need to write a summary (160–180 words) of the text "What is cryptanalysis?"**

Use the link: https://www.youtube.com/watch?v=PAylKVVSW-0.

17. **B. For your research, you need to write a summary (180–200 words) of the text "The science of codes: an intro to cryptography."**

Use the link: https://www.youtube.com/watch?v=-yFZGF8FHSg.

REFLECTION AND SYNTHESIS

18. **You have completed this unit. This word cloud can help you to reflect on and synthesise the key concepts from the topic. Focus on the most important terms and ideas that stood out to you. Using the word cloud as a visual tool, you have to illustrate your understanding.**

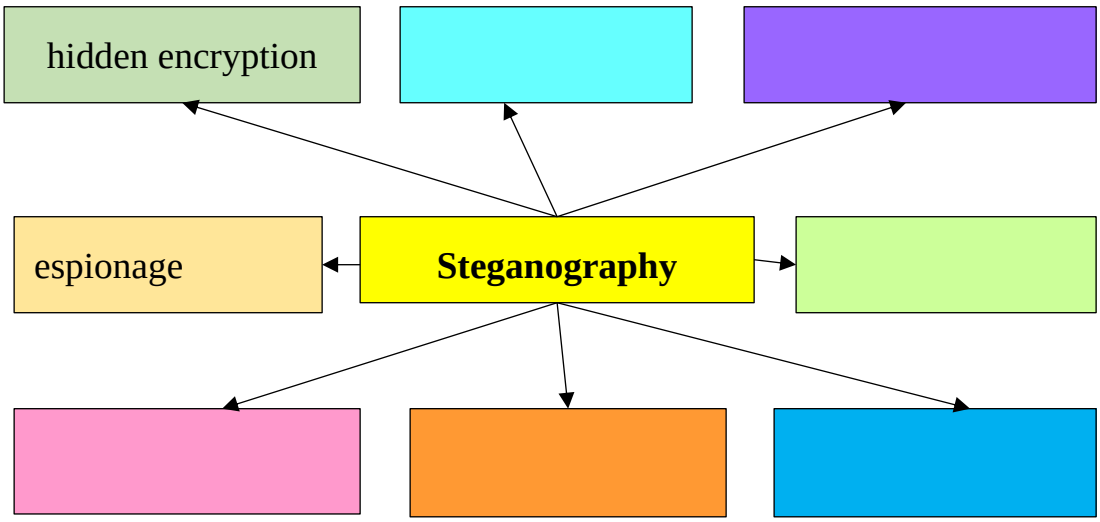
2.3. STEGANOGRAPHY

WARM UP

1. A. & B. Using your background knowledge, do the tasks according to your learning style (dominant or non-dominant modality).

1.1. *Visual Modality*

Work individually, then in small groups. Create a mind map with a central concept "Steganography". Start by brainstorming relevant terms related to steganography. Clearly illustrate how each term relates to the central theme.



1.2. *Auditory Modality*

Answer the questions.

1. What is steganography?
2. What is the aim of steganography?
3. What types of steganography do you know?
4. How does steganography work?
5. Who uses steganography?
6. What steganography tools do you know?

1.3. *Kinesthetic Modality*

Complete the table answering the question:

What advantages and disadvantages of steganography do you know? Then comment on the information in the table.

Advantages of steganography	Disadvantages of steganography
1. ***Secrecy:*** Steganography can be used to hide secret information in a way that is not easily detectable, making it a secure method for sharing confidential data.	1. ……
2. ……..	2. …….
3. …….....	3. …….
4. ……..	4. …….
5. ……	5. …….

READING

You are going to read an article about steganography.

2.

1. A. & B. Before reading, discuss the following statement.

Steganography can be considered as a double-edged sword.

2. A. & B. Before reading, look at the following words and phrases, which have been taken from the text. In what context might they be mentioned? Use Merriam-Webster Dictionary if necessary.

Inspection, concealed, analogous, conventional, payload, encoding density, unbreakable, innocuous, regrown, reusable, hidden, ciphertext, random data, modifying, available information, initial conductive target.

3. **Read the text about steganography. Five paragraphs have been removed. Choose which of the paragraphs fit into the gaps.**

A	The *payload* is the data covertly communicated. The *carrier* is the signal, stream, or data file that hides the payload, which differs from the channel, which typically means the type of input, such as a JPEG image. The resulting signal, stream, or data file with the encoded payload is sometimes called the *package*, *stego file*, or *covert message*. The proportion of bytes, samples, or other signal elements modified to encode the payload is called the *encoding density* and is typically expressed as a number between 0 and 1.
B	*Passive steganalysis*: does not alter the target stego, therefore, it examines the target stego in order to establish whether it carries hidden information and recovers the hidden message, the key used or both.
C	In communities with social or government taboos or censorship, people use *cultural or social steganography* – hiding messages in idiom, pop culture references, and other messages they share publicly and assume are monitored. This relies on social context to make the underlying messages visible only to certain readers. Examples include: hiding a message in the title and context of a shared video or image; misspelling names or words that are popular in the media in a given week, to suggest an alternate meaning; hiding a picture that can be traced by using Paint or any other drawing tool.
D	Encrypted messages, even if unbreakable, can arouse suspicion and be incriminating where encryption is illegal. While cryptography protects message contents, steganography conceals both the existence and content of the message.
E	Examples of this include changing pixels in image or sound files, properties of digital text such as spacing and font choice, Chaffing and winnowing, Mimic functions, modifying the echo of a sound file and including data in ignored sections of a file.

STEGANOGRAPHY

Steganography is the practice of hiding information within another message or object so that its presence is not obvious, often used in digital files, images, or videos. The term comes from Greek, meaning "*covered writing*", combining "*steganós*" (covered) and "*-graphia*" (writing).

Steganography uses terminology similar to radio and communication technology, but some terms specific to software can be confusing. Here are the most relevant ones for digital steganographic systems. **1. _____**

In a set of files, the files that are considered likely to contain a payload are *suspects*. A suspect identified through some type of statistical analysis can be referred to as a *candidate*.

Steganography and cryptography both hide sensitive information, but steganography has the advantage of not attracting attention, since the secret message itself isn't obvious. **2. _____**.

Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program, or protocol. Media files are ideal for steganographic transmission because of their large size. For example, a sender might subtly modify every hundredth pixel's color in an image to encode letters, changes so slight that they are unlikely to be noticed without specific inspection.

The earliest known uses of steganography date back to 440 BC in Greece, as noted by Herodotus, who described Herodotus shaving a servant's head to hide a message, and Demaratus writing on a wax tablet's backing to warn of an attack. Later, Johannes Trithemius in his Polygraphiae created the "Ave-Maria-Cipher", hiding information within Latin praise, such as concealing the word VICIPEDIA.

Steganography techniques. Numerous techniques throughout history have been developed to embed a message within another medium.

Physical steganography is the use of a physical medium to carry the secret, hidden message. It has been widely used for centuries. Some notable examples include: invisible ink on paper, writing a message in Morse code on yarn worn by a courier, microdots, or using a music cipher to hide messages as musical notes in sheet music.

3. _____

Since the dawn of computers, techniques have been developed to embed messages in digital cover mediums (*digital or electronic steganography*). The message to conceal is often encrypted, then used to overwrite part of a much larger block of encrypted data or a block of random data (an unbreakable cipher like the one-time pad generates ciphertexts that look perfectly random without the private key).

4. _____

Digital steganography output may be in the form of printed documents. A message, the plaintext, may be first encrypted by traditional means, producing a ciphertext. Then, an innocuous cover text is modified in some way so as to contain the ciphertext, resulting in the stegotext. For example, the letter size, spacing, typeface, or other characteristics of a cover text can be manipulated to carry the hidden message. Only a recipient who knows the technique used can recover the message and then decrypt it. Francis Bacon developed Bacon's cipher as such a technique.

Steganalysis. Stegoanalytical algorithms can be cataloged in different ways, highlighting: according to the available information and according to the purpose sought.

➢ *According to the information available.*

There is the possibility of cataloging these algorithms based on the information held by the stegoanalyst in terms of clear and encrypted messages. It is a technique similar to cryptography, however, they have several differences:

− chosen stego attack: the stegoanalyst perceives the final target stego and the steganographic algorithm used;

− known cover attack: the stegoanalyst comprises the initial conductive target and the final target stego;

− known stego attack: the stegoanalyst knows the initial carrier target and the final target stego, in addition to the algorithm used;

− stego only attack: the stegoanalyst perceives exclusively the stego target;

− chosen message attack: the stegoanalyst, following a message selected by him, originates a stego target;

− known message attack: the stegoanalyst owns the stego target and the hidden message, which is known to him.

➢ *According to the purpose sought.*

The principal purpose of steganography is to transfer information unnoticed, however, it is possible for an attacker to have two different pretensions: **5.** _____. *Active steganalysis*: changes the initial stego target, therefore, it seeks to suppress the transfer of information, if it exists.

Borrowed and modified from: Steganography https://en.wikipedia.org/wiki/Steganography, Steganography https://en.citizendium.org/wiki/Steganography
Modified by https://deepai.org/chat/text-generator

4. A. & B. Read the text again and do the following tasks.

4.1. Fill in the missing information in statements 1–8.

1. The resulting signal, stream, or data file with the _____ is sometimes called the _____, stego file, or covert message.
2. Steganography and cryptography are both techniques used to conceal _____ information.
3. Steganography offers the benefit of avoiding detection because the _____ _____ itself remains concealed and not easily noticeable, unlike _____.
4. Steganography is the _____ of information within computer files.
5. Demaratus sent a warning about a forthcoming attack to Greece by writing it directly on the wooden _____ of a wax tablet before applying its beeswax surface.
6. Cultural steganography means _____ in idiom, pop culture references, and other messages people share publicly and assume are monitored.
7. _____: the stegoanalyst, following a message selected by him, originates a stego target.
8. _____: changes the initial stego target, therefore, it seeks to suppress the transfer of information, if it exists.

4.2. Decide whether these sentences are *true or false*.

1. Steganographic techniques are used to conceal information within another message or physical object so that it can be detected by humans.
2. The term “payload” refers to the signal or data file that hides the encoded information.

3. Steganography is concerned with protecting the contents of a message alone.
4. The first recorded use of steganography dates back to ancient Greece.
5. One of the notable examples of physical steganography is invisible ink on paper.
6. The example of social steganography is hiding messages as musical notes in sheet music.
7. Digital steganography is the process of embedding messages in digital cover mediums.
8. Active steganalysis changes the target stego to conceal information.

4.3. Answer the questions.

1. What is steganography, according to the text?
2. What is the advantage of steganography over cryptography alone, according to the text?
3. Who is credited with the first recorded use of steganography in ancient Greece, according to the passage?
4. What is physical, social and digital steganography? Can you give some examples?
5. What are the specifics of stego-analytical algorithms according to the information available?
6. What are the specifics of stego-analytical algorithms according to the purpose sought?

5. **A. & B. In pairs, select one word from the provided list. Student A asks the questions below, putting the chosen word into each question, while Student B responds using that word. You may skip any questions that do not apply. After completing the questions, switch roles and repeat the activity with a different word. See the example below.**

Carrier, channel, density, suspect, message, attack, data, steganalysis, digital, alternate, payload, visible, encrypted, subtle.

1. What does _____ mean?
2. What is the plural / singular of _____?
3. What is the synonym of _____?
4. What is the opposite of _____?
5. What is the noun for _____?
6. What is the verb for _____?
7. What is the adjective for _____?
8. What is the adverb for _____?
9. Can you give _____ collocations?
10. How to use _____ in a sentence?
11. What is the translation for _____?

For example:

The chosen word is "project".

Student A: "What does project mean?"

Student B: "Project" is a planned set of activities or tasks intended to achieve a specific goal.

Student A: "What is the plural of project?"

Student B: "Projects."

6. **A. & B. Make a list of the five most important things that you have to remember about steganography. Compare your list to your partner's. Which three are the most popular among the class?**

USE OF ENGLISH

VOCABULARY

7. 1. A. & B. Match the words / phrases with their meaning.

1	steganography	**a**	hidden message
2	payload	**b**	coding density
3	carrier	**c**	a technique for hiding secret information within a non-secret message or other medium, in order to conceal the presence and content of the hidden information
4	covert message	**d**	indestructible
5	encoding density	**e**	to conceal
6	to hide	**f**	the covertly transmitted data
7	unbreakable	**g**	grown again
8	regrown	**h**	the signal, the stream or the data file in which the payload is hidden
9	reusable	**i**	a suspect identified by some statistical analysis
10	invisible	**j**	a form of steganography that uses digital media to hide secret information by embedding it in the digital carrier medium
11	social steganography	**k**	recyclable
12	electronic steganography	**l**	a form of steganography that uses social media platforms, online communities, and other digital communication channels to hide secret information in seemingly innocent social posts

2. A. & B. Complete the sentences. Use: *cryptography (2), hiding, steganography (2), encrypting, medium, sensitive, visible, unauthorised, embedding, algorithms*.

Steganography and cryptography are both techniques used to hide **1)** _____ information, but they are different in their approach. **2)** _____ is the practice of **3)** _____ information in order to make it unreadable to **4)** _____ parties, usually through the use of **5)** _____ and keys. **6)** _____, by contrast, is the practice of **7)** _____ the existence of the information itself by **8)** _____ it in another **9)** _____, such as an image or audio file, in a form that is not immediately **10)** _____. In other words, **11)** _____ deals with the protection of the secrecy of the message, while **12)** _____ deals with the concealment of the fact that a message exists at all.

PHRASAL VERBS

8. **A. Fill in the correct particles. Then explain the phrasal verbs. See Appendix 2, which contains a list of relevant phrasal verbs.**

1. The new steganographic algorithm **differs** _____ the old one in the use of more complex encryption techniques.
2. To enhance security, we need to **do** _____ any outdated steganography methods that are easy to detect.
3. When our latest approach faced problems, we had to **fall** _____ the conventional steganography techniques that were proven to work.
4. The main challenge was to **get** _____ the basic concepts of steganography to the audience without making the audience feel overwhelmed.
5. The researchers decided to **do** _____ the existing steganography software to use stronger encryption algorithms.

6. The different steganographic techniques can **fall** _____ categories based on the medium used, such as images or audio files.
7. The sophisticated use of algorithms allowed the developers to **get** _____ detection methods that aimed simpler steganography techniques.
8. After several vulnerabilities were identified, the team needed to **do** _____ the entire steganographic system to guarantee its integrity.

B. Replace the words or phrases in bold with the correct form of a phrasal verb using *differ, do,* and *get*. Then, create three interconnected sentences that include any phrasal verbs with "differ", "do" and "get".

1. The method of hiding messages in images can be **distinct** in some way from traditional encryption techniques.
2. Some experts believe that we need to **eliminate** old approaches to data privacy and instead adopt modern steganographic methods instead.
3. After realising the hidden message was corrupted, the expert had to **repeat** the encoding process using a different image.
4. He tried to fasten or secure his computer's software to include **advanced** steganography tools.
5. In times of heightened surveillance, many privacy-conscious individuals choose to **turn to** steganography as a covert method to protect their confidential messages.
6. Many people **are under** the misconception that steganography alone provides complete security.
7. The tutorial aims **to successfully communicate** the importance of using steganography to protect sensitive information.
8. Experts are continually working on ways to **bypass** the limitations of current steganographic techniques to enhance data protection.

GRAMMAR

9. **A. & B. Put the verbs into the correct past tense.**

Last year, two friends, Jake and Jane, who **1) _____ (to be)** both steganographers, **2) _____ (to work)** diligently in their university lab on a difficult project. Their task, which proved more complicated than they **3) _____ (to expect)**, **4) _____ (to be)** to develop a technique for hiding data within images. They **5) _____ (to experiment)** with various methods. While Jake **6) _____ (to analyse)** the properties of digital images, Jane **7) _____ (to research)** existing algorithms to find innovative solutions. After weeks of hard work and countless late nights, they finally **8) _____ (to come)** up with a promising approach that involved subtle changes to pixel values.

Before they **8) _____ (to realise)** it, time **9) _____ (to fly)**. The project deadline **10) _____ (to approach)**. They **11) _____ (to approach)** closely for months, sharing ideas and building on each other's strengths. By the time they **12) _____ (to complete)** the project, they **13) _____ (to improve)** the technique, ensuring that the hidden data remained undetectable. On the day of their presentation, they **14) _____ (to feel)** a mix of nervousness and excitement. As they presented their breakthrough work, they **15) _____ (to reflect)** on how much they **16) _____ (to learn)** and **17) _____ (to grow)** together. Their successful project not only strengthened their friendship, but also **18) _____ (to help)** set the foundation for future innovations in the field of steganography.

A. Choose the appropriate option.

1. Stego version of images **(may have / has to have)** different grades of visual and statistical undetectability due to their different contents.
2. A steganography method can employ a technique to embed in a cover image until it **(not attracts / does not attract)** the attention of steganalysis methods

and makes steganalysers misclassify the observed stego image as a cover (clean) image.

3. For steganographic systems, the major requirement is that the stego object **(is to / should be)** perceptually and statistically indistinguishable to the degree that it does not raise suspicion.
4. Since the communication channel is limited, we prefer to have the **(lower / lowest)** number of images in the stego image set to occupy the communication channel less.
5. Batch steganography **(is meaning / means)** hiding the secret data into multiple cover objects.
6. If the number of cover images is low and the total capacity of cover images is not enough **(to conceal / conceal)** the secret data, then each resulted stego image is overloaded, and its security would be low.
7. If the number of cover images is high, with **(spreading / spread)** the secret data equally between cover images, then the security of stego images is high but the communication channel will be occupied a lot.
8. **(Considered / Considering)** steganography capacity of an image, we can embed in the image a portion of secret data that its size is less or equal to the steganography capacity of the image.
9. The remaining **(unconcealed / unconcealing)** portion of secret data can be hidden in some other cover images.
10. An image histogram is **(a / the)** type of histogram acting as a graphical representation of the tonal distribution in a digital image.

Borrowed and modified from: Hedieh Sajedi "Recent Advances in Steganography", https://www.intechopen.com/books/2092

B. Put the words into the correct form.

1. The stego images that _____ **(produce)** by using such data hiding techniques are inherently robust against main geometrical attacks such as rotation, scattered tiles and warping, as well as other main attacks.
2. _____ **(Use)** data hiding techniques in secret communication purposes has been well proved to be promising.
3. The term "steganography" _____ **(state)** the disguise of secret / critical digital information within computer files.
4. For example, a sender might start with an ordinary _____ **(look)** digital image file, and then adjust the colour of every 10th pixel to correspond to a letter in the alphabet.
5. First of all, stego images and their histograms _____ **(can, not, detect)** by the HVS.
6. Secondly, data hiding capacity is _____ **(comparative, high)** than the other methods.
7. Its algorithm _____ **(can, apply)** easily because it is too simple.
8. The LSB replacement technique _____ **(know)** as one of the simplest steganography technique.
9. Most of the practical cases _____ **(meeting)** this condition when the amplitude modification level is small enough.
10. The amplitude modification may cause undesirable _____ **(clip)** in the 8 bit compression data, if its magnitude _____ **(exceed)** *127-j*.

Borrowed and modified from: Hedieh Sajedi "Recent Advances in Steganography", https://www.intechopen.com/books/2092

10. **Correct the mistakes.**

A. The underlined parts of the sentences may contain mistakes. Some underlined parts are correct. Write out parts that contain a mistake and correct it.

1. (a) **A** pixel or picture element is the **(b)** **smaller** item of information in a digital image (object) that **(c)** **is represented** by a series of X rows and Y columns.

2. Pixels are **(a)** **normally** arranged in a two-**(b)** **dimensionals grid** and are often signified **(c)** **using** tiny dots, squares, rectangles etc.

3. Each pixel **(a)** **are** the smallest sample of **(b)** **an** original image (object), where more samples naturally provide more accurate and **(c)** **better** demonstrations of the original.

4. The intensity **(a)** **of** each pixel **(b)** **is** **(c)** **typical** variable.

5. Digital **(a)** **images** are commonly **(b)** **saving** in a grayscale mode **(c)** **in** computer systems.

6. The number of bits in order **(a)** **to** represent each pixel **(b)** **establishes** how many colours or shades of grey are allowed to **(c)** **displayed**.

Borrowed and modified from: Hedieh Sajedi "Recent Advances in Steganography"
https://www.intechopen.com/books/2092

B. There is an odd word in some of the lines. Find it and write in the space provided.

Network steganography is a technique used to hide secret information	1 √
in a network by embedding it in innocent-looking data, when	2
such as images, audio files or text messages. This technique is being	3
designed to avoid detection in by security systems and remain	4
having undiscovered by network intrusion detection systems.	5

In a network steganography attack, the attacker embeds the secret	6
of information in a cover file. The cover file is then transmitted over	7
the network and along with the hidden data. Using an appropriate	8
the extraction key or algorithm, the recipient can then extract the	9
hidden message. Network steganography can be used for a variety of	10
purposes. These include data with exfiltration, unauthorised access	11
and malware of distribution.	12

LISTENING

You are going to watch a video that explores the specifics of steganography.

11. A. & B. Before watching a video, check if you know the meaning of the words / phrases. Use Merriam-Webster Dictionary if necessary.

Ordinary-looking files, scrambling, swapping, backmasking, identical, retrieved.

12. Watch the video "How to Hide Data Inside Images (Steganography)". Then answer the questions.

1. What is steganography used for, according to the text?
2. How is steganography different from cryptography?
3. What is text steganography?
4. What is image steganography?
5. What are some common methods used in image steganography?
6. What is audio steganography?
7. What is network steganography?
8. Can steganography be used for both good and bad purposes?

13. A. & B. Watch the video again and do the tasks.

13.1. Decide whether these sentences are true or false.

1. You can hide passwords, codes, or IP addresses in steganography files.
2. LSB technique hides data in the most significant bit of each pixel in an image.
3. Steganography is only used for hiding text information.
4. Masking and filtering are used for hiding data in audio files.
5. Backmasking is a method used in image steganography.
6. Network steganography involves hiding messages in network traffic.
7. Steghide is a tool that uses the least significant bit technique to hide data in images.
8. Steganography can only be used for good and bad purposes.

13.2. Fill in the missing information in statements 1–8.

1. You can hide things like passwords, codes, or _____ _____ in these files.
2. Steganography and cryptography are used together for extra _____ .
3. _____ _____ is about hiding secret messages or data inside digital images.
4. _____ and _____ method allows you to manipulate the image's colour values to hide the data.
5. _____ and _____ transformation uses mathematical transformations to embed the data in the image.
6. _____ _____ involves hiding messages in network traffic.
7. The _____ the bit depth and resolution, the _____ data you can hide.
8. Steganography can be used for _____ and _____ purposes.

SPEAKING

14. **A. Work in pairs. In your ESP class, discuss the five types of steganography. Conduct online research to gather some information about each type. Use information from the table. Based on your findings, create a dialogue that includes at least 5–6 exchanges per each participant. Be creative! Remember to keep the tone respectful!**

A	B
1. Have you heard about steganography?	1. Yes, isn't that hiding secret messages in images or something?
2. Exactly! There are many types of steganography. Let's start with text steganography. You can hide a message within a text document by using techniques like repeating certain words or using special characters.	2. Ok. What about image steganography?
3. …….	3. …….
4. …….	4. ……
5. …….	5. ……
6. …….	6. …….
7. …….	7. …….

B. In pairs, for your ESP class, create a dialogue about steganography. Your conversation should cover the following points: how steganography works, examples of steganographic techniques, and how malicious hackers use steganography for malicious purposes. Then role play it. Your dialogue should include at least 7–8 exchanges per each participant. Be creative! Remember to keep the tone respectful!

15. **A. You are asked to choose one specific issue related to steganography. Then prepare a brief talk. Use information from the text.**

1. What is steganography? What are the purposes of steganography? Who deals with steganography?
2. History of steganography.
3. Physical and electronic steganography.

B. You are asked to prepare a presentation on one of the topics. Follow the structure: introduction, main body, conclusions.

1. Steganography vs. cryptography.
2. Steganography software.
3. Steganalysis.
4. Countermeasures and detection of steganography.

WRITING

16. **A. & B. Read the for and against essay "The advantages and disadvantages of steganography" created by AI.**

1. **Identify clues in the text that it was created by artificial intelligence.**
2. **Outline the features that work for and against essays.**
3. **Highlight words and phrases that could be expressed in simpler terms.**
4. **Rewrite the essay in a simpler and more accessible way.**

"Steganography, the practice of concealing messages within other non-secret texts or media, offers notable advantages and disadvantages. On the one hand, it provides a robust means of securing sensitive information. By hiding data within seemingly innocuous files, individuals can protect their communications from unauthorised access, ensuring privacy and confidentiality. This is particularly valuable for whistleblowers and journalists who must safeguard their sources while exposing corruption or wrongdoing.

Conversely, steganography presents significant risks. Its very nature can be exploited for malicious purposes, such as concealing illicit activities or distributing harmful content, making it a tool for criminals. This dual-use nature complicates law enforcement efforts, as detecting hidden messages can be challenging. Furthermore, reliance on steganography does not eliminate the need for robust security measures; if the medium is compromised, the hidden data could still be exposed.

In conclusion, while steganography provides an effective way to protect information privacy, it also raises ethical concerns and risks associated with misuse. Thus, careful consideration is necessary when weighing its application in both personal and professional contexts."

AI Text Generator, https://deepai.org/chat/text-generator

17. **A. You take part in the Essay Contest. Write a "for and against essay" of 150–160 words. Choose one of the topics and structure your essay clearly with the following components: introduction, main body, conclusions.**

1. The role of steganography in national security (argue for its use in secure communications while discussing the potential for evasion of law enforcement).
2. The use of steganography in art: innovation or deception (assess the creative potential against the risk of fraudulent practices in digital media).

B. You take part in the *Essay Contest*. Write a "for and against essay" of 180–200 words. Choose one of the topics and and structure your essay clearly with the following components: introduction, main body, conclusions.

1. The ethical implications of steganography in digital communication (explore the benefits of privacy versus the risks of misuse for illegal activities).
2. Steganography vs. encryption (explore the advantages of covert communication against the perceived vulnerabilities of steganographic methods).

REFLECTION AND SYNTHESIS

18. **You have completed this unit. This word cloud can help you to reflect on and synthesise the key concepts from the topic. Focus on the most important terms and ideas that stood out to you. Using the word cloud as a visual tool, you have to illustrate your understanding.**

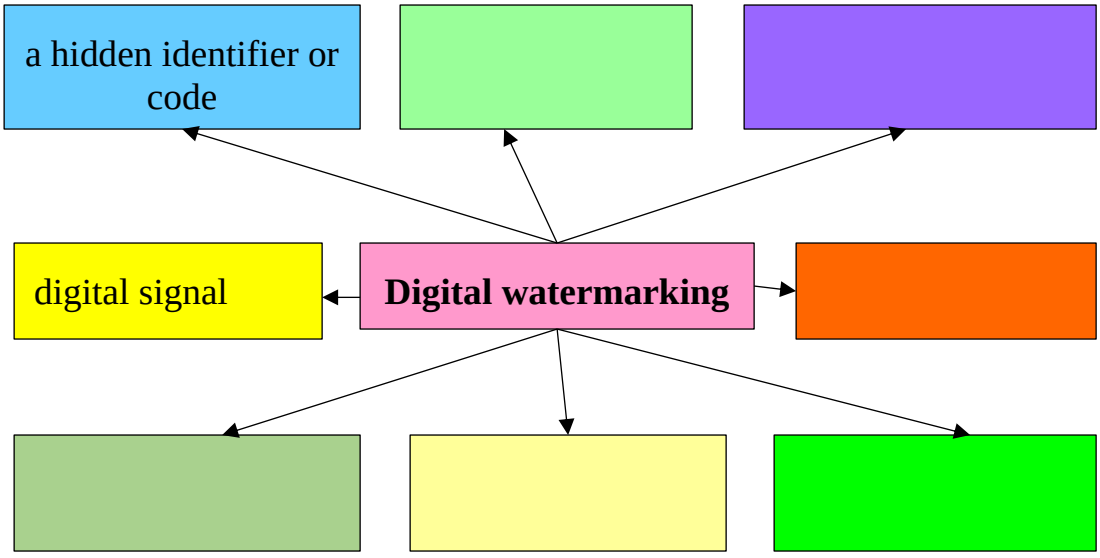
2.4. DIGITAL WATERMARKING

WARM UP

1. **A. & B. Using your background knowledge, do the tasks according to your learning style (dominant or non-dominant modality).**

1.1. *Visual Modality*

Work individually, then in small groups. Create a mind map with a central concept "Digital watermarking". Start by brainstorming relevant terms related to digital watermarking. Clearly illustrate how each term relates to the central theme.



1.2. *Auditory Modality*

Answer the questions.

1. What is digital watermarking?
2. What is the aim of digital watermarking?
3. What types of digital watermarking do you know?
4. How does digital watermarking work?
5. Who uses digital watermarking?

1.3. *Kinesthetic Modality*

Work in pairs to complete the table by listing the advantages and disadvantages of digital watermarking. Then, share your findings with your classmates, highlighting the key benefits and potential drawbacks of using watermarking technology.

Advantages of digital watermarking	Disadvantages of digital watermarking
1. ……...	1. *Complexity*
2. ……...	2. …….
3. ……...	3. …….
4. ……...	4. …….
5. ……...	5. …….

READING

You are going to read an article about digital watermarking.

2.

1. A. & B. Before reading, discuss the following statement.

Digital watermarking is a crucial mechanism for copyright protection.

2. A. & B. Before reading, look at the following words and phrases, which have been taken from the text. In what context might they be mentioned? Use Merriam-Webster Dictionary if necessary.

Watermarking, a carrier signal, to verify the authenticity or integrity, to show the identity, infringements, to distort, to employ, imperceptibility, to transmit, compression of the data, unmodified, robust, additive noise, semi-fragile, imperceptible, transparent / translucent, amplitude.

3. **Read the text about digital watermarking. Five sentences have been removed. Choose which of the sentences fit into the gaps.**

A	While steganography aims at imperceptibility to human senses, digital watermarking tries to control the robustness as a top priority.
B	Spread-spectrum involves additive modifications and offers moderate robustness but limited capacity.
C	Originally, watermarks were identification marks created during paper making, first appearing in 13th century Italy to identify paper makers or guilds, often made by sewing wire onto the paper mold.
D	Traditional watermarks may be applied to visible media (like images or video), whereas in digital watermarking, the signal may be audio, pictures, video, texts or 3D models.
E	Some perceptible watermarks are made translucent to minimise visual interference, but this differs from perceptual watermarking, which exploits human perception limits to remain unseen.

DIGITAL WATERMARKING

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio, video or image data. It is typically used to identify ownership of the copyright of such a signal. "*Watermarking*" is the process of hiding digital information in a carrier signal. The hidden information should, but does not need to, contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is used for tracing copyright infringements and for banknote authentication.

Like traditional physical watermarks, digital watermarks are often only perceptible under certain conditions, e.g. after using some algorithm. If a digital watermark distorts the carrier signal in a way that it becomes easily perceivable, it may be considered less effective depending on its purpose. **1. _____**. A signal may carry several different watermarks at the same time. Unlike metadata that is added to the carrier signal, a digital watermark does not change the size of the carrier signal.

The required characteristics of a digital watermark depend on the application in which it is used. For marking media files with copyright information, a digital watermark has to be rather robust against modifications that can be applied to the carrier signal. Instead, if integrity has to be ensured, a fragile watermark would be applied.

Both steganography and digital watermarking employ steganographic techniques to embed data covertly in noisy signals. **2. _____**.

Since a digital copy of data is the same as the original, digital watermarking is a passive protection tool. It just marks data, but does not degrade it or control access to the data.

One application of digital watermarking is source tracking. A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known. This technique reportedly has been used to detect the source of illegally copied movies.

The term “digital watermark” was coined by Tirkel and Osborne in 1992, with the first successful digital watermark demonstrated in 1993. **3. _____**. Today, watermarks are still used for branding and anti-forgery purposes.

Digital watermarking life-cycle phases (fig. 1). The information to be embedded in a signal is called a digital watermark, although in some contexts the phrase digital watermark means the difference between the watermarked signal and the cover signal.

The signal where the watermark is to be embedded is called the host signal. A watermarking system is usually divided into three distinct steps, embedding, attack, and detection. In embedding, an algorithm accepts the host and the data to be embedded, and produces a watermarked signal.

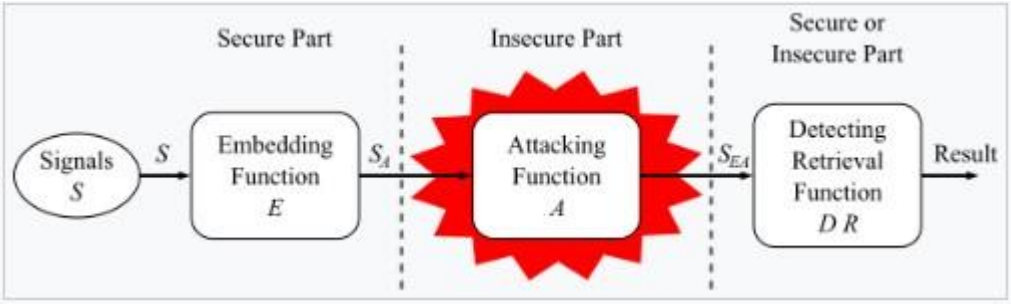


Figure 1. *General digital watermark life-cycle phases with embedding-, attacking-, and detection and retrieval functions*

Then the watermarked digital signal is transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called *an attack*. While the modification may not be malicious, the term attack arises from copyright protection application, where third parties may attempt to remove the digital watermark through modification. There are many possible modifications, for example, lossy compression of the data, cropping an image or video, or intentionally adding noise.

Detection (often called extraction) is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark still is present and it may be extracted. In robust digital watermarking applications, the extraction algorithm should be able to produce the watermark correctly, even if the modifications were strong. In *fragile* digital watermarking, the extraction algorithm should fail if any change is made to the signal.

Digital watermarking techniques may be classified in several ways.

Robustness includes fragile, semi-fragile, and robust watermarks. Fragile watermarks are easily destroyed by slight modifications and are mainly used for tamper

detection. Semi-fragile watermarks resist benign changes but fail under malicious alterations, making them useful for detecting serious tampering. Robust watermarks withstand specific transformations, supporting applications like copy protection.

Another technique is *perceptibility*. Imperceptible watermarks are indistinguishable from the original signal, while perceptible watermarks are noticeable, such as on-screen logos or content bugs. **4. _____**.

Capacity refers to the amount of information embedded within the watermark. Zero-bit schemes detect only the presence or absence of a watermark, whereas multiple-bit schemes encode a stream of data. The choice depends on the application's need for simple detection versus detailed information embedding.

Embedding methods also vary, including spread-spectrum, quantisation, and amplitude modulation. **5. _____**. Quantisation employs quantisation techniques, providing high capacity but lower robustness, while amplitude modulation embeds watermarks in the spatial domain through additive modifications.

Borrowed and modified from: Digital watermarking,
https://en.wikipedia.org/wiki/Digital_watermarking
Modified by https://deepai.org/chat/text-generator

4. **A. & B. Read the text again and do the following tasks.**

4.1. Fill in the missing information in statements 1–8.

1. "Watermarking" refers to the process of embedding digital information within a _____ _____.
2. Unlike traditional watermarks, which are applied to _____ media such as images or video, digital watermarking can be applied to audio, pictures, _____, text or 3D models.
3. Both steganography and digital watermarking employ steganographic techniques to _____ data covertly in noisy signals.

4. Today, watermarks are still used for branding and _____ purposes.
5. In some contexts the phrase digital watermark means the difference between the _____ signal and the _____ signal.
6. Fragile watermarks are easily destroyed by slight _____ and are mainly used for tamper detection.
7. Zero-bit schemes detect only the presence or absence of a _____, whereas _____ schemes encode a stream of data.
8. Quantisation employs quantisation techniques, providing high _____ but lower _____.

4.2. Decide whether these sentences are *true or false*.

1. Digital watermarks are only used to identify ownership of the copyright of an audio signal.
2. Digital watermarks are only used for tracing copyright infringements.
3. The first watermarks were produced during the paper-making process in Italy during the 13th century.
4. The digital watermark is the information embedded in a signal, and the host signal is where the watermark is embedded.
5. Attack in digital watermarking always refers to malicious activity aimed at destroying the watermark.
6. Fragile watermarks are used mainly for tamper detection because they are easily destroyed by slight modifications.
7. Imperceptible watermarks are designed to be indistinguishable from the original signal, while perceptible watermarks are noticeable.
8. Spread-spectrum embedding involves additive modifications and offers moderate robustness, while quantisation provides high capacity but lower robustness.

5. **A. & B. Give the synonyms to the words in italics. Use any AI tool to fill in the third rubric of the table. Then, make two sentences using different synonym phrases.**

Phrases	Synonyms suggested by students	Synonyms generated by AI
1) *hidden* information		
2) to *verify* the authenticity or integrity		
3) to *trace* copyright infringements		
4) to *distort* the carrier signal		
5) to *change* the size of the carrier signal		
6) *embedding*, attack, and *detection*		
7) to be *transmitted or stored*		
8) to *remove* the digital watermark through *modification*		
9) *imperceptible*		
10) to *minimise* visual *interference*		
11) *transparent / translucent*		

6. **A. & B. Make a list of the five most important things that you have to remember about digital watermarks. Compare your list to your partner's. Which three are the most popular among the class?**

USE OF ENGLISH

VOCABULARY

7. **A. Complete the sentences. Use: *invisible, a hidden pattern, spread-spectrum, watermarking, copyrights, authenticity, audio or video, embedded, hidden, security, detected, unauthorised.***

A digital watermark is a technology that embeds **1)** _____ or identification into digital content, like pictures, **2)** _____, in order to prove its **3)** _____ and ownership. The **4)** _____ marks can be used to identify and track the origin of content and prevent **5)** _____ copying or distribution. Digital watermarks can be **6)** _____ using a variety of algorithms and techniques, including **7)** _____, steganography and compression-based methods. Once the watermark has been embedded, it remains **8)** _____ in the background of the content and can only be **9)** _____ with the use of specialised software or equipment. Digital **10)** _____ has a wide range of applications in industries such as entertainment, media and finance, where the protection of **11)** _____ and the **12)** _____ of content are of critical importance.

B. Complete the sentences.

1. Digital _____ provides several _____, including: improved content _____, enhanced copyright _____, increased efficiency in content tracking and management, and enhanced revenue opportunities. **2.** It also offers a non-invasive and non-destructive way of tagging _____ content. **3.** This allows easy _____ and recognition without affecting the original quality of the _____. **4.** In addition, digital watermarketing can be used to _____ the origin and ownership of digital content. **5.** Moreover, digital watermarks can be adaptive, allowing them to be updated or _____ as required. **6.** They can be used in combination with other anti-piracy measures to provide a _____ defence against content theft.

IDIOMS

8. **A. Match the idioms in bold to their equivalents. Have you got any similar idioms / phrases in your language?**

The overall strength of a system depends on its most vulnerable component, safeguarding their sensitive information, taking small precautions can save us from bigger problems later, images convey significant meaning, are determined to continue, mustn't dismiss its benefits entirely, put the matter to rest.

1. In the digital age, implementing watermarking is crucial because **a picture is worth a thousand words,** and our ownership must remain clear.
2. Companies are **keeping their cards close to their chest** by embedding digital watermarks to ensure their work is protected from inappropriate use.
3. While some people argue that digital watermarking can complicate the distribution process, **we mustn't throw the baby out with the bathwater –** it remains an essential tool for protecting creative rights.
4. We are sticking to our guns about using digital watermarking, despite criticism from some content creators who don't see its value in the fight against piracy.
5. After a detailed investigation of the security breach, the company decided to implement digital watermarking to protect its content and finally **draw a line under the issue** to prevent future compromises.
6. Our team often reminds us that **an ounce of prevention is worth a pound of cure,** which is why we have chosen to invest in effective digital watermarking solutions.
7. In digital rights management, it is essential to recognise that **a chain is only as strong as its weakest link.**

B. Fill in the blanks using the idioms from the list below. You may need to change the verb tense.

A picture is worth a thousand words, keeping their cards close to their chest, don't throw the baby out with the bathwater, sticking to your guns, draw a line under the issue, an ounce of prevention is worth a pound of cure, a chain is only as strong as its weakest link.

The secret war over digital intellectual property is often fought in the invisible pixels of a file. When our agency developed a new forensic watermarking technique, we were **1)** _____, refusing to reveal the algorithm to even our closest partners. We knew that in this industry, **2)** _____, but a stolen high-resolution render can also be worth thousands of dollars in lost revenue.

Early in the beta test, a bug caused the watermark to slightly distort the color balance of the images. Some designers wanted to scrap the entire project, but I argued that we shouldn't **3)** _____. The core tech worked; it just needed a finer touch. By **4)** _____ and refusing to abandon the project, we eventually refined the code until the mark was completely invisible to the human eye but instantly detectable by our scanners.

We soon discovered that the distribution servers were stripping metadata, proving once again that **5)** _____. We had to convince the host sites to update their protocols, reminding them that **6)** _____; it's much cheaper to prevent a leak than to sue a pirate after the fact. Once the new security standards were signed into effect, we were finally able to **7)** _____ and focus on our next creative campaign.

Borrowed and modified from: https://gemini.google.com/

GRAMMAR

9. **A. & B. Use past tenses in the sentences below.**

1. A. Tirkel and Ch. Osborne _____ **(invent)** the term "digital watermark" in December 1992.
2. I _____ **(watermark)** the image at 5 o'clock in the morning.
3. The company _____ **(research)** digital watermarking techniques for months before they developed their own technology.
4. She watermarked all the pictures she _____ **(take)** on her birthday yesterday.
5. By the time I checked my email, the message _____ **(read, already)** and _____ **(delete)**.
6. The team _____ **(watermark)** a video at 5 am this morning.
7. The algorithm _____ **(train)** to detect watermarks in images before it was used in the production process.
8. I _____ **(watermark)** all my photos by the time I uploaded them to social media.
9. The hackers _____ **(try)** to remove the watermark from the stolen data as it was being transferred.
10. By the time we received the complaint, the watermark _____ **(remove, already)** from the video.

10. **A. Choose the correct option.**

1. A watermarking system _____ **formed / is formed** mainly by two processes: insertion and detection.
2. _____ **To improve / Improve** the robustness of the video watermarking technique, it is preferable to insert the mark in moving objects.

3. The robustness of the watermarking system is tested by _____ **applied / applying** several attacks known as: Gaussian noise, impulse noise, compression MPEG II, MP3 compression.
4. We have been able _____ **increase / to increase** the insertion capacity while maintaining a good criterion of imperceptibility and robustness.
5. Digital watermarking has been _____ **widely / wide** used for ownership identification and copyright protection.
6. Digital watermarking is _____ **the more / the most** secured way to protect copyright protection and authentication.
7. Various types of image watermarking methods _____ **have been proposed / have proposed** in past decades.
8. _____ **To verify / Verifying** the robustness of our proposed method, we applied different malicious attacks such as noise addition, cropping, rotation, filtering, blurring, sharpening, JPEG compression, etc. _____ **of / on** the watermarked image.
9. The initial input signal is _____ **an / a** uncompressed video file.
10. We think that we _____ **calculate / will calculate** the NC values between the mark before and after the attacks for both components.

B. Choose the correct option.

1. After _____ **got / getting** the watermarked audio signal and different watermarked images, we join _____ **this / these** two components (audio and image) to form the final watermarked video signal.
2. To assess the robustness, we have calculated normalised correlation (NC) which _____ **compute / computes** the difference _____ **of / between** original watermark and the extracted watermark.

3. The temporal methods _____ **based on / basing on** the least significant bit (LSB) provide good results _____ **on / in** terms of imperceptibility, insertion capacity, and robustness.
4. **_____ To test / Tested** the robustness of the technique against attacks, we will calculate the correlation NC between the original brand inserted and the mark _____ **detecting / detected** after the exposure of watermarked files to different attacks.
5. In this model, we _____ **do not distinguish / did not distinguish** between tonal and non-tonal components, but we calculate tonal indices that _____ **determine / determines** whether the components appear to be tonal or nontonal (noise).
6. The insertion _____ **performed / is performed** at _____ **moved / moving** objects and in non-successive images.
7. **_____ Guarantee / To guarantee** a good robustness criterion _____ **especially / especial** against the compression, we inserted the bits of the mark in the moving objects of the video.
8. The _____ **proposing / proposed** watermarking technique does not affect the quality of images and the inserted brand remains invisible _____ **to / of** the human eye.
9. This watermarking system watermarks both image _____ **as well as / and** audio components, if it _____ **will exist / exists**.
10. Experimental results indicate that the _____ **proposed / proposing** method is _____ **highly / high** robust against various attacks such as noise addition, cropping, filtering, blurring, rotation, JPEG compression etc.

Borrowed and modified from: "Digital Image and Video Watermarking and Steganography" S. Ramakrishnan

LISTENING

You are going to watch a video that explores the specifics of digital watermarking.

11. **A. & B. Before watching a video, check if you know the meaning of the words and phrases. Use Merriam-Webster Dictionary if necessary.**

Visible, invisible, fragile, obust, preventive control, detective control, embedded, detectable, robust, tampering, to deter errors or irregularities, verifying authenticity and integrity of files to show ownership, digital extraction process, to figure out some new technology, forgery and tampering detection, imprinted logos and photographs.

12. **Watch the video "Digital Watermarking". Then, answer the questions.**

1. What are digital watermarks?
2. What three steps of digital watermarking have been mentioned in the video presentation?
3. What is the difference in terminology:
   – visible and invisible;
   – invisible and imperceptible;
   – fragile and robust;
   – detective control and preventive control?
4. How is digital watermarking used?
5. What interesting application of digital watermarking has been mentioned in the video?

13. A. & B. Watch the video again and do the following tasks.

13.1. Decide whether these sentences are *true or false*.

1. Digital watermarks are codes added to various types of digital files.
2. The second step of digital watermarking involves directly embedding a watermark into the file.
3. Visible digital watermarks can be seen by the human eye.
4. Invisible digital watermarks can be detected without any special software.
5. Fragile digital watermarking is destroyed if any part of a file is modified.
6. Robust digital watermarking cannot be extracted if a file is modified.
7. Preventive controls aim to prevent errors or irregularities from happening.
8. Digital watermarking ensures that a file is 100% protected from tampering.
9. The first application of digital watermarking is copyright protection.
10. Digital watermarks can guarantee that an owner can prevent copying of their files completely.

13.2. Choose the correct option.

1. What is a digital watermark?
    a. A code added to a digital audio, video, image, or document file.
    b. A way to protect files from being copied.
    c. A type of antivirus software.
2. What is the three-step process involved with digital watermarking?
    a. Embed, modify / copy / replace, extract.
    b. Detect, extract, modify.
    c. Protect, scan, hide.
3. What is visible digital watermarking?
    a. Only detectable with special software.
    b. Not detectable at all.
    c. Viewable by human eye or detectable by ear.

4. What is fragile digital watermarking used for?
    a. Copyright protection and ownership protection.
    b. Tampered detection and data security.
    c. Forgery and tampering detection.
5. What is robust digital watermarking used for?
    a. Tampered detection and data security.
    b. Forgery and tampering detection.
    c. Copyright protection and ownership protection.
6. What is detective control in digital watermarking?
    a. A process designed to deter errors or irregularities from occurring.
    b. A process designed to identify if errors or irregularities have occurred.
    c. A type of antivirus software.
7. How can digital watermarking be used for copyright protection?
    a. By inserting digital watermarks within a file to identify the true owner.
    b. By preventing unauthorised distribution of files.
    c. By detecting tampered files.
8. How can digital watermarking be used for data security?
    a. By certifying and authenticating a file.
    b. By detecting tampered files.
    c. By protecting files from being copied.
9. What is an application of digital watermarking besides protection and security?
    a. Trade shows and open houses.
    b. Advertising and marketing.
    c. Education and training.

10. What happens when a tampered photo is run through a digital watermark detection program?

    a. The tampered areas are identified in black.

    b. The tampered areas are identified in white.

    c. The tampered areas are not identified at all.

SPEAKING

14. **A. Work in pairs. In the ESP class, discuss with your classmate the issue about digital watermarking. Your conversation should cover the following key aspects: definition of digital watermarking, hackers and digial watermarking, privacy concerns, a legal framework surrounding digital watermarks. Your dialogue should include at least 5–6 exchanges per each participant. Be creative! Remember to keep the tone respectful!**

A	B
1. I've been thinking a lot about digital watermarking lately. Have you ever heard of it?	1. Yes. It is a technology that is used to track and monitor digital content online. Like, to prevent piracy and stuff.
2. But it's more complex than that. Digital watermarks are …	2. That sounds cool. But how does it work?
3. …….	3. …….
4. …….	4. ……
5. …….	5. ……
6. …….	6. …….

B. Work in pairs. At the conference, you engage in a dialogue about digital watermarking with a colleague from MIT. Your conversation should cover the following aspects: how digital watermarking works; digital watermarking life-cycle phases; digital watermarking in the age of AI. The dialogue should

include at least 7–8 exchanges per each participant. Be creative! Remember to keep the tone respectful!

15. **A. You are asked to choose one specific issue related to digital watermarking. Then prepare a two-minute presentation.**

1. Ethical considerations in digital watermarking.
2. The effectiveness of digital watermarking in copyright protection.
3. The potential for misuse of digital watermarking technology.

B. You are asked to prepare a five-minute presentation on one of the topics.

1. Difference between cryptography, steganography and watermarking.
2. Digital watermarking in the age of AI.
3. The role of digital watermarking in digital forensics.
4. The impact of digital watermarking on the music industry.
5. The potential applications of digital watermarking in healthcare.
6. The security risks associated with digital watermarking.
7. The legal framework for digital watermarking.
8. The future of digital watermarking.

WRITING

16. **A. For your research, write a summary (160–170 words) of the text "Digital watermarking" in Ex. 3 (Reading section) or Ex. 12 (Listening section).**

Use a five-key-step list:

1. **Read the text.**
2. **Split it into parts.**
3. **Define the key points in each part.**
4. **Create a summary.**
5. **Compare the summary with the article.**

17. **B. For your research, write a summary (180–200 words) that combines information in both texts of Ex. 3 (Reading section) and Ex. 12 (Listening section).**

Use a five-key-step list:

1. **Read or listen to the text.**
2. **Split it into parts.**
3. **Define the key points in each part.**
4. **Create a summary.**
5. **Compare the summary with the articles.**

REFLECTION AND SYNTHESIS

18. **You have completed this unit. This word cloud can help you to reflect on and synthesise the key concepts from the topic. Focus on the most important terms and ideas that stood out to you. Using the word cloud as a visual tool, you have to illustrate your understanding.**

2.5. UNIT 2. REVISION 2

WARM UP

1. **A. & B. Decide whether these sentences are *true* or *false*.**

1. Cryptology is the overall discipline encompassing both cryptography and cryptanalysis.
2. Ciphers generally substitute different length strings of characters in the output, while codes generally substitute the same number of characters as are input.
3. "Eavesdropper" refers to someone who secretly listens to a conversation between other people.
4. Kerckhoffs' principle states that all security should be concentrated in the secrecy of the algorithms.
5. Brute force attack is an attack where every possible key is tried until the right one is found.
6. The name of *chosen-ciphertext attack* comes from the common security vulnerability where an employee logs on their encrypted computer and then leaves it unattended while they go to lunch, giving an attacker temporary access to the system.
7. The first recorded use of steganography dates back to ancient Greece.
8. Digital steganography is the process of embedding messages in digital cover mediums.
9. Digital watermarking is an active protection tool that degrades the data it marks.
10. The term "attack" in digital watermarking refers to any modification made to the watermarked signal, whether intentional or unintentional, with the goal of removing or tampering with the watermark.
11. Digital watermarks change the size of the carrier signal.
12. Quantisation watermarks suffer from low robustness.

READING

2. A. & B. Read the text and do the following tasks.

2.1. Decide if the statements are *true* or *false*.

1. Kleptography is the study of stealing information securely and subliminally.
2. The term "kleptography" was introduced by Gus Simmons.
3. A kleptographic backdoor is also known as an asymmetric backdoor.
4. Kleptography is the same as steganography.
5. A kleptographic attack utilises asymmetric cryptography to implement a cryptographic backdoor.
6. A reverse engineer can use a kleptographic backdoor even if it is asymmetric.
7. Kleptographic attacks have been designed for various cryptographic algorithms, including RSA and the Digital Signature Algorithm.
8. The KEGVER method allows the attacker to reproduce the private key through a kleptographic attack.

2.2. Fill in the missing information in statements 1–8.

1. Kleptography is a subfield of _____ and is a natural extension of the theory of _____ channels.
2. Kleptography encompasses secure and _____ communications through cryptosystems and cryptographic protocols.
3. A kleptographic attack is an attack which uses _____ cryptography to implement a cryptographic _____ .
4. If the infected cryptosystem is a _____ implementation such as a hardware security module, a smartcard, or a Trusted Platform Module, a successful attack could go completely unnoticed.
5. A _____ engineer might be able to uncover a backdoor inserted by an attacker and, if it is a _____ backdoor, even use it himself.

6. A kleptographic attack requires a _____ key known only to the attacker in order to use the backdoor.
7. SSL, SSH, and IPsec protocols are _____ to kleptographic attacks.
8. A. Juels and J. Guajardo proposed a method (KEGVER) through which a third party can _____ RSA key generation.

KLEPTOGRAPHY

Kleptography is the study of stealing information securely and subliminally. The term was introduced by Adam Young and Moti Yung in the Proceedings of Advances in Cryptology – Crypto '96. Kleptography is a subfield of cryptovirology and is a natural extension of the theory of subliminal channels that was pioneered by Gus Simmons while at Sandia National Laboratory. A kleptographic backdoor is synonymously referred to as an asymmetric backdoor. Kleptography encompasses secure and covert communications through cryptosystems and cryptographic protocols. This is similar to, but not the same as steganography that studies covert communications through graphics, video, digital audio data, and so forth.

A kleptographic attack is an attack which uses asymmetric cryptography to implement a cryptographic backdoor. For example, one such attack could be to subtly modify how the public and private key pairs are generated by the cryptosystem so that the private key could be derived from the public key using the attacker's private key. In a well-designed attack, the outputs of the infected cryptosystem would be computationally indistinguishable from the outputs of the corresponding uninfected cryptosystem. If the infected cryptosystem is a black-box implementation such as a hardware security module, a smartcard, or a Trusted Platform Module, a successful attack could go completely unnoticed.

A reverse engineer might be able to uncover a backdoor inserted by an attacker and, if it is a symmetric backdoor, even use it himself. However, by definition a kleptographic backdoor is asymmetric and the reverse engineer cannot use it. A kleptographic attack (asymmetric backdoor) requires a private key known only to the attacker in order to use the backdoor. In this case, even if the reverse engineer was well-funded and gained complete knowledge of the backdoor, it would remain useless for them to extract the plaintext without the attacker's private key.

Kleptographic attacks can be constructed as a cryptotrojan that infects a cryptosystem and opens a backdoor for the attacker, or can be implemented by the manufacturer of a cryptosystem. The attack does not necessarily have to reveal the entirety of the cryptosystem's output; a more complicated attack technique may alternate between producing uninfected output and insecure data with the backdoor present.

Kleptographic attacks have been designed for RSA key generation, the Diffie-Hellman key exchange, the Digital Signature Algorithm, and other cryptographic algorithms and protocols. SSL, SSH, and IPsec protocols are vulnerable to kleptographic attacks. In each case, the attacker is able to compromise the particular cryptographic algorithm or protocol by inspecting the information that the backdoor information is encoded in (e.g., the public key, the digital signature, the key exchange messages, etc.) and then exploiting the logic of the asymmetric backdoor using their secret key (usually a private key).

A. Juels and J. Guajardo proposed a method (KEGVER) through which a third party can verify RSA key generation. This is devised as a form of distributed key generation in which the secret key is only known to the black box itself. This assures that the key generation process was not modified and that the private key cannot be reproduced through a kleptographic attack.

Four practical examples of kleptographic attacks (including a simplified SETUP attack against RSA) can be found in JCrypTool 1.0, the platform-independent version of the open-source CrypTool project. A demonstration of the prevention of kleptographic attacks by means of the KEGVER method is also implemented in JCrypTool.

The Dual_EC_DRBG cryptographic pseudo-random number generator from the NIST SP 800-90A is thought to contain a kleptographic backdoor. Dual_EC_DRBG utilises elliptic curve cryptography, and NSA is thought to hold a private key which, together with bias flaws in Dual_EC_DRBG, allows NSA to decrypt SSL traffic between computers using Dual_EC_DRBG for example. The algebraic nature of the attack follows the structure of the repeated Dlog Kleptogram in the work of Young and Yung.

Borrowed and modified from: https://en.wikipedia.org/wiki/Kleptography.

3. Find words and phrases in the text that match definitions 1–6.

1. _____ is a field of study that combines cryptography and malware development, with a focus on how cryptographic techniques can be used to create malware that encrypts data and demands a decryption ransom.
2. _____ is the study of secretly and securely stealing information, in particular through methods that embed a hidden backdoor into cryptographic systems, allowing attackers to access data without being detected.
3. _____ to introduce malware into a computer system / network, compromising its integrity and functionality, often to enable unauthorised access or control.
4. _____ a type of cyber attack in which an adversary inserts malicious data into a digital certificate or other cryptographic material, allowing them to intercept or eavesdrop on encrypted communications.

5. _____ communication channels that operate below the conscious level of perception, allowing information to be transmitted covertly, often without the aware involvement of the communicating parties.
6. _____ takes apart, dissects, and analyses the internal workings of a product, system, or technology to understand its design, architecture, and underlying mechanisms.

4. **Discuss the questions.**

1. Who introduced the term "kleptography"?
2. How is kleptography related to cryptovirology and subliminal channels? What is cryptovirology?
3. What is a kleptographic backdoor? How does it differ from a symmetric backdoor?
4. Describe a potential scenario of a kleptographic attack involving key generation.
5. What types of cryptographic systems are vulnerable to kleptographic attacks?
6. What is the KEGVER method proposed by A. Juels and J. Guajardo? What purpose does it serve?
7. Can a reverse engineer use a kleptographic backdoor if it is asymmetric? Why or why not?
8. What is the significance of the Dual_EC_DRBG in the context of kleptographic backdoors?

USE OF ENGLISH

5. **A. Fill in with *stego-analytical algorithms, known-plaintexts, steganography, plaintext, robust, disclose, indecipherable, substitution, maid, cryptography, candidate, digital watermarking, attack*.**

1. The system must be practically, if not mathematically, _____ .

2. The Caesar Cipher is a type of _____ cipher where each letter in the _____ is shifted a fixed number of positions down the alphabet.
3. During theSecond World War, the Allies used _____ in their successful cryptanalysis of the Enigma machine cipher.
4. Evil maid attack refers to an unauthorised person such as a _____ getting physical access to the encryption equipment, and modifying it to _____ the plaintext or key when it is used.
5. A suspect identified through some type of statistical analysis can be referred to as a _____ .
6. The advantage of _____ over _____ alone is that the intended secret message does not attract attention to itself as an object of scrutiny.
7. _____ can be categorised in different ways, depending on the information available and the specific goal or purpose being achieved.
8. The _____ process typically involves three distinct phases: embedding, attack, and detection.
9. A digital watermark is called _____ with respect to transformations if the embedded information may be detected reliably from the marked signal, even if degraded by any number of transformations.
10. If this person makes a modification, this is called an _____ .

B. Complete the sentences.

Physical steganography, which involves using a **1) _____** medium to conceal a **2) _____** message, has been a widespread practice for centuries. One notable example is the use of **3) _____** ink on paper. Other methods include writing messages in Morse **3) _____** on yarn worn by a courier, microdots, and even **4) _____** messages as musical notes in sheet music.

In communities with **5) _____** or government restrictions, people often use *cultural or social steganography*, hiding messages in idiom, pop culture references, and publicly shared content. It relies on context and **6) _____**. For instance, a **7) _____** could be hidden in the title and context of a shared video or picture, or through misspelled words that suggest an alternative meaning.

With the development of computers, *digital steganography* techniques have emerged, enabling the **8) _____** of messages within digital cover mediums. This often involves **9) _____** the message before overwriting part of a larger block of data or random data. This makes it almost impossible to detect without the decryption **10) _____** .

6. **A. Put the verbs in brackets into the correct past tense.**

1. He informed that they _____ **(encrypt)** the message.
2. In 1883, A. Kerckhoffs _____ **(formulate)** the principle, which states that a cryptographic system should be secure even if the adversary has full knowledge of the system's details, except for the secret key or encryption method.
3. Ann _____ **(analyse)** a suspicious image, carefully examining each pixel, while Tom _____ **(develop)** a new algorithm to conceal digital data within a seemingly innocuous file.
4. Jane _____ **(study)** cryptography for five years before she _____ **(enter)** university.
5. Yesterday at 7 o'clock the researchers _____ **(analyse)** the image for hidden messages, using advanced algorithms to detect any signs of steganography.

6. By the time the authorities discovered the hidden message, the sender _____ **(encode)** already it into an innocent image using steganography.
7. They _____ **(study)** the suspect's computer files for hours before they finally _____ **(find)** the digital note that hinted at the existence of a secret communication.
8. After analysing the suspicious file, forensic experts _____ **(discover)** that it contained a hidden audio file that had been embedded using steganographic techniques.
9. Last year, I _____ **(attend)** a watermarking workshop where I _____ **(learn)** how to detect and remove digital watermarks from various types of media.
10. Sam _____ **(read)** the book on steganography at 6 o'clock last night.

B. Put the verbs into the correct past tense.

Always interested in the concept of digital watermarking, Alex **1) _____ (decide)** to attend a training course to learn more about it. Before the course **2) _____ (start)**, he **3) _____ (hear)** never of steganography. On the first day of the course, he **4) _____ (learn)** that it was actually a related but distinct concept. Steganography **5) _____ (be)** about hiding information within a medium without altering its appearance, while digital watermarking was about embedding a unique message into a digital file to prove ownership or authenticity. At that time, he **6) _____ (learn)** about the different types of digital watermarking as invisible watermarks and visible watermarks.

Alex **7) _____ (learn)** about digital watermarking for several days before he **8) _____** access to some software and **9) _____ (start)** creating his

digital watermarks. With the instructor's guidance, Alex **10) _____ (learn)** to detect and extract watermarks using specialised software.

While working on the course, Alex **11) _____ (realise)** that digital watermarking was not only a powerful tool for copyright protection. It **12) _____ (be)** also an interesting area of research. He **13) _____ (gain)** a comprehensive understanding of digital watermarking by the end of the course.

SPEAKING

7. Work in groups. Choose one of the rubrics and discuss the questions.

1. Ciphers and codes

1. What is the difference between ciphers and codes?
2. What is the main difference between a substitution cipher and a transposition cipher?
3. How does the Caesar Cipher work, and what is its limitation?
4. What is the concept of a "key" in cryptography? How is it used in ciphers?

2. Cryptanalysis. Cryptanalysis attacks

5. What is cryptanalysis? What is the aim of cryptanalysis?
6. How does cryptanalysis work?
7. What cryptanalysis attacks do you know? What are their specifics?
8. What are the main types of cryptanalysis?

3. Steganography

9. What is steganography?
10. How is it different from cryptography?
11. What are some common applications of steganography? Why is it used?
12. What steganography techniques do you know?

4. Digital watermarking

13. What is digital watermarking? What are its primary uses?
14. How does a digital watermark differ from traditional physical watermarks?
15. What is the main difference between steganography and digital watermarking?
16. What are the main digital watermarking life-cycle phases?

5. Kleptography

17. What is kleptography?
18. How does it differ from cryptography?
19. What are some potential applications of kleptography? Why is it used?
20. Can you compare kleptography and steganography according to: purpose, abstraction level, methods, implementation, counteracting transmission?

6. Cryptovirology

21. What is cryptovirology?
22. How does cryptovirology differ from traditional computer viruses?
23. How do cryptovirology attacks work? What are their primary goals?
24. What are some common defense mechanisms against cryptovirology attacks?

8. Work in groups. Create a comprehensive mind map that visually illustrates the relationships and connections between the concepts of cryptography, cryptanalysis, steganography, digital watermarking, kleptography, and cryptovirology. After completing the mind map, provide a clear explanation of how these concepts interrelate and their respective roles in information security.

WRITING

9. **You are asked to write a paragraph (150–160 words) on one of the topics given below. Use any 5 phrasal verbs from the list: *come across, come into play, deal out, decide against, decide upon, come together, deal with, differ from, do away with, fall back, get across, do up, fall into, get around, do over*.**

1. **Ciphers and codes.**
2. **Cryptanalysis. Cryptanalysis attacks.**
3. **Steganography.**
4. **Digital watermarking.**
5. **Kleptography.**
6. **Cryptovirology.**

10. **To participate in the *Opinion Essay Contest*, you need to write an essay (180–200 words) on one of the topics given below. Your essay should follow a clear structure, consisting of an introduction, main body, and conclusion.**

Additionally, you must incorporate the idioms: *spill the beans, read between the lines, cutting edge, the weakest link, playing cat and mouse, under lock and key, an open book, a picture is worth a thousand words, draw a line under the issue, a chain is only as strong as its weakest link, don't throw the baby out with the bathwater, sticking to your guns, an ounce of prevention is worth a pound of cure*.

A. Use at least seven idioms.

B. Use at least ten idioms.

Topics:

1. **Ciphers and codes.**
2. **Cryptanalysis. Cryptanalysis attacks.**
3. **Steganography.**
4. **Digital watermarking.**
5. **Kleptography.**
6. **Cryptovirology.**

PROJECT

11. **1. Work in small groups. You are in the cryptography workshop. You are asked to apply different cryptanalysis techniques to break the cipher.**

CIPHERTEXT 1.

Cipher: Substitution Cipher (Caesar Cipher)

Text: GUR PENML XRL VF ZL FRPERG CBFG

Description: The ciphertext is a substitution cipher where each letter has been replaced by a letter a fixed number of positions down the alphabet. In this case, each letter has been replaced by the letter three positions down the alphabet.

Techniques to break:

Frequency analysis: Look for common letter combinations in the ciphertext and try to identify the corresponding letters in the original message.

Kasiski examination: Look for repeated patterns in the ciphertext and try to identify the key used to encrypt the message.

CIPHERTEXT 2

Cipher: Transposition Cipher

Text: T E A R O F S U P E R C A L I F

Description: The ciphertext is a transposition cipher where each letter has been rearranged according to a specific pattern.

Techniques to break:

Frequency analysis: Look for common letter combinations in the ciphertext and try to identify the corresponding letters in the original message.

Cryptanalysis by permutation: Try to identify the pattern used to rearrange the letters and then use frequency analysis or Kasiski examination to break the cipher.

2. Work in small groups. You are in the cryptography workshop. You are asked to apply different cryptanalysis techniques to create a ciphered text. Then exchange the ciphertexts and break the ciphers.

Tips:

1. **Use one of the following techniques:**
   - ✓ **Substitution Cipher (Caesar Cipher)**
   - ✓ **Vigenère Cipher**
   - ✓ **Transposition Cipher**
   - ✓ **Polyalphabetic Cipher (Rail Fence Cipher)**
2. **Write the ciphertext on a piece of paper.**
3. **Keep your original plaintext secret.**
4. **Exchange the ciphertexts with other group members, but not the original plaintext.**

5. **Using the exchanged ciphertexts, try to break the ciphers using the following techniques:**
   - ✓ **Frequency analysis**
   - ✓ **Kasiski examination**
   - ✓ **Cryptanalysis by permutation**
   - ✓ **Brute force attack**
6. **Record your findings gained during the process.**
7. **Once you think you have broken the cipher, attempt to decrypt the original plaintext.**

UNIT 3

UNIT	WARM UP	READING	USE OF ENGLISH	LISTENING	SPEAKING	WRITING	REFLECTION
3.1. **Identification. Verification. Authentication. Authorisation. Accounting**	Students' background knowledge about identification, verification, authentication, authorisation, accounting	Identification – what is it? What is verification? What is authentication?	Language use in terms of the topic; expanding vocabulary using AI. Future tenses	AAA – Authentication, Authorisation, and Accounting	Speaking about the specifics of authentication, authorisation, verification, and identification	Writing definitions of terms; an opinion essay	Reflecting and synthesising
3.2. **Passwords**	Students' background knowledge about passwords	Passwords	Language use in terms of the topic. Future tenses	What's wrong with your pa$$w0rd?	Speaking about passwords and passphrases, password creation, storage, security, sharing, expiration	Writing recommendations how to create strong passwords, how to memorise passwords. Simplifying the text created by AI. Writing an opinion essay	Reflecting and synthesising
3.3. **Biometrics**	Students' background knowledge about biometrics	Biometrics	Language use in terms of the topic. Future tenses	What is Biometrics and How Safe is it?	Speaking about the work of biometrics, types of biometrics, examples of biometrics	Analysing for and against arguments created by AI. Writing a for and against essay	Reflecting and synthesising
3.4. **Security Tokens**	Activating students' background knowledge about security tokens	Security tokens	Language use in terms of the topic; expanding vocabulary using AI. Future tenses	Smart card introduction	Speaking about the specifics of token-based authentication; the ways of authentication tokens hacking; measures to prevent hacking of tokens authentication	Writing a blog entry	Reflecting and synthesising

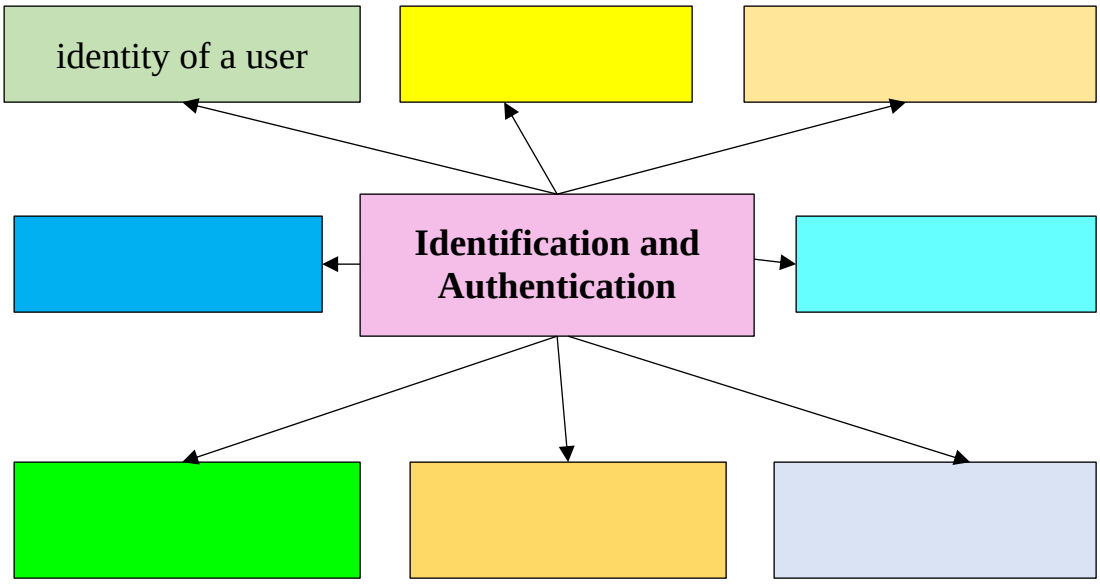
3.1. IDENTIFICATION. VERIFICATION. AUTHENTICATION. AUTHORISATION. ACCOUNTING

WARM UP

1. A. & B. Using your background knowledge, do the tasks according to your learning style (dominant or non-dominant modality).

1.1. *Visual Modality*

Work individually, then in small groups. Create a mind map with a central concept "*Identification and Authentication*". Start by brainstorming relevant terms related to identification and authentication. Clearly illustrate how each term relates to the central theme.



1.2. *Auditory Modality*

Work in a small group. Discuss the following questions.

1. What does the term *authentication* stand for?
2. What does the term *authorisation* stand for?
3. What types of authentication do you know?

4. What is the difference between authentication and authorisation?
5. What are the similarities between authentication and authorisation?
6. Which is the first, authentication or authorisation?
7. How is access control connected with authentication?

1.3. *Kinesthetic Modality*

Work in pairs. You've got a list of questions about authentication and authorisation. Fill in the table answering these questions. Then summarise information given in the table.

Questions	A	B
	Authentication	**Authorisation**
1. What is the purpose?		
2. How is it used?		
3. Can users see it?		
4. Can it be modified by the user?		

READING

You are going to read an article about identification, verification, and authentication.

2. **1. A. & B. Before reading, discuss the following quotation.**

"Trust, but verify."

Ronald Reagan

2. A. & B. Before reading, look at the following words and phrases, which have been taken from the text. In what context might they be mentioned? Use Merriam-Webster Dictionary if necessary.

Authentication, authorisation, access control, verification, credentials, entity, single-factor authentication, to corporate, to grant access, to gain access, inherence factor, stateless, attribute, privileges, preferences.

3. Read the text about identification, verification, and authentication. Five sentences have been removed. Choose which of the sentences fit into the gaps.

A	The use of multiple authentication factors to prove one's identity is based on the premise that an unauthorised actor is unlikely to be able to supply the factors required for access.
B	Software tokens are stored on a general-purpose electronic device (a desktop computer, laptop, PDA, mobile phone) and can be duplicated.
C	In online transactions, users identify themselves by sharing their name, email, or phone number, and as long as the information matches, they are accepted without verification.
D	Mutual authentication is found in two types of schemes: username-password based schemes and certificate based schemes, and these schemes are often employed in the Internet of Things (IoT).
E	According the the National Institute of Standards and Technology authentication is defined as "Authentication: verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system".

IDENTIFICATION. VERIFICATION. AUTHENTICATION

Identification is when someone claims to be a specific person, such as showing an ID, providing a name, or an email address. **1. _____.** This approach assumes the user is truthful, similar to just asking "Who are you?" and accepting the answer. To truly confirm identity, verification is needed.

Verification goes beyond asking "Who are you?" to confirm "Are you really who you say you are?" This requires high confidence, typically by validating multiple IDs, including at least one with a photo, like a driver's license, passport, or military ID. While some organisations aim for quick onboarding with minimal checks, thorough identity proofing ("vetting") often involves real-time validation of personal information, especially when the person isn't physically present.

In security, **authentication** is the process of verifying whether someone (or something) is, in fact, who (or what) it is declared to be. **2. _____ .**

The ways in which someone may be authenticated fall into three categories, based on what are known as **the factors of authentication**: something the user knows, something the user has, and something the user is. Security research has determined that for a positive authentication, elements from at least two, and preferably all three, factors should be verified. The four factors are:

− *knowledge* (something the user knows, e.g., a password, partial password, pass phrase, personal identification number (PIN), challenge response (the user must answer a question or pattern), security question));

− *ownership* (something the user possess, e.g., wrist band, ID card, security token, implanted device, cell phone with built-in hardware token, software token, or cell phone holding a software token);

− *inherence* (something the user is or does, e.g., fingerprint, retinal pattern, DNA sequence, signature, face, voice, unique bio-electric signals, or other biometric identifier);

− *location* (somewhere the user is, e.g., connection to a specific computing network or using a GPS signal to identify the location).

Multi-factor authentication is an electronic authentication method in which a computer user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something only the user knows), possession (something only the user has), and inherence (something only the user is). It protects the user from an unknown person trying to access their data such as personal ID details or financial assets.

3. _____ . If, in an authentication attempt, at least one of the components is missing or supplied incorrectly, the user's identity is not established with sufficient certainty and access to the asset (e.g., a building, or data) being protected by multi-factor authentication then remains blocked.

Knowledge. Knowledge factors, like passwords, are the most common form of authentication, requiring users to prove knowledge of a secret, such as a password, passphrase, or PIN. However, some secret questions, like "Where were you born?", are poor choices since they can be easily known or researched.

Possession. Possession factors, like keys, have long been used for authentication, with security tokens being a modern example. Disconnected tokens display a one-time password on a screen for manual entry, while connected tokens, such as card readers or USB tokens, are physically connected and transmit data automatically.

A software token (a soft token) is a type of two-factor authentication security device that may be used to authorise the use of computer services. **4. _____ .**

Hardware tokens, where the credentials are stored on a dedicated hardware device and therefore cannot be duplicated, absent physical invasion of the device.

Inherent. These are factors associated with the user, and are usually biometric methods, including fingerprint, face, voice, or iris recognition. Behavioral biometrics such as keystroke dynamics can also be used.

Location. Increasingly, location is becoming a fourth authentication factor, allowing users to log in with just a PIN when off the network or requiring a code from a soft token for added security, especially for office access. Network admission control systems grant access based on the network, such as Wi-Fi or wired, allowing users to move between offices and maintain consistent access levels.

Mutual authentication or two-way authentication (not to be confused with two-factor authentication) refers to two parties authenticating each other at the same time in an authentication protocol. It was previously referred to as "mutual entity authentication", as two or more entities verify the others' legality before any data or information is transmitted.

Mutual authentication is a desired characteristic in verification schemes that transmit sensitive data, in order to ensure data security. **5. _____**.

Borrowed from:
https://eng.libretexts.org/Courses/Delta_College/Information_Security/02%3A_Authenticate_and_Identify/2.1%3A_Identification;
https://eng.libretexts.org/Courses/Delta_College/Information_Security/02%3A_Authenticate_and_Identify/2.2%3A_Authentication
Borrowed and modified from:
https://eng.libretexts.org/Courses/Delta_College/Information_Security/02%3A_Authenticate_and_Identify/2.1%3A_Identification;
https://eng.libretexts.org/Courses/Delta_College/Information_Security/02%3A_Authenticate_and_Identify/2.2%3A_Authentication
Modified by https://deepai.org/chat/text-generator

4. A. & B. Read the text again and do the following tasks.

4.1. Fill in the missing information in statements 1–7.

1. _____ occurs when an individual asserts their identity, such as by presenting an ID, sharing a name, or providing an email address.
2. _____ extends beyond simply asking "Who are you?" to ensure "Are you truly who you claim to be?"
3. _____ involves confirming whether an individual or entity truly is who or what they claim to be.
4. If any component of an authentication attempt is missing or incorrect, the user's _____ cannot be reliably _____ , and access to the protected asset – such as a building or data – remains denied in multi-factor authentication systems.
5. A software token is a type of _____ authentication security device that may be used to authorise the use of computer services.
6. _____ biometrics such as keystroke dynamics can also be used.
7. _____ authentication refers to two parties authenticating each other at the same time in an authentication protocol.

4.2. Decide whether these sentences are *true or false*.

1. Identification involves claiming to be a specific person by showing an ID or providing personal information.
2. In online transactions, users are accepted without verification as long as their information matches.
3. Authentication is the process of verifying whether someone or something is who they claim to be.
4. According to the National Institute of Standards and Technology, authentication involves verifying the identity of a user, process, or device.

5. Knowledge factors include passwords, PINs, or security questions.
6. Possession factors are things the user has, like security tokens or ID cards.
7. Location is always a reliable authentication factor regardless of the user's environment.

5. A. & B. Match the terms (1–9) with their explanations (a–i).

1	Identification	**a**	the process of verifying whether someone / something is
2	Verification	**b**	something the user possess
3	Authentication	**c**	when two parties authenticate each other at the same time in an authentication protocol
4	Knowledge factors	**d**	something the user is or does
5	Ownership factors	**e**	the process of confirming the authenticity and accuracy of information, data, or identity
6	Inherence factors	**f**	a security process that requires a user to provide two or more authentication factors to access a system, network, or application
7	Location factors	**g**	somewhere the user is
8	Multi-factor authentication	**h**	the process by which someone claims to be a particular person
9	Mutual authentication	**i**	something the user knows

6. A. & B. Make a list of the five most important things that you have to remember about identification, verification, and authentication. Compare your list to your partner's. Which three are the most popular among the class?

USE OF ENGLISH

VOCABULARY

7. **A. Arrange the following words according to similar meaning:**

to permit, verification, accurate, criminals, to validate, false, precise, fake, to grant, to prove, access, to prevent, confirmation, to stop, right, fraudsters.

B. Give "strong" and "weak" synonyms to the words in italics. Then use any AI tool to fill in the third rubric of the table.

Phrases	Strong synonyms	Weak synonyms	Synonyms generated by AI
1) to *verify* someone's identity			
2) to *prevent* fraudsters			
3) identity "*proofing*" or "*vetting*"			
4) to *grant* access			
5) to *validate* the personal information			
6) the verification *requirements*			
7) devices *transmit* data automatically			
8) *a lack* of mutual authentication			

PHRASAL VERBS

8. **A. Fill in the correct particles. Then explain the phrasal verbs. See Appendix 2, which contains a list of relevant phrasal verbs.**

1. Before finishing the report, we need to **go** _____ all the data to make sure it is correct.
2. The company will **give** _____ temporary verification codes via email.
3. To prevent fraud, it's essential to **keep** _____ all user logins.
4. The IT team will **go** _____ the latest security protocols.
5. After many failed attempts to log in, she decided to **give** _____ and reset her password for the authentication process.
6. It's important for cybersecurity experts to **keep** _____ the latest threats to effectively protect sensitive data.
7. To simplify the onboarding process, we will **go** _____ the new verification procedures.
8. The increase in digital transactions is expected to **give** _____ innovative authentication methods that enhance security.

B. Replace the words or phrases in bold with the correct form of a phrasal verb using *give, go* and *keep*. Then, create three interconnected sentences that include any phrasal verbs with "give", "go" and "keep".

1. Before approving access, the security team will **examine** user's credentials to ensure authentication.
2. The IT department will **distribute** new identification badges to all employees to improve security measures.
3. It's important to **monitor** all user activities to detect any unauthorised access attempts during the verification processes.

4. We need to **check** the authentication procedures again to confirm that all understand the new requirements.
5. If a user fails to log in three times, they must **lock** their access for a period of time before trying again.
6. We need to **stay current with** the latest trends in identity verification technologies to ensure compliance with industry standards.
7. The team decided to **adopt** a multi-factor authentication system to enhance security protocols.
8. The rise of digital identities **has led to** innovative ways of verification.

GRAMMAR

9. A. & B. Put the verbs in brackets into the future simple, the future continuous, the future perfect, the future perfect continuous.

1. I think that I _____ **(implement)** a new identification system to enhance user security.
2. By the end of next week, we _____ **(complete)** our cyber security project in our company.
3. I believe that in the near future, employees _____ **(adopt)** multifactor authentication for accessing sensitive information.
4. By the end of the month, our system _____ **(support)** biometric identification methods.
5. By May, the IT department _____ **(finish)** conducting training sessions on best practices for verification.
6. This time next month, the team **_____ (conduct)** a complete review of user authentication processes.
7. By next year, the team _____ **(work)** on enhancing the identification protocol for over six months.

8. Next week at this time, our team _____ **(monitor)** the identification process to identify areas for improvement.
9. By the end of December, the users _____ **(adopt)** multifactor authentication practices for several months.
10. Probably, we _____ **(require)** users to set up multifactor authentication during their next login.

A. Choose the correct answer.

1. Mutual authentication is a process in which both the sending **and / as well as** receiving parties verify each **others / other's** identities to ensure that communication is secure.
2. The term "authenticate" refers to the procedure used **verifying / to verify** that users, devices or systems are genuine and **authorised / authorising** to access the network / system / resource.
3. Authentication techniques **includes / include** something you know, something you have, and something you are.
4. The authorisation process is different **of / from** the authentication process.
5. The **users / user's** identity was verified by the system.
6. The data **encrypted / was encrypted** with a digital signature to ensure **its / it's** authenticity.
7. Mutual authentication involves two types of schemes: username-password **basing / based** schemes and certificate **basing / based** schemes.
8. Mutual authentication **can / have to** prevent many adversarial attacks.
9. A software token is a type of **two-factors / two-factor** authentication security device that can be **using / used** for authorisation of use of computer services.
10. For most organisations, there is a need **to / for** a validation process of the personal information provided **by / with** the individual.

B. There is an odd word in some of the lines. Find it and write in the space provided.

Verification is being a critical process in information security.	1 being
It ensures the accuracy and integrity of data, with systems and	2
networks. It is involves verifying the identity of users, devices	3
and data to ensure what they are authentic and trustworthy. In the	4
case of encryption,verification is used to confirm of that the data	5
that is been decrypted is identical to the original data sent by the	6
sender. Verification can also be used to ensure that software	7 √
upgrades are legitimate and do not contain to malware.	8
Digital signatures also verify the one authenticity and integrity of	9
digital of documents and messages.	10

10. **A. Put the words into the correct form.**

Conventional computer systems **1)** _____ **(authentication)** users only at the initial log-in session, which can be the cause of a **2)** _____ **(critic)** security flaw. To resolve this problem, systems need continuous user **3)** _____ **(authenticate)** methods that **4)** _____ **(continuous)** monitor and authenticate users **5)** _____ **(base)** on some biometric trait(s). A study used behavioural biometrics based on **6)** _____ **(write)** styles as a continuous authentication method.

Recent research has shown the possibility of **7)** _____ **(use)** smartphones sensors and accessories **8)** _____ **(extract)** some behavioral attributes such as touch dynamics, keystroke dynamics and gait recognition. These attributes **9)** _____ **(know)** as behavioral biometrics and could be used to verify or identify users **10)** _____ **(implicit)** and **11)** _____

(continuous) on smartphones. The authentication systems that **12) _____ (build)** based on these behavioral biometric traits are known as active or continuous authentication systems.

Borrowed and modified from: https://en.wikipedia.org/wiki/Authentication

B. Complete the sentences.

Authorisation is the function of specifying **1)** _____ rights / privileges to resources, which is related to general information **2)** _____ and computer security, and to access control in particular. More formally, "to authorise" is to define an **3)** _____ policy. For example, human resources staff are normally **4)** _____ to access employee records and this policy is often formalised as access control rules in a computer **5)** _____. During operation, the system uses the access control rules to decide whether access requests from (authenticated) consumers shall be **6)** _____ (granted) or **7)** _____ (rejected). Resources include individual **8)** _____ or an item's data, computer programs, computer devices and functionality provided by computer **9)** _____. Examples of consumers are computer **10)** _____, computer software and other hardware on the computer.

Borrowed and modified from: https://en.wikipedia.org/wiki/Authorization

LISTENING

You are going to watch a video that explores authentication, authorisation, and accounting.

11. A. & B. Before watching a video, check if you know the meaning of the words and phrases. Use Merriam-Webster Dictionary if necessary.

Verify, identity, the backbone of online data protection, to explore, granting access to information or resources, a verification code on your phone, your data is a treasure chest, a gatekeeper, discretion, a more rigid and policy-driven approach, manifold, do not overstep their boundaries, to handle current and future demands, mandatory, to navigate and protect our online presence.

12. Watch the video "AAA – Authentication, Authorisation, and Accounting". Then answer the questions.

1. What is the "invisible fortress" mentioned in the text? What are its three main components?
2. What is the purpose of authentication in online data protection?
3. What are the three key factors of authentication? How do they work together?
4. What is multi-factor authentication, and why is it important?
5. Why is it crucial to have a strong lock on your digital data? What does it depend on?
6. What is authorisation, and how does it work in the digital world?
7. What are the three main types of authorisation? How do they differ?
8. How does accounting work? What is its role in online data protection?
9. What are the purposes of accounting? How does it help in authorisation control and resource planning?
10. Why is understanding the AAA crucial in navigating and protecting our online presence?

13. Watch the video again. Do the following tasks.

13.1. Fill in the missing information in statements 1–10.

1. Invisible fortress involves such components as: _____.
2. Authorisation determines what we're allowed to do, controlling our _____.
3. "Something you are" is the most personal and hardest to _____.
4. These factors can work alone or _____.
5. Authentication is like the lock on that _____.
6. Discretionary access control allows the owner of the information or resource to personally decide who _____.
7. Access permissions are assigned by a central authority based on multiple factors such as the _____ and the data's classification.
8. In the role-based access control model, access rights are based on the _____ have within the system.
9. Enter accounting is the unsung hero that diligently keeps tabs on everything that transpires once _____.
10. Accounting is a final component, maintaining a record of user activities and _____.

13.2. Decide whether these sentences are *true* or *false*.

1. The invisible fortress is a physical structure.
2. The three main components of the invisible fortress are authentication, authorisation, and communication.
3. Authentication verifies our identity and ensures we are who we claim to be.
4. Multi-factor authentication uses only two of the three authentication factors.
5. There are four main types of authorisation.
6. Authorisation determines what we can do after our identity has been authenticated.

7. Authorisation controls access using methods like discretionary, mandatory, or role-based access control.
8. Accounting keeps track of what we do and logs our activities for further analysis.
9. Accounting is responsible for controlling access to resources.
10. Understanding the AAA is crucial to navigate and protect our online presence effectively.

SPEAKING

14. **A. Work in pairs. A cybersecurity conference, where a panel of experts is discussing online security. The question from the audience: What is the difference between authentication and authorisation? Make up a dialogue and role play it. Your dialogue should include at least 5–6 exchanges per each participant. Be creative! Remember to keep the tone respectful!**

A	B
1. Let's start with the first question from the audience: What's the difference between authentication and authorisation? It's a great question! Authentication is ….	1. That's right. Authentication is like the "Who are you?" question. Once you've authenticated …
2. That's right. Authentication is like …..	2. ……..
3. …….	3. …….
4. …….	4. ……
5. …….	5. ……
6. ...…..	6. …….

B. Work in pairs. For your ESP lesson, make up a dialogue about the difference between authentication, authorisation, verification, and identification. Then, role play it. Your dialogue should include at least 7–8 exchanges per each participant. Be creative! Remember to keep the tone respectful!

15. **A. You are asked to choose one of the topics and prepare a talk: 1) the role of identification in cyber security; 2) the role of authentication in cyber security; 3) the role of verification in cyber security; 4) the role of authorisation in cyber security. Use information from reading and listening sections. Follow the stages: introduction, main body, conclusions.**

B. You are asked to prepare a presentation on one of the topics:

1. How are fake identities changing the face of authentication?
2. How is social media redefining identity and verification?
3. The evolution of authentication.
4. The unseen struggle for digital identity and authorisation.

Follow a clear structure, including an introduction, a main body, and conclusions.

WRITING

16. **Work in small groups. Write a definition of terms: *identification, authentication, verification, and authorisation*.**

A. Create definitions that are appropriate for individuals with no background in information security. Your definitions should use simple language and relatable examples.

B. Create definitions for your groupmates within your graduate programme. These definitions should include specific terminology relevant to your field of study.

After writing the definitions, pair up with another group. Share your definitions and discuss how each definition meets the specific needs of your target audience. Consider aspects such as complexity, terminology, and the use of examples that are relevant to each group's background.

17. **To participate in the *Opinion Essay Contest*, you have to choose one of the topics and write an opinion essay.**

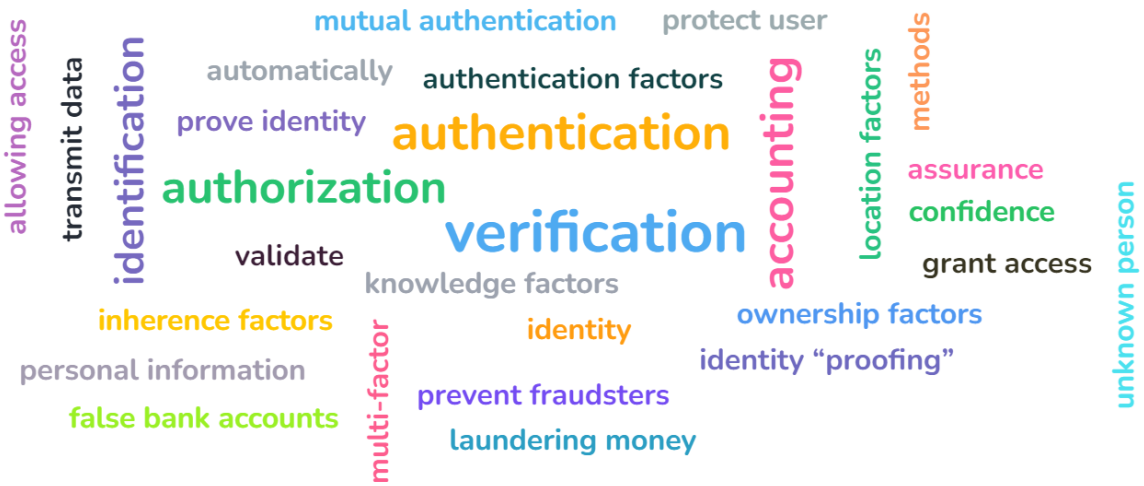
A. Write an opinion essay (160–170 words): "The role of authentication and authorisation in the digital world".

B. Write an opinion essay (180–200 words): AAA as a powerful trio in protecting our online data.

Follow the stages: introduction, main body, conclusions.

REFLECTION AND SYNTHESIS

18. **You have completed this unit. This word cloud can help you to reflect on and synthesise the key concepts from the topic. Focus on the most important terms and ideas that stood out to you. Using the word cloud as a visual tool, you have to illustrate your understanding.**



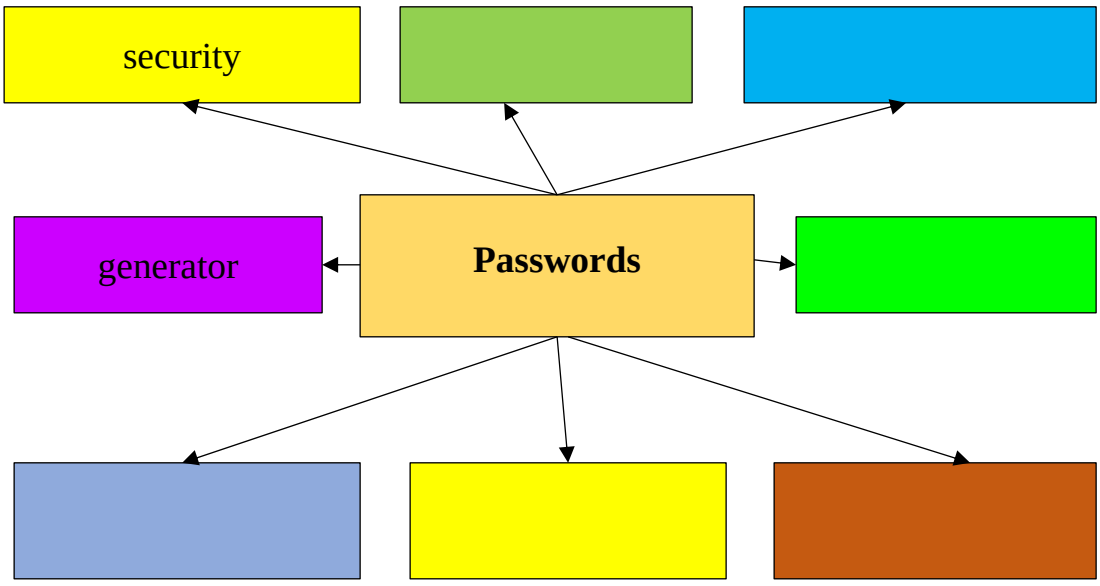
3.2. PASSWORDS

WARM UP

1. **A. & B. Using your background knowledge, do the tasks according to your learning style (dominant or non-dominant modality).**

1.1. *Visual Modality*

Work individually, then in small groups. Create a mind map with a central concept "*Passwords*". Start by brainstorming relevant terms related to passwords. Clearly illustrate how each term relates to the central concept.



1.2. *Auditory Modality*

Discuss the following questions.

1. Why is the topic "*Passwords*" important for information security?
2. Have you ever had a password guessed or hacked? What did you do?
3. What is the difference between the terms "*password*" and "*password phrase*"?
4. What does the notion "*strong password*" mean?

5. Why do people continue to use "*weak passwords*"?
6. How fast can a password be cracked?
7. What problems do people have with passwords?
8. What recommendations can you give to remember passwords?

1.3. *Kinesthetic Modality*

Work in a group. Conduct a survey among your groupmates. Then collect responses and analyse them. Present the results to your group, outlining the key trends.

1. Do you use different passwords for various websites?
    a) every time
    b) often
    c) never
2. How often do you change your passwords?
    a) once per month
    b) every three months
    c) every six month
    d) every year
    e) use the same password for a long time
3. Your password is _____ characters long.
    a) 8
    b) 16
    c) more than 16
4. Do you share your passwords?
    a) yes (if the situation requires)
    b) no

5. Is complexity in terms of passwords for _____?
    a) a human being
    b) a computer
6. Do you use a real word in any language in your password?
    a) yes
    b) no
7. Do you write your passwords?
    a) yes
    b) no
8. To be secure, I prefer using _____ .
    a) a password
    b) biometrics
    c) both

READING

You are going to read an article about passwords.

2.

1. A. & B. Before reading, discuss the following quotation.

"If you've never mistyped your password, it isn't complex enough."

D. Clarence Snyder

2. A. & B. Before reading, look at the following words and phrases, which have been taken from the text. In what context might they be mentioned? Use Merriam-Webster Dictionary if necessary.

Threats, sniffers, bystanders, impose, to be subjected, infeasible, consecutive, mitigation, compromised, snooper, password cracking tools, iterated, adjustable cost.

3. **A. & B. Read the texts about passwords. Six sentences have been removed. Choose which of the sentences fit into the gaps.**

A	Similarly, the more stringent the password requirements, such as "have a mix of uppercase and lowercase letters and digits" or "change it monthly", the greater the degree to which users will subvert the system.
B	Employing password managers to securely store and generate complex passwords, enforcing strong password policies, and educating users about social engineering and phishing threats are also crucial.
C	These passwords combine visual, behavioral, and contextual elements – such as personalised gestures, images, or patterns – creating a more complex and difficult-to-crack security layer.
D	A memorised secret consisting of a sequence of words or other text separated by spaces is sometimes called a **passphrase**.
E	Other scenarios include cracking, where attackers use password files to try all possible combinations, sniffing, where unencrypted data is intercepted over the internet, and guessing, where users choose weak or predictable passwords based on familiar objects or brands.
F	Graphical passwords can improve both usability and security, particularly against brute-force attacks, but they require careful design to mitigate vulnerabilities such as shoulder surfing.

PASSWORDS

A **password**, sometimes called a **passcode**, is secret data, typically a string of characters, usually used to confirm a user's identity. Despite its name, a password does not need to be an actual word; indeed, a non-word (in the dictionary sense) may be harder to guess, which is a desirable property of passwords. **1.** _____ . A passphrase is similar to a password in usage, but the former is generally longer for added security.

The easier a password is for the owner to remember generally means it will be easier for an attacker to guess. However, passwords that are difficult to remember may also reduce the security of a system because (a) users might need to write down or electronically store the password, (b) users will need frequent password resets and (c) users are more likely to re-use the same password across different accounts. **2.** _____ . Others argue longer passwords provide more security (e.g., entropy) than shorter passwords with a wide variety of characters.

Password attacks are a significant threat to online security, allowing cybercriminals to gain unauthorised access to accounts or systems. Common types of password attacks include:

- **Brute-force attack –** tries an enormous number of password combinations until the password is found;
- **Dictionary attack –** uses pre-existing lists of common words, phrases, leaked passwords to try and match them with the target account;
- **Phishing –** tricks users into revealing their passwords through fake emails, websites, or messages that appear legitimate;
- **Credential stuffing** – uses stolen login credentials from previous breaches to access multiple accounts, often exploiting the same password across different sites;
- **Keylogging** – records keystrokes to capture passwords and other sensitive information as users type them in;
- **Password spraying** – attempts a few common passwords across many different accounts to avoid account lockout;
- **Man-in-the-Middle (MitM)** – involves intercepting communication between a user and a server to steal sensitive data.

Common scenarios involving the exposure of passwords usually occur as a result of physical security breaches, such as the installation of keyloggers or the theft of hardware, which compromises all data. **3.** _____ .

Effective strategies for preventing password-related attacks entail implementing strong and unique passwords for each account, utilising multi-factor authentication (MFA) and regularly updating passwords. **4.** _____ . Additionally, securing communications with encryption protocols like SSL / TLS, monitoring login activities for suspicious behavior, and conducting periodic security audits help identify and address potential weaknesses.

Besides traditional passwords that include symbols, letters, and numbers, researchers are increasingly advocating for the use of graphical passwords – an authentication method where users select images, patterns, or visual elements instead of relying solely on text. This approach capitalises on human memory for images, making it easier to recall complex passwords while maintaining strong security. Common types include click-based passwords, where users select specific points within an image, and pattern-based passwords, where users draw a shape or pattern. **5.** _____ .

3D passwords represent an advanced security paradigm that enhances traditional systems by integrating multi-dimensional authentication factors. **6.** _____ . By leveraging multiple verification layers, 3D passwords offer a more robust defense against unauthorised access, making them a promising innovation in cybersecurity for safeguarding sensitive information.

Borrowed and modified from: https://deepai.org/chat/text-generator, https://en.wikipedia.org/wiki/Password, https://eng.libretexts.org/Courses/Delta_College/Information_Security/02:_Authenticate_and_Identify/2.3:_Authentication_Methods_-_Password

4. **A. & B. Read the text again and do the following tasks.**

4.1. Fill in the missing information in statements 1–7.

1. A _____ is a sequence of words or a string of characters used to secure access to a system or account, often longer and more complex than a traditional password.

2. As password requirements become more strict, like needing a combination of _____ and _____ letters and digits or requiring monthly changes, users are more likely to find ways to bypass or undermine the system.
3. _____ – involves intercepting communication between a user and a server to steal sensitive data.
4. Physical security _____, such as the installation of _____ or hardware theft, can compromise all data by gaining unauthorized access to sensitive information.
5. An effective strategy for preventing password-related attacks is to use password _____, which securely store and generate complex, unique passwords for each account.
6. _____ passwords involve users selecting specific points within an image.
7. 3D passwords integrate visual, behavioral, and _____ elements to create a more secure and multi-faceted _____ method.

4.2. Decide whether these sentences are *true* and *false*.

1. A password, also called a passcode, is secret data used to verify a user's identity.
2. Easier-to-remember passwords are generally easier for attackers to guess.
3. Complex password requirements can lead users to reuse passwords or write them down, reducing security.
4. Brute-force attacks systematically try many password combinations until the correct one is found.
5. Phishing involves intercepting communication between a user and a server to steal data.
6. Using stolen login credentials from previous breaches in multiple accounts is called credential stuffing.
7. Graphical passwords, such as click-based or pattern-based passwords, leverage human memory for images and patterns.

5. A. & B. In pairs, select one word from the provided list. Student A asks the questions below, putting the chosen word into each question, while Student B responds using that word. You may skip any questions that do not apply. After completing the questions, switch roles and repeat the activity with a different word. See the example below.

Password, attacker, attack, passphrase, reset, unique, protection, limit, weak, interception, subvert, leak, fake, mitigate, vulnerability.

1. What does _____ mean?
2. What is the plural / singular of _____?
3. What is the synonym of _____?
4. What is the opposite of _____?
5. What is the noun for _____?
6. What is the verb for _____?
7. What is the adjective for _____?
8. What is the adverb for _____?
9. Can you give _____ collocations?
10. How to use _____ in a sentence?
11. What is the translation for _____?

For example:

The chosen word is "project".

Student A: "What does project mean?"

Student B: "Project" is a planned set of activities or tasks intended to achieve a specific goal.

Student A: "What is the plural of project?"

Student B: "Projects."

6. **A. & B. Make a list of the five most important things that you have to remember about passwords. Compare your list to your partner's. Which three are the most popular among the class?**

USE OF ENGLISH

VOCABULARY

7. **A. Complete the sentences. Use: *claimant, passcode, identity, infer, verifying, password, characters, authentication, verifier*.**

A password, sometimes called a **1)** _____, is a memorised secret, typically a string of **2)** _____, usually used to confirm a user's **3)** _____. Using the terminology of the NIST Digital Identity Guidelines, "the secret is memorised by a party called the **4)** _____ while the party **5)** _____ the identity of the claimant is called the **6)** _____. When the claimant successfully demonstrates knowledge of the **7)** _____ to the verifier through an established **8)** _____ protocol, the verifier is able to **9)** _____ the claimant's identity".

Borrowed and modified from: https://en.wikipedia.org/wiki/Password

B. Complete the sentences.

Passwords have been used with **1)** _____ since the earliest days of computing. The Compatible Time-Sharing System (CTSS), an operating **2)** _____ introduced at MIT in 1961, was the first computer system to implement password **3)** _____. CTSS had a LOGIN command that **4)** _____ a user password. "After typing PASSWORD, the system turns off the printing mechanism, if possible, so that the user may type in his password with **5)** _____". In the early 1970s, Robert Morris developed a system of

storing **6)** _____ passwords in a hashed form as part of the **7)** _____ operating system. The system was based on a simulated Hagelin rotor crypto **8)** _____, and first appeared in 6th Edition Unix in 1974. A later version of his algorithm, known as crypt(3), used a 12-bit salt and invoked a modified form of the DES **9)** _____ 25 times to reduce the **10)** _____ of pre-computed dictionary attacks.

Borrowed and modified from: https://en.wikipedia.org/wiki/Password

IDIOMS

8. **A. Match the idioms in bold to their equivalents. Have you got any similar idioms / phrases in your language?**

Creating an easy opportunity for hackers to gain access, make an additional effort beyond what is expected or required in order to achieve a goal, protect your passwords, don't use the same password for multiple accounts, update passwords frequently.

1. To keep your accounts safe, remember to **lock up your secrets** and use complex passwords.
2. When I delt with passwords for different accounts, I decided **never** to **put all my keys in one basket**.
3. To enhance security I have decided to **change the locks regularly** in terms of password usage.
4. To secure the accounts, make sure to **go the extra mile** by using complicated passwords.
5. Using weak passwords is like **leaving the front door wide open** for hackers.

B. Fill in the blanks using the idioms from the list below. You may need to change the verb tense.

Lock up your secrets, never put all my keys in one basket, change the locks regularly, go the extra mile, leaving the front door wide open.

Managing digital security is a constant battle against complacency. When I first started my tech firm, I treated our security protocols as **1)** _____, but after a minor data breach, I realised I needed to **2)** _____ with much more rigor.

I decided to **3)** _____ by implementing multi-factor authentication and biometric scans for every employee. I also taught my team a vital lesson in digital hygiene: **4)** _____. We stopped using a single master password for our databases and instead distributed encrypted fragments across different secure servers.

Despite these advanced measures, we knew that human habits are often **5)** _____. To prevent old credentials from being exploited by hackers **6)** _____ with our firewall, we established a strict policy to **7)** _____. We understood that neglecting a simple update was essentially **8)** _____ for any cybercriminal to walk right in.

Borrowed and modified from: https://gemini.google.com/

GRAMMAR

9. **A. & B. Put the verbs into the correct future tenses: the future simple, the future continuous, the future perfect, the future perfect continuous.**

1. This time next week, Sam _____ **(create)** a password protection policy for his company.
2. I believe that in future people _____ **(use)** passwords as well password phrases.

3. By the end of the week, I _____ **(finish)** creating strateges to enhance password protection.
4. This time next month, our company _____ **(provide)** a password hygiene training course.
5. I don't think that he _____ **(create)** a strong password.
6. By the end this week, he _____ **(use)** the same password for over six months.
7. I think I _____ **(use)** passphrases instead of passwords in future.
8. By the end of the year, our entire company _____ **(stop)** using pictures as passwords.
9. By the end of the year, our company _____ **(use)** pictorial passwords for three months.

A. Choose the appropriate option.

The **1)** _____ **(easy / easier)** a password **2)** _____ **(was / is)** for the owner to remember generally means it will be **3)** _____ **(easiest / easier)** for an attacker to guess. However, passwords that are difficult **4)** _____ **(to remember / remembering)** may also reduce the security of a system because *(a)* users might need to write down or **5)** _____ **(electronic / electronically)** store the password, *(b)* users will need **6)** _____ **(frequent / frequency)** password resets and *(c)* users are more likely to re-use the same password across different accounts. **7)** _____ **(Similar / Similarly)**, the more stringent the password requirements, such as "have a mix of uppercase and lowercase letters and digits" or "change it monthly", the **8)** _____ **(great / greater)** the degree to which users will subvert the system. Others argue **9)** _____ **(longer / long)** passwords provide more security (e.g., entropy) than shorter passwords with a wide variety of characters.

B. Put the words into the correct form.

In The Memorability and Security of Passwords, Jeff Yan et al. examine the effect of advice **1)** _____ **(give)** to users about a good **2)** _____ **(choose)** of password. They found that passwords based on **3)** _____ **(think)** of a phrase and **4)** _____ **(talk)** the first letter of each word are just as **5)** _____ **(memory)** as naively selected passwords, and just as hard to crack as **6)** _____ **(random)** generated passwords.

7) _____ **(Combine)** two or more unrelated words and **8)** _____ **(alter)** some of the letters to special characters or numbers is another good method, but a single dictionary word is not. **9)** _____ **(Have)** a personally designed algorithm for **10)** _____ **(generate)** obscure passwords is another good method.

Borrowed and modified from:
https://eng.libretexts.org/Courses/Delta_College/Information_Security/02:_Authenticate_and_Identify/2.3:_Authentication_Methods_-_Password

10. **A. Choose the correct answer.**

1. Your password _____ be at least 12 characters long including uppercase and lowercase letters, numbers, and special characters.
    a) must
    b) should
    c) ought to
2. The company's password policy requires all employees _____ their passwords _____ 60 days.
    a) change, once
    b) changing, twice
    c) to change, every
3. A weak password is one that is easily _____ by hackers.
    a) guessed
    b) found
    c) discovered

4. You should never share your password with anyone, _____ friends and family, as it is a compromise to your online security.
    a) included
    b) include
    c) including
5. Passwords that are similar to your birthdate _____.
    a) consider weak
    b) are considered weak
    c) is considered average
6. I have accidentally typed in my password _____ and I _____ out of my account.
    a) incorrectly, have been locked
    b) incorrect, have locked
    c) incorrectly, locked
7. He tried to reset his password online but _____ his old one, so he _____ to contact customer support for help.
    a) forget, has
    b) forgot, had
    c) forgot, must
8. IT specialists recommend _____ a passphrase instead of a traditional password _____ it is more secure and harder to guess.
    a) to use, because of
    b) to use, because
    c) using, because

9. _____ a unique password for each account, I always use a password manager that _____ random combinations of letters and numbers.
    a) To create, generates
    b) Create, am generating
    c) To create, have generated
10. The _____ way to stay safe online is to use strong, unique passwords _____ each account and keep them confidential.
    a) best, for
    b) good, of
    c) best, of

B. Complete the sentences.

Asking users to remember a password consisting **1)** _____ a "mix of uppercase and **2)** _____ characters" is similar to asking them **3)** _____ a sequence of bits: hard to remember, and only a little **4)** _____ harder to crack (e.g. only 128 times harder to crack for 7- **5)** _____ passwords, less if the user simply capitalises one of the letters). Asking users **6)** _____ use "both letters and digits" will often lead to easy-to-**7)** _____ substitutions such as "E" → "3" and "I" → "1", substitutions which are well known to **8)** _____. Similarly typing the password one keyboard row **9)** _____ is a common trick known to attackers.

In 2013, Google released a list of the most **10)** _____ password types, all of which are considered insecure because they are too easy to guess:

- the name of a pet, child, family **11)** _____;
- significant anniversary dates and **12)** _____;
- birthplace;

- name of a favourite holiday;
- something related to a favourite **13)** _____ team;
- the word "**14)** _____".

Borrowed and modified from:
https://eng.libretexts.org/Courses/Delta_College/Information_Security/02:_Authenticate_and_Identify/2.3:_Authentication_Methods_-_Password

LISTENING

You are going to watch a video about passwords.

11. A. & B. Before watching a video, check if you know the meaning of the words and phrases. Use Merriam-Webster Dictionary if necessary.

Unusable privacy and security, frustration, entropy, requirements, rules of thumb, to figure out, valid, to affiliate, feedback, cracking passwords, quilts.

12. Watch the video "What's wrong with your pa$$w0rd?". Then answer the questions.

1. What is the main goal of the talk?
2. What password requirements are mentioned? What do you think about them?
3. What is information entropy?
4. To what conclusions did the scientists come after asking 470 students, faculty and staff?
5. How do bad guys crack passwords?
6. What is a password meter?
7. What conclusions were made about pass phrases?
8. Do you agree with Lorrie Faith Cranor that when we make passwords, we think about things that make us happy? Give your reasons.

13. A. & B. Watch the video again and do the following tasks.

13.1. Fill in the missing information in statements 1–10.

1. At the end of 2009, you couldn't use the same character more than _____, and it wasn't allowed to be in a dictionary.
2. _____ is a complicated term, but basically it measures the strength of passwords.
3. 80 percent of people said they were _____ their password.
4. We collected 5,000 passwords, and we gave people a bunch of different _____ to create passwords with.
5. According to the survey, there's only a _____ that people are actually using in their passwords.
6. The scientists found that people were really frustrated by the very complex passwords, and the long passwords were a lot more _____, and in some cases, they were actually even _____ than the complex passwords.
7. We decided to do a study to find out whether these _____ actually work.
8. People were not really better at remembering the pass phrases than these _____ passwords, and because the pass phrases are longer, they took longer to type and people _____ while typing them in.
9. The passwords created by people affiliated with the school of computer science were actually 1.8 times _____ than those affiliated with the business school.
10. The speaker made a quilt. It's called "_____".

13.2. Decide whether these sentences are *true* or *false*.

1. The new password policy at Carnegie Mellon required passwords to have at least 16 characters.
2. The National Institute of Standards and Technology has guidelines for

measuring password strength.

3. The National Institute of Standards and Technology has a lot of data on passwords.
4. The researchers used Amazon Mechanical Turk to collect 5,000 passwords for their study.
5. The researchers found that long passwords were generally stronger than complex passwords.
6. The dancing bunny password meter was not effective.
7. Most password meters on the Internet are too soft and give false positives too easily.
8. Pass phrases are generally considered to be a good way to improve password security.
9. The researchers analysed real passwords from 25,000 CMU students, faculty, and staff for their study.
10. The final thought of the speaker is that creating a password based on things that make us happy, makes it easier for others to guess our password.

SPEAKING

14. **A. Work in pairs. As information security experts, you are discussing the differences between passwords and passphrases as well as various apps that generate passwords. Role play this conversation, outlining the advantages and disadvantages of each option. Your dialogue should include at least 5–6 exchanges per each participant. Be creative! Remember to keep the tone respectful!**

A	B
1. Well, I've been using a passphrase instead of a traditional password.	1. A passphrase? What is the difference between passwords and passphrases?
2. …..	2. …….
3. …….	3. …….
4. …….	4. ……
5. …….	5. ……
6. ……	6. ……

B. Work in pairs. As information security experts, you are talking about picture passwords. Role play this conversation, covering the following aspects: 1) definition of a picture password; 2) the specifics of work; 3) the main advantages and disadvantages of a picture passwords. Your dialogue should include at least 7–8 exchanges per each participant. Be creative! Remember to keep the tone respectful!

15. **A. During a cybersecurity training session for Google employees aimed at improving security, you are going to discuss the topics below. Choose one of the topics and prepare a brief talk (2–3 minutes), structured as follows: introduction, main body, conclusions.**

1. Password creation **(**creation of a strong password; common password creation mistakes and their avoidance; guidelines for creating passwords).
2. Password storage (different methods for storing passwords, e.g. password manager, written down, memorised); the pros and cons of each method; your experience in keeping your passwords safe).
3. Password security (common password security threats; protection of your

passwords from these threats; practices for keeping your passwords secure).

4. Password sharing (sharing a password with someone else (e.g. spouse, business partner; safe sharing a password with someone).
5. Password expiration (changing your passwords; frequency of changing your passwords).

B. In the workshop with a focus on cybersecurity, you are asked to comment on one of the quotations.

1. "I changed my password everywhere to "incorrect". That way when I forget it, it always reminds me, "Your password is incorrect." *Unknown Author.*
2. "The whole notion of passwords is based on an oxymoron. The idea is to have a random string that is easy to remember. Unfortunately, if it's easy to remember, it's something nonrandom like "Susan". And if it's random, like "r7U2*Qnp", then it's not easy to remember." *Bruce Schneier*.
3. "By now, you've heard endless warnings about the risk of short, trivial passwords. There's a good chance you ignore them." *Barton Gellman.*
4. "Choosing a hard-to-guess, but easy-to-remember password is important!" *Kevin Mitnick.*
5. "Treat your password like your toothbrush. Don't let anybody else use it, and get a new one every six months." *Clifford Stoll.*
6. "I speak the password primeval; I give the sign of democracy." *Walt Whitman.*
7. "It seems that "national security" is the root password to the Constitution. As with any dishonest superuser, the best countermeasure is strong encryption." *Phil Karn.*

The quotes are borrowed from: https://www.azquotes.com/quotes/topics/passwords.html

WRITING

16. **A. Provide your friend with a list of effective recommendations for creating strong passwords. Write at least 5–6 tips.**

B. Create a list of effective recommendations for remembering passwords, focusing on techniques that improve recall and security. Suggest clear and practical tips that can be easily implemented to help users manage their passwords more effectively.

17. **A. & B. Work with AI.**

Read the text about passphrases created by AI. Replace complex words and phrases with simpler alternatives, and break long sentences into shorter ones for better clarity.

"Passphrases are a type of authentication method that enhances security by using a sequence of words or a memorable phrase instead of a traditional password. They are typically longer and can include spaces, punctuation, and a mix of letters, making them harder to crack while still being easier for users to remember. Passphrases are particularly effective against brute-force attacks and can significantly reduce the risk of unauthorised access to accounts. To maximise their strength, it's advisable to create unique passphrases that incorporate personal significance and a variety of character types."

AI Text Generator, https://deepai.org/chat/text-generator

A. For an *Opinion Essay Contest*, write an essay "Passwords: a necessary evil or a modern threat?" (150–170 words), structured as follows: introduction, main body, conclusions.

Discuss the impact of password culture on personal and professional security, propose solutions to balance security and usability in the era of "password fatigue". Follow the stages: introduction, main body, conclusions.

B. Write an opinion essay (180–200 words) on the topic "3D password: advantages and disadvantages", structured as follows: introduction, main body, conclusions.

REFLECTION AND SYNTHESIS

18. **You have completed this unit. This word cloud can help you to reflect on and synthesise the key concepts from the topic. Focus on the most important terms and ideas that stood out to you. Using the word cloud as a visual tool, you have to illustrate your understanding.**

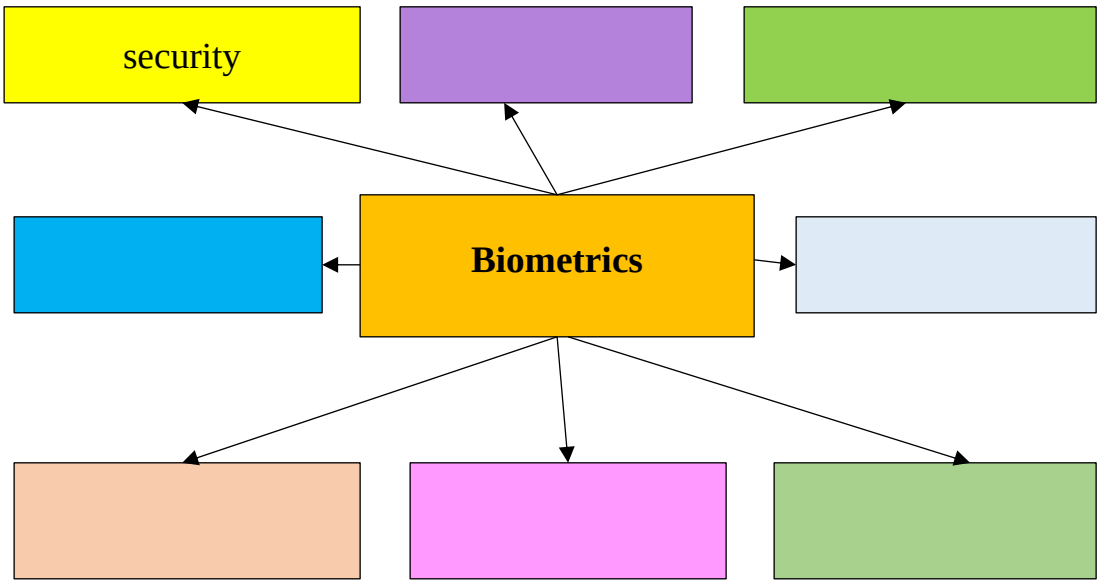
3.3. BIOMETRICS

WARM UP

1. **A. & B. Using your background knowledge, do the tasks according to your learning style (dominant or non-dominant modality).**

1.1. *Visual Modality*

Work individually, then in small groups. Create a mind map with a central concept "*Biometrics*". Start by brainstorming relevant terms related to biometrics. Clearly illustrate how each term relates to the central theme.



1.2. *Auditory Modality*

Discuss the following questions.

1. What does the term "biometrics" mean?
2. Do you use biometric recognition methods? Why?
3. What types of biometrics do you know?
4. What type of biometrics is mostly used nowadays? Give your reasons.
5. Is it possible to steal biometric data?

1.3. *Kinesthetic Modality*

Work in pairs. Identify the advantages and disadvantages of biometrics. Fill in the table with your findings. Then present your findings to the class.

Advantages of biometrics	Disadvantages of biometrics
1. ……	1. ……
2. ……	2. ……
3. ……	3. ……
4. ……	4. ……
5. ……	5. ……

READING

You are going to read an article about biometrics.

2

1. A. & B. Before reading, discuss the following quotation.

"Biometrics is certainly the most secure form of authentication, … It's the hardest to imitate and duplicate."

Avivah Litan

2. A. & B. Before reading, look at the following words and phrases, which have been taken from the text. In what context might they be mentioned? Use Merriam-Webster Dictionary if necessary.

Distinctive, measurable, recognition, keystroke, reliable in verifying identity, the ultimate use of this information, universality, uniqueness, permanence, robustness, circumvention, to generate the genuine and impostor scores, enrollment.

3. **A. & B. Read the text about biometrics. Three paragraphs of the text have been removed. Choose which of the paragraphs fit into the gaps.**

A	During the enrollment phase, the template is simply stored somewhere (on a card or within a database or both). During the matching phase, the obtained **template** is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Hamming distance). The matching program will analyse the template with the input. This will then be output for a specified use or purpose (e.g. entrance in a restricted area), though it is a fear that the use of biometric data may face mission creep.
B	Biometric identifiers are the **distinctive**, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorised as physiological versus behavioral characteristics. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odor / scent. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, keystroke, signature, behavioral profiling, and voice. Some researchers have coined the term behaviometrics to describe the latter class of biometrics.
C	Second, in identification mode, the system compares a biometric sample against a database to establish the individual's identity, succeeding if the **comparison** falls within a set threshold. It can be used for "positive recognition", where no prior information is needed, or for "negative recognition", to verify if the person is who they deny being, a task uniquely suited to biometrics since other methods like passwords or keys are ineffective.

BIOMETRICS

Biometrics is the term that means body measurements and calculations related to human **characteristics**. Biometrics authentication (or realistic authentication) is used in computer science as a form of identification and **access control**. It is also used to identify individuals in groups that are under surveillance.

1. _____

More traditional means of access control include token-based **identification** systems, such as a driver's license or passport, and knowledge-based identification systems, such as a password or personal identification number. Since biometric identifiers are unique to individuals, they are more reliable in **verifying** identity than token and knowledge-based methods. However, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information.

Many different aspects of human physiology, chemistry or behavior can be used for biometric authentication. The selection of a particular biometric for use in a specific application involves a weighting of several factors. Jain et al. (1999) identified seven such factors to be used when assessing the suitability of any trait for use in biometric authentication.

1. **Universality** means that every person using a system should possess the trait.

2. **Uniqueness** means the trait should be sufficiently different for individuals in the relevant population such that they can be distinguished from one another.

3. **Permanence** relates to the manner in which a trait varies over time. More specifically, a trait with "good" permanence will be reasonably invariant over time with respect to the specific matching algorithm.

4. **Measurability** (collectability) relates to the ease of acquisition or measurement of the trait. In addition, acquired data should be in a form that permits subsequent processing and extraction of the relevant feature sets.

5. **Performance** relates to the accuracy, speed, and robustness of technology used.

6. **Acceptability** relates to how well individuals in the relevant population accept the technology such that they are willing to have their biometric trait captured and assessed.

7. **Circumvention** relates to the ease with which a trait might be imitated using an artifact or substitute.

Proper biometric use is very application dependent. Certain biometrics will be better than other based on the required levels of convenience and security. No single biometric will meet all the requirements of every possible application.

The block diagram illustrates the two basic modes of a biometric system. First, in verification (or authentication) mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be. Three steps are involved in the verification of a person. In the first step, reference models for all the users are **generated** and **stored** in the model database. In the second step, some samples are matched with reference models to generate the genuine and impostor scores and calculate the threshold. The third step is the testing step. This process may use a smart card, username or ID number (e.g. PIN) **to indicate** which template should be used for comparison. “Positive recognition” is a common use of the verification mode, “where the aim is to prevent multiple people from using the same identity”.

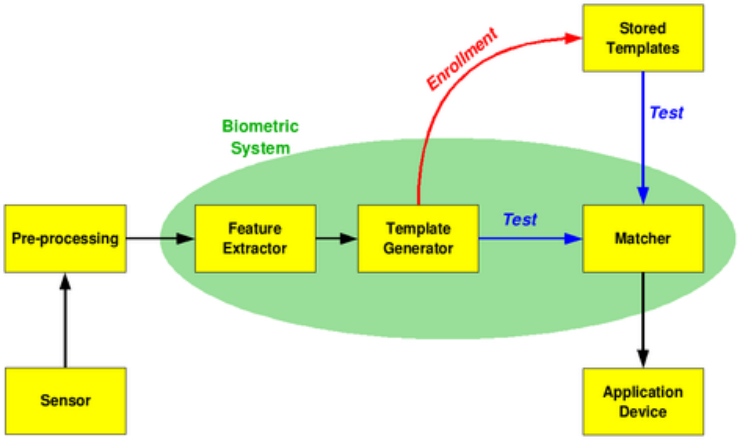


Figure 1. *Biometric System ("Biometric System" by Multiple Contributors, Wikipedia is licensed under CC BY-SA 3.0)*

2. _____

Enrollment is the initial process where biometric data is captured and stored, and subsequent uses involve comparing new data to this stored information. The system's security depends on protecting the storage and retrieval processes. The sensor gathers data, usually an image, which is then pre-processed to remove noise and artifacts. Next, important features are extracted to create a compact, relevant template, discarding unnecessary data to protect privacy and reduce size. Depending on the system, original biometric images may also be retained, such as PIV-cards in federal identity verification.

3. _____

In selecting a particular biometric, factors to consider performance, social acceptability, ease of circumvention and / or spoofing, robustness, population coverage, size of equipment needed and identity theft deterrence. The selection of a biometric is based on user requirements and considers sensor and device **availability**, computational time and **reliability**, cost, sensor size, and power consumption.

Borrowed and modified from:
https://eng.libretexts.org/Courses/Delta_College/Information_Security/02:_Authenticate_and_Identify/2.3:_Authentication_Methods_-_Password/2.3.2:_Authentication_Methods_-_Biometrics,
Biometrics is shared under a CC BY-SA license.
Modified by https://deepai.org/chat/text-generator

4. A. & B. Read the text again and do the following tasks.

4.1. Fill in the missing information in statements 1–10.

1. Biometrics authentication is also used to identify individuals in groups that are under _____.
2. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing _____, gait, keystroke, _____, behavioral profiling, and _____.
3. _____ relates to the ease of acquisition or measurement of the trait.
4. _____ relates to the ease with which a trait might be imitated using an artifact or substitute.
5. "_____ _____" is a common use of the verification mode, "where the aim is to prevent multiple people from using the same identity".
6. In _____mode the system performs a one-to-many comparison against a biometric database in an attempt to establish the _____ of an unknown individual.
7. The first time an individual uses a biometric system is called _____.
8. A _____ is a synthesis of the relevant characteristics extracted from the source.
9. During the _____ phase, the template is simply stored somewhere.
10. During the _____ phase, the obtained template is passed to a _____ that compares it with other existing templates, estimating the distance between them using any algorithm.

4.2. Decide whether these sentences are *true* or *false*.

1. Biometric authentication is used for both access control and identification.
2. Physiological characteristics include fingerprints and face recognition.

3. The collection of biometric identifiers raises privacy concerns about the ultimate use of this information.
4. Permanence refers to how much a biometric trait can change over time.
5. The verification mode performs a one-to-one comparison.
6. The testing step uses identifying information like a smart card or ID number.
7. Identification mode can be used for both positive and negative recognition.
8. Enrollment is the initial phase where biometric information is captured and stored.
9. The matcher compares the obtained template with existing templates to determine identity.
10. Factors like social acceptability and robustness are important in selecting a biometric system.

5. **A. & B. Cross the odd word out:**

1) fingerprint, palm veins, face recognition, gait;
2) driver's license, password, passport, USB token;
3) universality, stability, uniqueness, permanence;
4) time, feature extractor, template generator, matcher;
5) individual, biometric information, enrollment, solutions;
6) biometric technology, biometric duties, biometric engine, biometric application;
7) iris, retina, face, heartbeat;
8) hard to fake, easy to use, speed, privacy cocerns.

6. **A. & B. Make a list of the five most important things that you have to remember about biometrics. Compare your list to your partner's. Which three are the most popular among the class?**

USE OF ENGLISH

VOCABULARY

7. **1. A. & B. Match 1–9 with a–i.**

1	Fingerprint Recognition	**a**	analyses the distance between eyes, nose shape, and jawline
2	Facial Recognition	**b**	analyses the unique walking patterns of individuals
3	Iris Recognition	**c**	analyses the unique vocal characteristics and speech patterns
4	Retina Recognition	**d**	analyses the individual's handwriting, including the speed, pressure and number of strokes
5	Voice Recognition	**e**	analyses the shape and size of the hand
6	Hand Geometry	**f**	analyses the unique patterns of ridges and valleys on fingers
7	Signature Recognition	**g**	analyses the pattern of blood vessels in the retina at the back of the eye
8	Gait Analysis	**h**	analyses the typing rhythm, speed, and patterns
9	Keystroke Dynamics	**i**	analyses the unique patterns in the coloured part of the eye

2. A. Group the following words into pairs of synonyms.

To extract, to prove, access, to show, to verify, avoidance, universality, determining, permanence, to take, circumvention, to save, to store, resilience, to indicate, admission, to prevent, durability, recognition, registration, robustness, generality, enrollment, to block.

B. Give synonyms to the words in bold in Ex. 3.

PHRASAL VERBS

8. **A. Fill in the correct particles. Then explain the phrasal verbs. See Appendix 2, which contains a list of relevant phrasal verbs.**

1. Our tech team must **keep** _____ the latest advancements in biometric recognition software.
2. Developers often **play** _____ different biometric features, such as voice recognition and fingerprint scans, to find the most effective solution.
3. By using biometric data, companies can **keep** _____ employee attendance.
4. After testing, the company decided to **put** _____ a fingerprint scanner at all entry points.
5. The biometric security system is designed to **keep** _____ unauthorised access to sensitive areas.
6. The hospital plans to **put** _____ use a new retinal recognition system to improve patient identification and safety.
7. Privacy concerns have **put** _____ some companies from integrating biometric technology into their systems.

B. Replace the words or phrases in bold with the correct form of a phrasal verb using *keep*, *put* and *play*. Then, create three interconnected sentences that include any phrasal verbs with "keep", "put", and "play".

1. To improve the security, companies need to **be informed** about new biometric technologies.
2. The biometric security system is designed to **prevent** unauthorised access of individuals to restricted areas.
3. Organisations can effectively **monitor** employee attendance using biometric fingerprint systems.

4. After assessing the needs, the company decided to **establish** a facial recognition system for secure access.
5. I am ready to **apply** biometric identification systems to improve the customer security.
6. Due to privacy problems, some companies have chosen to **postpone** the use of biometric technologies for the present.
7. Developers like to **experiment** with different biometric methods to see which ones work best for user authentication.

GRAMMAR

9. **A. & B. Use the future tenses in the text.**

In May, Jane **1) _____ (start)** organising a comprehensive training course on biometric recognition systems, where participants **2) _____ (learn)** about fingerprint scanning, facial recognition, and iris detection. At this time each week, she **3) _____ (conduct)** interactive workshops. By the end of September, participants **4) _____ (gain)** not only theoretical knowledge but also practical skills in implementing these technologies. As the course progresses, she **5) _____ (ensure)** that everyone understands the ethical implications of biometric data use. By the end of the course finishes, she **6) _____ (address)** all major concerns and shared best practices. Throughout these months, Jane **7) _____ (dedicate)** her evenings to refining the course materials, making sure that every session is engaging and informative. She knows this effort **8) _____ (result)** in successful and knowledgeable professionals ready to tackle future challenges in the field.

A. The underlined parts of the sentences may contain mistakes. Some underlined parts are correct. Write out parts that contain a mistake and correct it.

1. Face recognition technology **(a) has** the potential to match human faces **(b) on** digital images or video frames **(c) with** face databases.
2. Such **(a) a** system works by **(b) identified and measured** facial features from a given image, and is typically used **(c) to** authenticate users through ID verification services.
3. The development of similar systems **(a) begun** in the 1960s. **(b) It** started as a form of computer **(c) application**.
4. In recent times, facial recognition systems **(a) have used** more **(b) widely** in smart phones and in other forms of technology, such as **(c) robotics**.
5. Facial recognition systems **(a) are classified** as biometrics because **(b) computerising** facial recognition **(c) involves** the measurement of a person's physiological characteristics.
6. Though **(a) least** accurate than iris, fingerprint, palm or voice biometrics, face recognition systems **(b) have gained** widespread acceptance because they are **(c) contactless**.
7. Facial recognition **(a) is used** in advanced human-computer interaction, video surveillance, law enforcement, passenger screening, employment and **(b) housing** decisions, and automated image **(c) indexed**.
8. Governments and private companies around **(a) the** world **(b) using** facial recognition **(c) systems**.
9. Their effectiveness **(a) varies**. Some systems **(b) have been scrapped already** because of **(c) their** ineffectiveness.
10. The use of facial recognition systems **(a) has also been controversial**. It **(b) has**

<u>been argued</u> that these systems violate **(c) <u>citizens'</u>** privacy, often lead to false identifications, encourage gender norms and racial profiling, and fail to protect sensitive biometric data.

Borrowed and modified from: https://en.wikipedia.org/wiki/Facial_recognition_system

B. There is an odd word in some of the lines. Find it and write in the space provided.

The biometric technologies are likely being to be the future of	1
payments. The use of biometric facial of recognition to make	2
payments anywhere had is already being trialled in countries such	3
as China.This technology will remove the need with to carry cash,	4
cards or smartphones to pay. All of you have to do is look at the	5
software, enter the amount and the payment is have made.	6
The first commercial and system for the recognition of hand	7
geometry was available as early as 1974. This system was used as	8
for 3 main purposes – controlling physical access, but recording	9
time and personal identification.	10 √

10. A. & B. Choose the correct answer.

1. Automated facial recognition was pioneered in the 1960s _____ Woody Bledsoe, Helen Chan Wolf and Charles Bisson. Their work focused _____ teaching computers to recognise human faces.

    a) with, in
    b) by, on
    c) by, of

2. Their early facial recognition project _____ “man-machine”. This was because a human had _____ the coordinates of facial features in a photograph before they could be used by a computer for recognition.
    a) called, determining
    b) was called, determine
    c) was called, to determine
3. _____ a graphics tablet, a human determined the coordinates of facial features, such as the centre of the pupils, the inner and outer corners of the eyes, and the _____ peak of the hairline.
    a) Using, widow’s
    b) Used, widow
    c) Using, widow
4. Twenty individual distances, _____ mouth and eye widths, _____ from the coordinates.
    a) included, was calculated
    b) including, were calculated
    c) including, calculated
5. A human could process about 40 images per hour, _____ a database of these _____ distances.
    a) built up, calculated
    b) build up, calculating
    c) building up, calculated
6. The computer then _____ compared the distances for _____ photograph, calculated the difference between the distances and returned the closed sets as possible matches.
    a) automatically, each
    b) automatical, each
    c) automatical, every

7. In 1970, Takeo Kanade publicly demonstrated a _____ that detected _____ features like chins and calculated facial distance ratios without human intervention.

    a) face-matched system, anatomy
    b) face-matching system, anatomy
    c) face-matching system, anatomical

8. Later tests showed that the system _____ always be reliable in the _____ of facial features.

    a) could not, identification
    b) ought not, identify
    c) had not, identification

9. However, interest in _____ subject continued to grow and in 1977 Kanade published _____ first book to provide detailed information _____ facial recognition technology.

    a) a, a, in
    b) the, the, on
    c) the, a, of

10. In 1993, the Defense Advanced Research Agency and the Army Research Laboratory _____ FERET to create "automated face recognition capabilities" to "assist security, intelligence, and law enforcement personnel _____ the performance of their missions".

    a) establish, off
    b) established, on
    c) established, in

The sentences are borrowed and modified from:
https://en.wikipedia.org/wiki/Facial_recognition_system

LISTENING

You are going to watch a video about biometrics.

11. A. & B. Before watching a video, check if you know the meaning of the words and phrases. Use Merriam-Webster Dictionary if necessary.

An integral part of our lives, unique physical and behavioral characteristics, the identification of individuals, a replacement, encryption, consent, surveillance, data breaches.

12. Watch the video "What is Biometrics and How Safe is it?" and then summarise the key points discussed. Provide a clear and concise response.

13. Watch the video again and do the following tasks.

13.1. Fill in the missing information in statements 1–7.

1. The term is derived from "bio" meaning _____ and "metrics" meaning units of _____.
2. _____ biometrics. The way we speak, type, and sign documents are all traits that are unique to every individual.
3. For security, biometrics works as a _____ when you register your biometrics on your personal devices.
4. Biometric security systems store data directly on a device and protect it through _____.
5. The main advantage of biometric data is its _____.
6. Personal data can be easily collected without _____.
7. It is recommended that you take the time to install updates regularly, _____, and keep your devices up to date with the latest security updates.

13.2. Decide whether these sentences are *true* or *false*.

1. Biometrics refers to the measurement of unique physical and behavioral characteristics of a living organism.
2. Behavioral biometrics include traits such as the way we speak or type.
3. Physiological biometrics can recognise unique physical attributes like fingerprints and facial features.
4. Biometric security systems are easier to hack than traditional passwords due to the simplicity of biometrics.
5. Personal data can be collected without consent, raising concerns about privacy and surveillance.
6. It is safe to store biometric data with service providers rather than on personal devices.
7. If biometric data is stolen, it may be permanently compromised since it cannot be changed like a password.

SPEAKING

14. **A. Work in pairs. During cybersecurity workshops, the experts talk about biometrics, its significance in the digital world, how biometric systems function, the various types of biometrics, and examples of their everyday applications. Role play a dialogue with your partner that involves at least 5–6 exchanges per each participant. Be creative! Remember to keep the tone respectful!**

A	B
1. You have noticed how important biometrics has become nowadays.	Sure! Biometrics offers enhanced security and convenience, …
2. …..	…….

A	B
3. …….	…….
4. …….	……
5. …….	……

B. Work in groups of four to discuss and choose the most suitable biometric technologies for a Ukrainian company. Your task is to engage in a polylogue with James Clifton, a biometric consultant from the USA, and decide on the top three biometric solutions that would enhance the company's cyber security level. The biometric solutions should provide a means to achieve fast, user-friendly authentication with a high level of accuracy and cost savings. Give arguments against some biometric technologies. Use the tables below.

1. Analyse biometric characteristics.

Biometric characteristic	***Description of the features***
Fingerprint	Ridges and valleys on fingers
Signature	Handwriting (the speed, pressure and number of strokes)
Facial geometry	Distance of specific facial features (eyes, nose, mouth)
Iris	
Retina	
Hand geometry	
Finger geometry	
Voice	
DNA	
Keyboard strokes	
Password	

2. Analyse the permanence of biometric characteristics over time on a scale of 1 (less permanent) to 5 (most permanent).

Biometric characteristic	***Permanence over time***
Fingerprint	
Signature	
Facial geometry	
Iris	
Retina	
Hand geometry	
Finger geometry	
Voice	
DNA	
Keyboard strokes	
Password	

3. Analyse the suitability of biometrics for the company's recognition needs based on the following criteria: convenience, precision, availability, cost.

Biometric characteristic	***Convenience***	***Precision***	***Availability***	***Cost***
Fingerprint				
Signature				
Facial geometry				
Iris				
Retina				
Hand geometry				
Finger geometry				

Voice				
DNA				
Keyboard strokes				
Password				

15. **A. For your ESP lesson, choose one biometric recognition type to present to your groupmates. Your presentation should last 2–3 minutes and be structured into three stages: an introduction, a main body, and a conclusion.**

1. Fingerprint
2. Signature
3. Facial geometry
4. Iris
5. Retina
6. Hand geometry
7. Finger geometry
8. Vein Structure of the hand
9. Ear form
10. Voice
11. DNA
12. Keyboard strokes
13. Odor
14. Mouse movement
15. Gait

B. For your ESP lesson, choose one biometric issue to present to your groupmates. Your presentation should last 3–4 minutes and be structured into three stages: an introduction, a main body, and a conclusion.

1. Privacy concerns (impact of biometric use on personal privacy and individual rights).

2. Data Security (the challenges and vulnerabilities associated with storing and managing biometric information).
3. Ethical Considerations (the ethical implications of biometric technology on freedom and moral responsibility).
4. Biometrics hacking (a way to spoof fingerprint scanning devices).

WRITING

16. **Work with AI.**

Analyse the AI-generated arguments for and against the topic of "Privacy concerns surrounding biometric data collection and storage".

Consider the following questions:

1. **What are the features of AI writing style?**
2. **Do you agree with the arguments presented by AI?**
3. **How can you simplify the arguments for clarity?**

Write your own 1–2 arguments both for and against this topic. Then ask AI to improve your arguments. Compare the difference in depth, clarity, and persuasion.

For: *"Increased Security: Biometric systems offer a higher level of security because they are unique to each individual, making it extremely difficult for unauthorised users to gain access. Unlike passwords, which can be forgotten or stolen, biometric traits such as fingerprints or facial recognition are inherent to the user."*

Against: *"Data Vulnerability: The central storage of biometric data can create a single point of failure, where hackers may target these databases to steal sensitive information. If compromised, stolen biometric data cannot be reissued like a lost password, leading to lasting security concerns for individuals."*

AI Text Generator, https://deepai.org/chat/text-generator

17. **A. To participate in *For* and *Against Essay Contest,* you have to write an essay (150–170 words) on the topic: "The effectiveness of biometric security systems versus traditional password methods". Follow the stages: introduction, main body, conclusions. Present a balanced discussion that critically analyses both perspectives before concluding your argument.**

Cover the following points:

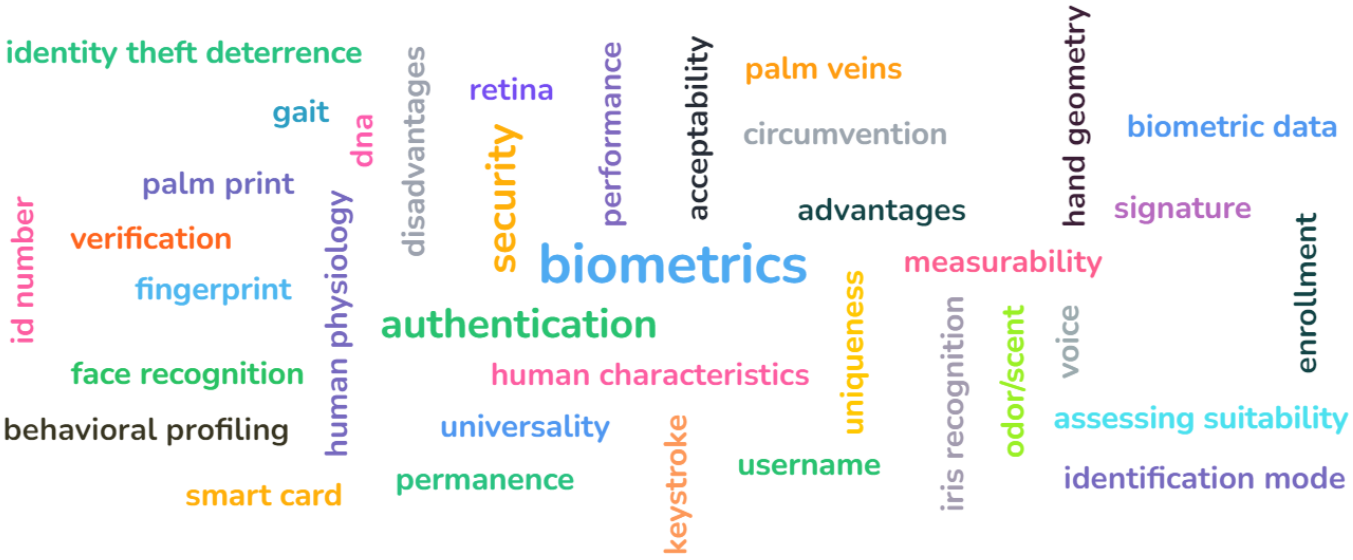
For	Against
enhanced security	privacy problems
convenience	potential for false positives
and reduced risk of hacking	and issues surrounding data breaches

B. To participate in *For* and *Against Essay Contest,* you have to choose one of the topics and write a for and against essay (180–200 words). Follow the stages: introduction, main body, conclusions. Present a balanced discussion that critically analyses both sides.

1. The role of biometrics in enhancing national security versus individual rights.
2. The impact of biometric technology on data breaches and identity theft.
3. The accessibility of biometric technology for people with disabilities versus its potential for exclusion.
4. The reliability of biometric identification systems under varying conditions versus their limitations.
5. The potential benefits of biometrics in streamlining healthcare processes against confidentiality risks.

REFLECTION AND SYNTHESIS

18. **You have completed this unit. This word cloud can help you to reflect on and synthesise the key concepts from the topic. Focus on the most important terms and ideas that stood out to you. Using the word cloud as a visual tool, you have to illustrate your understanding.**



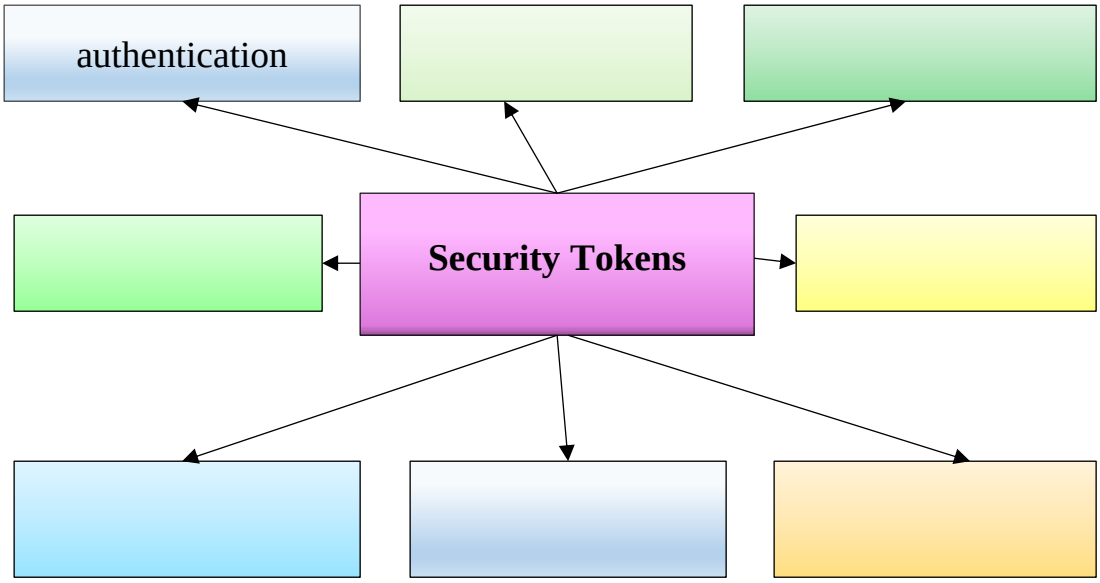
3.4. SECURITY TOKENS

WARM UP

1. **A. & B. Using your background knowledge, do the tasks according to your learning style (dominant or non-dominant modality).**

1.1. *Visual Modality*

Work individually, then in small groups. Create a mind map with a central concept "*Security Tokens*". Start by brainstorming relevant terms related to security tokens. Clearly illustrate how each term relates to the central concept.



1.2. *Auditory Modality*

Discuss the following questions.

1. What does the term "security token" mean?
2. How does a security token work?
3. What do you know about the historical facts of how tokens came to exist?
4. What are the ways to hack tokens?

1.3. ***Kinesthetic Modality***

Work in small groups. Identify the advantages and disadvantages of security tokens. Fill in the table with your findings. Then present your findings to the class.

Advantages of security tokens	Disadvantages of security tokens
1. ……..	1. …….
2. ……..	2. …….
3. ……..	3. …….
4. ……..	4. …….
5. ……..	5. …….

READING

You are going to read an article about security tokens.

2. **1. A. & B. Before reading, discuss the following statement.**

Security tokens in information security serve as a dual-edged sword.

2. A. & B. Before reading, look at the following words and phrases, which have been taken from the text. In what context might they be mentioned? Use Merriam-Webster Dictionary if necessary.

Synchronisation, asynchronous, static, identity, decrypted, unsynchronised, disconnected, contactless.

3. **A. & B. Read the text about security tokens. Six sentences have been removed. Choose which of the sentences fit into the gaps.**

A	They typically do not require a special input device, and instead use a built-in screen to display the generated authentication data, which the user enters manually themselves via a keyboard or keypad.
B	The absence of the need for physical contact makes them more convenient than both connected and disconnected tokens.
C	Examples include a wireless keycard unlocking a door or a bank token verifying a customer's identity online.
D	Usually most tokens store a cryptographic hash of the password so that if the token is compromised, the password is still protected.
E	Time-synchronised one-time passwords change constantly at a set time interval; e.g., once per minute.
F	They enable a broad range of security solutions and provide the abilities and security of a traditional smart card without requiring a unique input device.

SECURITY TOKENS

A security token is a peripheral device used to gain access to an electronically restricted resource. The token is used in addition to or in place of a password. It acts like an electronic key to access something. **1 _____**.

Some tokens store cryptographic keys, biometric data, or passwords. Some may feature tamper-resistant packaging, small keypads for PIN entry, or buttons to generate keys, with displays showing the results. Connected tokens utilise interfaces including USB, near-field communication (NFC), radio-frequency identification (RFID), or Bluetooth, and some include audio features for vision-impaired users.

Password types. All tokens contain some secret information that is used to prove identity. There are four different ways in which this information can be used:

− *Static password token*. The device contains a password which is physically hidden (not visible to the possessor), but which is transmitted for each authentication. This type is vulnerable to replay attacks.

− *Synchronous dynamic password token*. A timer is used to rotate through various combinations produced by a cryptographic algorithm. The token and the authentication server must have synchronised clocks.

− *Asynchronous password token*. A one-time password is generated without the use of a clock, either from a one-time pad or cryptographic algorithm.

− *Challenge response token*. Using public key cryptography, it is possible to prove possession of a private key without revealing that key. The authentication server encrypts a challenge (typically a random number, or at least data with some random parts) with a public key; the device proves it possesses a copy of the matching private key by providing the decrypted challenge.

Several types of security tokens are in use for the protection of a wide variety of assets and applications. They comprise the following:

One-time passwords. 2 _____. To do this some sort of synchronisation must exist between the client's token and the authentication server. For disconnected tokens this time-synchronisation is done before the token is distributed to the client. Other token types do the synchronisation when the token is inserted into an input device. The main problem with time-synchronised tokens is that they can, over time, become unsynchronised. However, some such systems, such as RSA's SecurID, allow the user to resynchronise the server with the token, sometimes by entering several consecutive passcodes.

Physical types. Tokens can contain chips with functions varying from very simple to very complex, including multiple authentication methods.

Disconnected tokens have neither a physical nor logical connection to the client computer. **3 _____**. Disconnected tokens are the most common type of security token used (usually in combination with a password) in two-factor authentication for online identification.

Connected tokens are tokens that must be physically connected to the computer with which the user is authenticating. Tokens in this category automatically transmit the authentication information to the client computer once a physical connection is made, eliminating the need for the user to manually enter the authentication information. However, in order to use a connected token, the appropriate input device must be installed.

Many connected tokens use smart card technology. **Smart cards** can be very cheap and contain proven security mechanisms. However, computational performance of smart cards is often rather limited because of extreme low power consumption and ultra-thin form-factor requirements.

Smart-card-based USB tokens which contain a smart card chip inside provide the functionality of both USB tokens and smart cards. **4 _____**. From the computer operating system's point of view such a token is a USB-connected smart card reader with one non-removable smart card present.

Unlike connected tokens, **contactless tokens** form a logical connection to the client computer but do not require a physical connection. **5 _____**. As a result, contactless tokens are a popular choice for keyless entry systems and electronic payment solutions such as Mobil Speedpass, which uses RFID to transmit authentication info from a keychain token. However, there have been various security concerns raised about RFID tokens after researchers at Johns Hopkins University and RSA Laboratories discovered that RFID tags could be easily cracked and cloned.

Single sign-on software tokens. Some types of single sign-on (SSO) solutions, like enterprise single sign-on, use the token to store software that allows for seamless authentication and password filling. As the passwords are stored on the token, users need not remember their passwords and therefore can select more secure passwords, or have more secure passwords assigned. **6 _____**.

Programmable tokens are marketed as "drop-in" replacement of mobile applications such as Google Authenticator (miniOTP). They can be used as mobile app replacement, as well as in parallel as a backup.

Borrowed and modified from:
https://eng.libretexts.org/Courses/Delta_College/Information_Security/02%3A_Authenticate_and_Identify/2.3%3A_Authentication_Methods_-_Password/2.3.3%3A_Authentication_Methods_-_Security_Tokens
Modified by https://deepai.org/chat/text-generator

4. **A. & B. Read the text again and do the following tasks.**

4.1. Fill in the missing information in statements 1–7.

1. A security token is a _____ device used to gain access to an electronically _____ resource.
2. Some tokens may store _____ keys that may be used to generate a digital signature, or _____ data, such as fingerprint details.
3. _____ contains a password which is physically hidden, but which is transmitted for each authentication.
4. _____ are tokens that must be physically connected to the computer with which the user is authenticating.
5. _____, which contain a smart card chip inside, provide the functionality of both USB tokens and smart cards.
6. RFID tags can be easily cracked and _____.
7. Programmable tokens can be used as mobile app replacement, as well as in parallel as a _____.

4.2. Decide whether these sentences are *true* or *false*.

1. A security token is used in addition to or in place of a password, but is not solely a replacement.
2. All security tokens contain secret information that is necessary for proving identity.
3. Time-synchronised one-time password tokens can become unsynchronised over time.
4. Connected tokens require a physical connection to the computer for authentication.
5. Disconnected tokens require manual input from the user to enter the authentication data.
6. Contactless tokens use RFID technology and do not require physical contact with the authentication device.
7. Programmable tokens can serve as a replacement for mobile applications like Google authenticator.

5. **A. & B. In pairs, select one word from the provided list. Student A asks the questions below, putting the chosen word into each question, while Student B responds using that word. You may skip any questions that do not apply. After completing the questions, switch roles and repeat the activity with a different word. See the example below.**

Token, device, resource, access, key, password, generate, variety, prove, visible, replay, synchronous, private, manual, ability.

1. What does _____ mean?
2. What is the plural / singular of _____?
3. What is the synonym of _____?

4. What is the opposite of _____?
5. What is the noun for _____?
6. What is the verb for _____?
7. What is the adjective for _____?
8. What is the adverb for _____?
9. Can you give _____ collocations?
10. How to use _____ in a sentence?
11. What is the translation for _____?

For example:

The chosen word is "project".

Student A: "What does project mean?"

Student B: "Project" is a planned set of activities or tasks intended to achieve a specific goal.

Student A: "What is the plural of project?"

Student B: "Projects."

6. **Answer the questions.**

1. What is the function of a security token?
2. What are the four different ways in which the secret information contained in security tokens can be used to prove identity?
3. What are the specifics of one-time passwords?
4. What is the difference between disconnected and connected tokens?
5. What are the specifics of smart-card-based USB tokens?
6. What makes contactless tokens convenient compared to connected and disconnected tokens?
7. What are the specifics of single sign-on software tokens?
8. What is the purpose of programmable tokens?

USE OF ENGLISH

VOCABULARY

7. A. & B. Work with AI. Give the synonyms to the words in italics. Use any AI tool to fill in the third rubric of the table. Then make up two sentences using several synonym phrases.

Words	Synonyms suggested by students	Synonyms generated by AI
1. the *generated* authentication data		
2. to *gain* access		
3. *restricted* resource		
4. *tamper resistant*		
5. to *prove* possession of a private key		
6. the *matching* private key		
7. *disconnected* tokens		
8. *connected* tokens		
9. the token is *compromised*		
10. *"drop-in" replacement*		

A. Complete the sentences. Use: *physical display, plug into, tokens, cryptographic operation, Bluetooth, connection, mobile device, log in, client, PIN*.

1 _____ can contain chips with functions varying from very simple to very complex, including multiple authentication methods.

The simplest security tokens do not need any **2 _____** to a computer. The tokens have a **3 _____**; the authenticating user simply enters the

displayed number to **4** _____. Other tokens connect to the computer using wireless techniques, such as **5** _____. These tokens transfer a key sequence to the local **6** _____ or to a nearby access point.

Alternatively, another form of token that has been widely available for many years is a **7** _____ which communicates using an out-of-band channel (like voice, SMS, or USSD).

Still other tokens **8** _____ the computer, and may require a **9** _____. Depending on the type of the token, the computer OS will then either read the key from the token and perform a **10** _____ on it, or ask the token's firmware to perform this operation.

B. Complete the sentences.

A related application is the hardware dongle required by some computer **1** _____ to prove ownership of the software. The **2** _____ is placed in an input device and the software accesses the I/O device in question to **3** _____ the use of the software in question.

Commercial solutions are provided by a variety of vendors, each with their own proprietary (and often patented) implementation of variously used **4** _____ features. **5** _____ designs meeting certain security standards are certified in the United States as compliant with FIPS 140, a federal security **6** _____. Tokens without any kind of **7** _____ are sometimes viewed as suspect, as they often do not meet accepted government or industry security standards, have not been put through rigorous testing, and likely cannot provide the same **8** _____ of cryptographic security as token solutions which have had their designs independently audited by **9** _____ -party agencies.

Borrowed and modified from:
https://eng.libretexts.org/Courses/Delta_College/Information_Security/02%3A_Authenticate_and_Identify/2.3%3A_Authentication_Methods_-_Password/2.3.3%3A_Authentication_Methods_-_Security_Tokens

IDIOMS

8. **A. Match the idioms in bold to their equivalents. Have you got any similar idioms / phrases in your language?**

Staying updated, diversifying, navigating laws, creating strong, defenses, control access, building trust.

1. Many people are **hedging the bet** by spreading their portfolios across various security tokens.
2. It's important for token users to **keep their keys close** to prevent unauthorised transactions.
3. The company is **riding the compliance wave** to adapt to the changing regulations around security tokens.
4. Smart policies act like **building a fortress** for the secure issue of security tokens.
5. By using security tokens, companies are effectively **bridging the trust gap** between users and their electronic systems, ensuring secure access to restricted resources.
6. With the increasing regulations in the digital domain, companies are **charting the compliance waters** to make sure their security tokens are properly secured.

B. Fill in the blanks using the idioms from the list below. You may need to change the verb tense.

Hedging the bet, keeping the keys close, riding the compliance wave, building a fortress, bridging the trust gap, charting the compliance waters.

The transition from traditional passwords to physical security tokens was a massive shift for our IT department. We weren't just changing hardware; we were **1) _____** around our sensitive data, ensuring that even if a password was stolen, the physical token remained an impassable barrier.

Initially, the legal department spent months **2)** _____ trying to understand how new data privacy laws would affect our global offices. Instead of resisting these strict new rules, our specialists suggested **3)** _____, using the mandatory upgrades as an opportunity to modernise our entire infrastructure. By doing so, we were effectively **4)** _____; if a major audit occurred, we wouldn't just be "passing" – we would be the gold standard.

However, the hardware itself was only half the battle. We focused on **5)** _____ with our employees, who were initially frustrated by the extra step in their login process. We explained that by **6)** _____ – quite literally, on a USB device at their side – they were protecting not just the company's secrets, but their own digital identities as well.

Borrowed and modified from: https://gemini.google.com/

GRAMMAR

9. **A. & B. Put the verbs into the correct form. Use future tenses in the sentences below.**

1. By 2030, developers _____ **(integrate)** advanced security features into smart cards, ensuring safer transactions.
2. In the next few years, banks _____ **(introduce)** smart cards that enable contactless payments for everyday transactions.
3. By September, IT specialists _____ **(develop)** more advanced security tokens for two months.
4. I think, in the coming years, organisations _____ **(implement)** security tokens to enhance their authentication processes.
5. By the end of next month, Jane _____ **(study)** for seven hours.
6. IT departments _____ **(train)** employees to use security tokens effectively to protect sensitive information.

7. By the end of this year, IT specialists _____ **(use)** disconnected tokens into secure systems to strengthen access controls for 6 months.
8. I think the user _____ **(re-authenticate)** to receive a new access token.
9. By the end of the month, I _____ **(use)** a smart card in multifactor authentication schemes for 2 weeks.
10. I _____ **(finish)** the report about security tokens by 5 o'clock.

10. **A. Choose the correct answer.**

1. _____ **(The simplest / The simpler)** vulnerability of any password container is theft or loss.
2. The likelihood of this happening, or happening unnoticed, _____ **(ought / can)** be reduced by _____ **(using / used)** physical security such as locks, electronic leashes or body sensors and alarms.
3. Token theft _____ **(can / has / ought)** be prevented through the use of two-factor authentication.
4. Typically, authentication requires a Personal Identification Number (PIN) _____ **(to enter / to be entered / enter)** at the same time as the token is issued, along with the information _____ **(providing / provided)** by the token.
5. Any system that allows users _____ **(to authenticate / authenticating / authenticate)** over an untrusted network is vulnerable to man-in-the-middle attacks.
6. In this type of attack, an attacker acts as the "go-between" _____ **(--- / in / of)** the user and the legitimate system, _____ **(obtained / obtaining)** the token output from the legitimate user and then passing it to the authentication system itself.

7. As the token value is _____ **(mathematic / mathematics / mathematically)** correct, authentication is successful and the fraudster _____ **(grantes / is granted)** access.
8. In 2006, Citibank _____ **(had / was / had been)** the victim of an attack.
9. _____ **(It's / Its)** business users, equipped _____ **(on / with)** hardware tokens, were the victims of a major man-in-the-middle phishing operation _____ **(based / basing)** in the Ukraine.
10. Smart cards offer a secure and convenient way to authenticate users _____ **(in / on)** various online and offline transactions.

Borrowed and modified from: https://en.wikipedia.org/wiki/Security_token

B. Complete the sentences using the words in bold. Use two to six words.

1. It was the first time they had used a smart card.
   never They _____ a smart card before.
2. The professor made us read information about smart cards.
   made We _____ about a smart card by the professor.
3. Accessing the sensitive data is not allowed without a valid security token.
   access Without a valid security token, _____ is not allowed.
4. When did he join this IT company?
   ago How long _____ this IT company.
5. She has never used tokens before.
   first It's the _____ used tokens.
6. I advise you to consider utilising a smart card for its numerous benefits.
   should You _____ for its numerous benefits.
7. Let's have a five-minute break.
   can We _____ break.

8. The scientists say that an authentication token is a one-time key that verifies identity and grants access to resources.

   be An authentication token _____ a one-time key that verifies identity and grants access to resources.

9. Jane needs someone to help her with her smart card.

   be Jane needs _____ with her smart card.

10. Someone sent us a phishing letter.

    were We _____ a phishing letter.

LISTENING

You are going to watch a video about smart cards.

11. A. & B. Before watching a video, check if you know the meaning of the words / phrases. Use Merriam-Webster Dictionary if necessary.

Embedded, bank-issued chip cards, identification, authentication, VPN access, email signature, email encryption, disk encryption, digital certificate, admin PIN, to unblock, to reset, to impersonate, to retrieve.

12. Watch the video "Smart Card Introduction" and then summarise the key points discussed. Provide a clear and concise response.

13. A. & B. Watch the video again and do the following tasks.

13.1. Fill in the missing information in statements 1–5.

1. A smart card is a plastic card that has the appearance of a typical credit card, but with an _____ .
2. With smart cards, enterprises provide _____ through strong two-factor authentication.

3. With two-factor authentication, organisations can significantly reduce the likelihood that the person requesting _____ will provide false proof of _____ .
4. Organisations using smart cards for strong authentication need _____ that is issued to the smart card.
5. A smart card management system protects _____ for each smart card.

13.2. Decide which statements are *true* and which are *false*.

1. Smart cards provide a less secure method of protecting data compared to passwords alone.
2. Two-factor authentication with smart cards requires both a physical card and a PIN.
3. The public key infrastructure (PKI) is irrelevant to the function of smart cards.
4. Smart card management systems help to protect the admin pin from being retrieved by malicious users.
5. Common uses for smart cards in businesses include email encryption and secure VPN access.

SPEAKING

14. A. Work in pairs. In a cyber security workshop, you are talking about security tokens as a tool for authentication and authorisation. Role play a conversation with your partner about security tokens, focusing on the profits and drawbacks of token-based authentication. Your dialogue should include at least 5–6 exchanges per each participant. Be creative! Remember to keep the tone respectful!

A	B
1. I've been reading about token-based authentication. It seems efficient, right?	**1.** It is! Tokens can be easily used across different domains and services, facilitating single sign-on implementations and enhancing user convenience.
2. …..	**2.** …….
3. …….	**3.** …….
4. …….	**4.** ……
5. …….	**5.** ……

B. Work in groups of two. In a cyber security workshop, you are talking about different types of authentication tokens. Your conversation should include at least 7–8 exchanges per each participant. Be creative! Remember to keep the tone respectful!

15. **A. You are presenting information about authentication tokens to a group of cyber security professionals in a workshop setting. Prepare a brief presentation (2–3 minutes), structured as follows: introduction, main body, conclusions. Cover the following points:**

1. **An authentication token definition.**
2. **A brief history of token-based authentication.**
3. **The work of authentication tokens.**
4. **Types of authentication tokens (connected, disconnected, contactless).**

B. You are presenting information about authentication tokens to a group of cyber security professionals in a workshop setting. Search the internet and prepare a presentation on one of the suggested topics.

1. **The ways of authentication tokens hacking.**
2. **Measures to prevent hacking of authentication tokens.**

Structure your presentation as follows: introduction, main body, conclusions.

WRITING

16. **A. You've got your own website, where you inform your audience about different cyber security issues. This time you need to write about authentication tokens. Choose one of the topics and write a blog entry (150–160 words). Follow the stages: introduction, main body, conclusions.**
    1. **When is an authentication token recommended?**
    2. **How do you implement an authentication token?**

17. **B. You've got your own website, where you inform your audience about different cyber security issue. This time you need to write about authentication tokens. Choose one of the topics and write a blog entry (180–200 words). Follow the stages: introduction, main body, conclusions.**
    1. **Hardware vs. software security tokens: what's the difference?**
    2. **Smart cards.**
    3. **Best practices for securing tokens, including encryption and storage methods.**
    4. **Exploring how tokens work in mobile applications and Internet of Things (IoT) devices.**
    5. **Common challenges faced when integrating token-based authentication with existing systems.**

REFLECTION AND SYNTHESIS

18. **You have completed this unit. This word cloud can help you to reflect on and synthesise the key concepts from the topic. Focus on the most important terms and ideas that stood out to you. Using the word cloud as a visual tool, you have to illustrate your understanding.**

3.5. UNIT 3. REVISION 3

WARM UP

1. **A. & B. Decide whether these sentences are *true* or *false*.**

1. A driver's license, a Social Security card, a valid passport, or military photograph identification are some forms of identification.
2. The knowledge factor: something the user possesses.
3. Authentication takes place when someone tries to log into a computer resource (such as a network, device, or application).
4. A salt does not prevent attackers from easily building a list of hash values for common passwords.
5. Biometric authentication is used for both access control and identification.
6. Enrollment is the initial phase where biometric information is captured and stored.
7. "Positive recognition" is a common use of the verification mode, "where the aim is to prevent multiple people from using the same identity".
8. Biometric security systems are easier to hack than traditional passwords due to the simplicity of biometrics.
9. The token is used in addition to or in place of a password.
10. Disconnected tokens require manual input from the user to enter the authentication data.
11. Biometric systems are never wrong and never produce false positives or negatives.
12. Biometric data can be easily changed or reset, similar to a password, making it a flexible security option.

READING

2. A. & B. Read the text and do the following tasks.

2.1. Choose the correct answer.

1. What does keystroke dynamics refer to?
    a. The physical structure of a keyboard
    b. The collection of biometric information from key-press events
    c. The history of password development
2. How are keystrokes classified in keystroke dynamics?
    a. Simple and complex
    b. Static and dynamic
    c. Fast and slow
3. What is the purpose of measuring a user's keystroke rhythms?
    a. To improve keyboard design
    b. To track typing speed
    c. To develop a unique biometric template for authentication
4. What is the main purpose of keystroke dynamic information?
    a. To improve typing speed
    b. To verify or determine the identity of the user
    c. To enhance keyboard design
5. What are the two key time metrics that characterise an individual's typing pattern?
    a. Seek-time and press-time
    b. Seek-time and hold-time
    c. Press-time and release-time

6. How do right-handed users typically perform compared to left-handed users when pressing keys?
    a. They are slower overall
    b. They are faster on keys hit with their right-hand fingers
    c. They have no difference in speed
7. What type of errors can be characteristic of a user's typing?
    a. Only spelling errors
    b. Common substitutions, reversals, and hold-length-errors
    c. Punctuation errors
8. What category of biometrics does keystroke dynamics belong to?
    a. Physical biometrics
    b. Behavioral biometrics
    c. Digital biometrics
9. How do behavioral biometrics measure authentication success?
    a. With pass / fail measurements
    b. With confidence measurements
    c. With numerical scores

2.2. Fill in the missing information in statements 1–9.

1. Keystroke dynamics refers to the collection of _____ information generated by key-press-related events that occur when a user types on a keyboard.
2. The user's keystroke rhythms are measured to develop a unique biometric template of the user's typing pattern for future _____.
3. Keystrokes are divided into _____ and dynamic typing.
4. Right-handed people may be statistically faster in getting to _____ they hit with their right-hand fingers than with their left-hand fingers.
5. The time to _____ and depress a key and the time the key is _____

down may be characteristic of an individual, regardless of the total speed at which they type.

6. Ending “ing” may be entered far faster than the same letters in _____ order (“gni”).
7. Keystroke dynamics is part of biometrics known as _____ biometrics.
8. One problem is that a user’s _____ varies considerably throughout the day and from day to day.
9. Even if you don’t know what language the user is working in, the _____ may be detected by looking at the rest of the text and what letters the user goes back and replaces.

KEYSTROKE DYNAMICS

Keystroke dynamics (keystroke biometrics, typing dynamics, or typing biometrics) refers to the collection of biometric information generated by key-press-related events that occur when a user types on a keyboard. The use of keystroke patterns to identify operators predates modern computing. It has been proposed as an authentication alternative to passwords and PIN numbers.

In the late 19th century, telegram operators developed unique tapping signatures. During World War II, Morse Code was used, with military intelligence identifying individuals by their distinctive rhythm of “dots” and “dashes”, known as “The Fist of the Sender”, to distinguish allies from enemies.

Keyboard dynamics received attention as a potential alternative to short PIN numbers, which were widely used for authentication early in the expansion of networked computing.

The behavioral biometric of keystroke dynamics uses the manner and rhythm in which an individual types characters on a keyboard or keypad. The user’s keystroke rhythms are measured to develop a unique biometric template of the user’s typing

pattern for future authentication. Keystrokes are separated into static and dynamic typing, which are used to help distinguish between authorised and unauthorised users. Vibration information may be used to create a pattern for future use in both identification and authentication tasks.

Keystroke dynamic information could be used to verify or determine the identity of the person producing the keystrokes. The techniques used to do this vary widely in sophistication and range from statistical techniques to artificial intelligence approaches such as neural networks.

The time to seek and depress a key (seek-time) and the time the key is held down (hold-time) may be characteristic of an individual, regardless of the total speed at which they type. Most people take longer to find or get to specific letters on the keyboard than their average seek-time for all letters. Which letters require more time vary dramatically and consistently for different people. Right-handed people may be statistically faster in getting to keys they hit with their right-hand fingers than with their left-hand fingers. Index fingers may be faster than other fingers, consistent for a user, regardless of their overall speed.

In addition, sequences of letters may have characteristic properties for a user. In English, the use of “the” is very common, and those three letters may be known as a rapid-fire sequence. Common endings, such as “ing”, may be entered far faster than the same letters in reverse order (“gni”) to the degree that varies consistently by user. This consistency may hold and reveal common sequences of the user’s native language even when they are writing entirely in a different language.

Common “**errors**” may also be quite characteristic of a user. There is a taxonomy of errors, such as the user’s most common “substitutions”, “reversals”, “drop-outs”, “double-strikes”, “adjacent letter hits”, “homonyms” and hold-length-errors (for a shift key held down too short or too long a time). Even without knowing what language the

user is working in, these errors may be detected by looking at the rest of the text and what letters the user goes back and replaces.

Keystroke dynamics is a type of behavioral biometrics, which relies on statistical patterns and is considered less reliable than physical biometrics like fingerprints or retinal scans. Instead of pass / fail metrics, it uses confidence measures, making False Acceptance Rate (FAR) and False Rejection Rates (FRR) less directly connected.

The benefit to keystroke dynamics is that FRR / FAR can be adjusted by changing the acceptance threshold at the individual level. This allows for explicitly defined individual risk mitigation that physical biometric technologies could not achieve.

One of the major problems that keystroke dynamics runs into is that a user's typing varies substantially during a day and between different days and may be affected by any number of external factors.

Because of these variations, any system will make false-positive and false-negative errors. Some successful commercial products have strategies to handle these issues and have proven effective in large-scale use in real-world settings and applications.

Borrowed and modified from: https://en.wikipedia.org/wiki/Keystroke_dynamics

3. Find words and phrases in the text that match definitions 1–6.

1. _____ is a biometric authentication method that analyses an individual's typing patterns, including rhythm, speed, and pressure, to verify their identity based on the unique characteristics of their keystrokes.
2. _____ is the process of verifying the identity of a person or system, typically through the use of credentials like biometric data.
3. _____ is a digital representation of a person's unique biometric data, such as fingerprints or facial recognition, used for identity verification in biometric systems.

4. _____ is a deviation from accuracy or correctness, often occurring in communication.
5. _____ are individuals who predominantly use their right hand for activities such as writing, eating, and performing tasks.
6. _____ refers to the measurement and analysis of unique patterns in human behavior (typing speed, gait, etc,) to verify an individual's identity or authenticate access to systems.

4. Discuss the questions.

1. What is keystroke dynamics?
2. What types of keystrokes do you know?
3. What historical facts about the appearance of keystroke dynamics do you know?
4. What are the specifics of keystroke dynamics?
5. What is the benefit to keystroke dynamics?

USE OF ENGLISH

5. A. Fill in with *uniqueness, mutual authentication, smart card, tokens, password, identifiers, manner, disconnected, authentication, backup, privacy*.

1. _____ is the process of verifying whether someone (or something) is, in fact, who (or what) it is declared to be.
2. A _____ is a secret word or string of characters that is used for user authentication.
3. Software _____ are stored on a general-purpose electronic device such as a desktop computer, laptop, PDA, or mobile phone and can be duplicated.
4. _____ is found in two types of schemes: username-password based schemes and certificate based schemes, and these schemes are often employed in the Internet of Things (IoT).

5. _____ means the trait should be sufficiently different for individuals in the relevant population such that they can be distinguished from one another.
6. The collection of biometric _____ raises _____ concerns about the ultimate use of this information.
7. The behavioral biometric of keystroke dynamics uses the _____ and rhythm in which an individual types characters on a keyboard or keypad.
8. Many connected tokens use _____ technology.
9. _____ tokens have neither a physical nor logical connection to the client computer.
10. Programmable tokens can be used as mobile app replacement, as well as in parallel as a _____.

B. Complete the sentences.

Smart cards are plastic cards with **1) _____** microprocessors or memory chips that securely store and process data. These cards can perform a variety of functions, including identity **2) _____**, secure transactions, and access control. Smart cards use **3) _____** and can be either contact or contactless, allowing users to tap or insert the card into a **4) _____** for instant **5) _____**. They are widely used in various applications, such as banking for credit and debit **6) _____**, transportation for fare payment, and in security for **7) _____** to buildings or systems. The versatility and **8) _____** of smart cards make them an essential tool in modern business and everyday transactions, helping to protect **9) _____** personal and financial **10) _____**.

6. **A. Choose the correct tense.**

1. Once I receive the new card, I **will use / will have used** it for all my transactions in future.
2. Ann will have completed / will have been completing her "Biometrics" course by the end of June.
3. By the time I arrive at the company, I **will have been reading / will read** the documents for three hours.
4. I **will help / will have helped** you understand how biometrics can enhance security measures.
5. By next year, I **will be upgrading / will have upgraded** my smart card to include additional security features.
6. This time tomorrow, our team **will have been re-writing / will be re-writing** the information security policy.
7. Nick **will have assisted / will assist** you set up biometric authentication on your devices for easier access.
8. This time next week, experts **will be discussing / will discuss** the evolution of multi-factor authentication techniques at the security conference.

B. Put the verbs into the correct future tenses: the future simple, the future continuous, the future perfect, the future perfect continuous.

1. I believe that companies _____ **(implement)** biometric systems that analyse voice patterns, increasing security in customer service interactions.
2. In the near future, users _____ **(be able)** to combine security tokens with biometrics, creating a robust layer of protection against unauthorised access.
3. By the end of the year, we _____ **(finish)** the course "Biometrics".
4. At this time next month, I _____ **(work)** on the project titled "AI and Biometric systems".

5. By the end of the year, our company _____ **(use)** biometric systems for three months.
6. By the time the new security protocols are implemented, our company _____ **(educate)** the employees about password hygiene for several months.
7. By the end of September, the users _____ **(change)** their passwords for three months.
8. Instead of traditional passwords, I think we _____ **(see)** a lot of people using biometric authentication methods.

SPEAKING

7. **Work in groups. Choose one of the rubrics and discuss the questions.**

1. Identification, verification, authentication, authorisation.

1. What are the differences between identification and authentication in the context of information security?
2. How does the verification process enhance the reliability of user identity?
3. Why is it important to implement multi-factor authentication as part of a robust authentication strategy?
4. In what ways can the principle of least privilege be applied during the authorisation process?

2. Passwords.

5. What are the characteristics of a strong password? Why are they important in protecting accounts?
6. How often should passwords be changed? What are the best practices for managing password rotation?
7. What are the potential risks associated with using the same password across multiple accounts?
8. How do password managers help in enhancing password security for users?

3. Biometrics.

9. What are the most common types of biometric authentication methods currently in use?
10. What are the privacy concerns associated with the storage and use of biometric data?
11. How can biometric systems be vulnerable to spoofing or fraud?
12. What role will biometrics play in the future of secure access management?

4. Security tokens.

13. What is a security token?
14. How does it differ from traditional authentication methods?
15. What challenges do companies face when implementing security token systems for users?
16. How can companies educate users on the importance of securing their security tokens to prevent unauthorised access?

8. Work in groups. Create a mind map that visually represents the relationships between the following concepts: identification, verification, authentication, authorisation; passwords, biometrics; security tokens. Each group member has to present one of these concepts, focusing on its connections to the others and its significance within the context of information security. Highlight how these concepts interact with and support each other in protecting information assets.

WRITING

9. **You are asked to write a paragraph (120–150 words) on one of the topics given below.**

Use any five phrasal verbs: *go through, give out, keep track of, go over, give up, keep up with, go along with, give rise to, play with, put in place, keep out, put to use, put off*.

1. **Identification, verification, authentication, authorisation.**
2. **Passwords.**
3. **Biometrics.**
4. **Security tokens.**

10. **To participate in the *Opinion Essay Contest*, you need to write an essay (180–200 words) on one of the topics given below. Your essay should follow a clear structure, consisting of an introduction, main body, and conclusion.**

Additionally, you must incorporate the idioms: *to lock up your secrets, never put all my keys in one basket, change the locks regularly, go the extra mile, leaving the front door wide open, hedging the bet, keep the keys close, riding the compliance wave, building a fortress, bridging the trust gap, charting the compliance waters*.

A. Use at least seven idioms.

B. Use at least ten idioms.

Topics:

1. **Identification, verification, authentication, authorisation.**
2. **Passwords.**
3. **Biometrics.**
4. **Security tokens.**

PROJECT

11. **1. Work in small groups in terms of the project "The Future of Authentication: Designing a Secure Digital Environment for a New Bank".**

Objective: explore and design a hypothetical secure authentication system for a newly opening bank, using a variety of authentication methods while meeting the requirements of the bank's information security department to improve security.

Project Outline:

System Design Phase: **design a secure authentication system tailored for the bank; outline how the system will manage identification, verification, authentication, and authorisation processes specific to banking needs.**

Authentication Mechanisms: **discuss a mix of authentication methods, the use of strong password policies, implementing biometric solutions (for example, facial recognition, fingerprint scanning, etc.), and integrating security tokens (like one-time passwords or authentication apps) to ensure a strong security framework.**

Risk Assessment: **conduct a thorough risk assessment to identify potential security threats that the bank might face, such as phishing attacks or identity theft; propose solutions to mitigate these risks and develop a list of best practices for users to enhance security.**

Prototype Development: **create a visual representation of their authentication system's user interface, and demonstrate how customers interact with the system when opening accounts, logging in, and conducting transactions securely.**

Presentation: **present the design of the system, the rationale for the authentication methods chosen and the results of the risk assessment to the class; provide constructive feedback on the projects.**

References

UNIT 1

1.1. IT Project Management Methods

1. AI Text Generator [Electronic resource]. – Access link : https://deepai.org/chat/text-generator
2. DevOps In 5 Minutes. What Is DevOps? [Electronic resource]. – Access link : https://www.youtube.com/watch?v=Xrgk023l4lI&t=9s
3. Reaiche C., Papavasiliou S. Management methods for complex projects. James Cook University, 2022. – [Electronic resource]. – Access link : https://researchonline.jcu.edu.au/78851/
4. Today's Top 10 Agile Quotes and Ideas [Electronic resource]. – Access link : https://blog.iil.com/todays-top-10-agile-quotes-and-ideas/

1.2. Types of Websites

1. AI Text Generator [Electronic resource]. – Access link : https://deepai.org/chat/text-generator
2. Popular Types of Websites That You Should Know [Electronic resource]. – Access link : https://www.youtube.com/watch?v=0tu9PjwiAwk
3. Static and dynamic websites [Electronic resource]. – Access link : https://en.wikipedia.org/wiki/Website
4. Top 25 Web Development Quotes: Inspirational and Motivational [Electronic resource]. – Access link : https://shourai.io/blog/2020/11/13/top-25-web-development-quotes-inspirational-and-motivational/

1.3. Website Design. Security of Websites

1. AI Text Generator [Electronic resource]. – Access link : https://deepai.org/chat/text-generator
2. How to Perform a Website Security Check [Electronic resource]. – Access link : https://www.youtube.com/watch?v=ENvlIBxo9Es
3. Top 25 Web Development Quotes: Inspirational and Motivational [Electronic resource]. – Access link : https://shourai.io/blog/2020/11/13/top-25-web-development-quotes-inspirational-and-motivational/
4. Trust T. Web Design Basics for Educators. 2019. [Electronic resource]. – Access link : https://edtechbooks.org/webdesign/interfacedesign

1.4. Web Servers. Security of Webservers

1. AI Text Generator [Electronic resource]. – Access link : https://deepai.org/chat/text-generator
2. AZ Quotes [Electronic resource]. – Access link : https://www.azquotes.com/quotes/topics/server.html
3. Demystifying Web Server Hacking: Techniques, Vulnerabilities, and Counter-measures [Electronic resource]. – Access link : https://www.youtube.com/watch?v=5pTHvFABSzc
4. Web Development and Programming [Electronic resource]. – Access link : https://eng.libretexts.org/Bookshelves/Computer_Science/Web_Design_and_Development/Book%3A_Web_Development_and_Programming_(Mendez)/01%3A_Web_Development/1.03%3A_Web_Servers

UNIT 2

2.1. Classical Cryptography. Ciphers and Codes

1. AI Text Generator [Electronic resource]. – Access link : https://deepai.org/chat/text-generator
2. AZ Quotes [Electronic resource]. – Access link : https://www.azquotes.com/quotes/topics/server.html
3. Cipher [Electronic resource]. – Access link : https://en.wikipedia.org/wiki/Cipher
4. Secret Codes: A History of Cryptography (Part 1) [Electronic resource]. – Access link : https://www.youtube.com/watch?v=9pp9YpginNg
5. Kerckhoffs's principle [Electronic resource]. – Access link : https://en.wikipedia.org/wiki/Kerckhoffs%27s_principle
6. Rosulek M. The Joy of Cryptography. / M. Rosulek, School of Electrical Engineering & Computer Science Oregon State University, Corvallis, Oregon, USA, 2021. – 275 p. [Electronic resource]. – Access link : https://open.umn.edu/opentextbooks/textbooks/897
7. Trevisan L. Cryptography. Lecture Notes from CS276, Spring 2009. / L. Trevisan, Stanford University, 2009. – 154 p. [Electronic resource]. – Access link : https://lucatrevisan.github.io/books/crypto.pdf
8. Wonderful Cryptography [Electronic resource]. – Access link : https://mrxor.github.io/cryptoquotes.html

2.2. Cryptanalysis

1. AI Text Generator [Electronic resource]. – Access link : https://deepai.org/chat/text-generator
2. Attack model [Electronic resource]. – Access link : https://en.wikipedia.org/wiki/Attack_model
3. Cryptanalysis [Electronic resource]. – Access link : https://en.citizendium.org/wiki/Cryptanalysis
4. OpenWorkbook of Cryptology. A project-based introduction to crypto in Python [Electronic resource]. – Access link : http://www.freetechbooks.com/open-workbook-of-cryptology-a-project-based-introduction-to-crypto-in-python-t1378.html
5. The science of codes: an intro to cryptography [Electronic resource]. – Access link : https://www.youtube.com/watch?v=-yFZGF8FHSg
6. What is cryptanalysis? [Electronic resource]. – Access link : https://www.youtube.com/watch?v=PAylKVVSW-0
7. Wonderful Cryptography [Electronic resource]. – Access link : https://mrxor.github.io/cryptoquotes.html

2.3. Steganography

1. AI Text Generator [Electronic resource]. – Access link : https://deepai.org/chat/text-generator
2. How to Hide Data Inside Images (Steganography) [Electronic resource]. – Access link : https://www.youtube.com/watch?v=u1oTteKYWEk
3. Steganography [Electronic resource]. – Access link : https://en.wikipedia.org/wiki/Steganography

4. Sajedi H. Recent Advances in Steganography / H. Sajedi, University of Tehran, Iran, 2012. – 102 p. [Electronic resource]. – Access link : https://www.intechopen.com/books/2092
5. Steganography [Electronic resource]. – Access link : https://en.citizendium.org/wiki/Steganography

2.4. Digital Watermarking

1. AI Text Generator [Electronic resource]. – Access link : https://deepai.org/chat/text-generator
2. Digital watermarking [Electronic resource]. – Access link : https://en.wikipedia.org/wiki/Digital_watermarking
3. Digital Watermarking [Electronic resource]. – Access link : https://www.youtube.com/watch?v=763ELerm_rA
4. McClanahan P. Information Security / P. McClanahan, San Joaquin Delta College, LibreTexts [Electronic resource]. – Access link : https://eng.libretexts.org/Courses/Delta_College/Information_Security/5%3A_Cryptography/5.7%3A_Cryptography_Applications
5. Ramakrishnan S. Digital Image and Video Watermarking and Steganography / S. Ramakrishnan, IntechOpen, 2019. – 90 p.

UNIT 3

3.1. Identification. Verification. Authentication. Authorisation. Accounting

1. AAA – Authentication, Authorisation, and Accounting [Electronic resource]. – Access link : https://www.youtube.com/watch?v=MVYswO4QI8c&t=26s
2. AI Text Generator [Electronic resource]. – Access link : https://deepai.org/chat/text-generator
3. BrainyQuote [Electronic resource]. – Access link : https://www.brainyquote.com/quotes/ronald_reagan_147717?src=t_verify
4. Identification – What is it? What is verification? [Electronic resource]. – Access link : https://eng.libretexts.org/Courses/Delta_College/Information_Security/02%3A_Authenticate_and_Identify/2.1%3A_Identification
5. What is authentication? [Electronic resource]. – Access link : https://eng.libretexts.org/Courses/Delta_College/Information_Security/02%3A_Authenticate_and_Identify/2.2%3A_Authentication
6. Authentication [Electronic resource]. – Access link : https://en.wikipedia.org/wiki/Authentication
7. Authorisation [Electronic resource]. – Access link : https://en.wikipedia.org/wiki/Authorization

3.2. Passwords

1. AI Text Generator [Electronic resource]. – Access link : https://deepai.org/chat/text-generator
2. Password [Electronic resource]. – Access link : https://eng.libretexts.org/Courses/Delta_College/Information_Security/02:_Authenticate_and_Identify/2.3:_Authentication_Methods_-_Password
3. Password [Electronic resource]. – Access link : https://en.wikipedia.org/wiki/Password
4. Password Quotes [Electronic resource]. – Access link : https://www.goodreads.com/quotes/tag/password
5. AZ Quotes [Electronic resource]. – Access link : https://www.azquotes.com/quotes/topics/passwords.html
6. What's wrong with your pa$$w0rd? [Electronic resource]. – Access link : https://www.youtube.com/watch?v=0SkdP36wiAU

3.3. Biometrics

1. AI Text Generator [Electronic resource]. – Access link : https://deepai.org/chat/text-generator
2. Authentication Methods – Biometrics [Electronic resource]. – Access link : https://eng.libretexts.org/Courses/Delta_College/Information_Security/02:_Authenticate_and_Identify/2.3:_Authentication_Methods_-_Password/2.3.2:_Authentication_Methods_-_Biometrics
3. Facial recognition system [Electronic resource]. – Access link : https://en.wikipedia.org/wiki/Facial_recognition_system
4. What is Biometrics and How Safe is it? [Electronic resource]. – Access link : https://www.youtube.com/watch?v=GytLOow-7OY

3.4. Security Tokens

1. AI Text Generator [Electronic resource]. – Access link : https://deepai.org/chat/text-generator
2. Authentication Methods – Security Tokens [Electronic resource]. – Access link : https://eng.libretexts.org/Courses/Delta_College/Information_Security/02%3A_Authenticate_and_Identify/2.3%3A_Authentication_Methods_-_Password/2.3.3%3A_Authentication_Methods_-_Security_Tokens
3. Smart Card Introduction [Electronic resource]. – Access link : https://www.youtube.com/watch?v=_iEnR6doeSA

Appendix 1. Mini-Dictionary

1.1. IT PROJECT MANAGEMENT METHODS

1	project management	управління проєктами
2	software development projects	проєкти розробки програмного забезпечення
3	agile software development	гнучка розробка програмного забезпечення
4	increment	приріст
5	to adjust	регулювати
6	manifesto	маніфест
7	sustainable development	сталий розвиток
8	stakeholders and developers	зацікавлені сторони та розробники
9	rapid deployment of solutions	швидке розгортання рішень
10	iteration	ітерація
11	cumbersome methodologies	громіздкі методики
12	customer requirements	вимоги замовника
13	increased flexibility and adaptability to change	підвищена гнучкість і здатність до змін
14	fast turnaround times	швидкий час виконання
15	a constant pace	постійний темп
16	optimal project outcomes	оптимальні результати проєкту
17	face-to-face meetings	очні зустрічі
18	to streamline	впорядкувати
19	to identify and adjust for issues and defects	виявляти та усувати проблеми і недоліки
20	scrum	скрам
21	a product backlog	беклог продукту
22	sprint planning	планування спринту
23	update the content	оновити вміст
24	agile frameworks	гнучкі фреймворки
25	to assess progress	оцінити прогрес
26	a sprint review and retrospective	огляд спринту та ретроспектива
27	the budget is depleted	бюджет виснажується
28	hybrid solution	гібридне рішення
29	static website, dynamic website	статичний вебсайт, динамічний вебсайт
30	corporate and government website	корпоративний та державний сайт
31	currency of information	актуальність інформації
32	authority	повноваження
33	accuracy	точність
34	navigation	навігація
35	functionality	функціональність
36	feedback	зворотній зв’язок
37	consistency	послідовність

38	website map	карта сайту
39	usability	зручність використання
40	assessing the quality of information	оцінка якості інформації

1.2. TYPES OF WEBSITES

1	website	вебсайт
2	web pages	вебсторінки
3	hyperlinking	гіперпосилання
4	to store	зберігати
5	navigation	навігація
6	structure and functionality	структура та функціональність
7	a dynamic website	динамічний вебсайт
8	non-interactive	неінтерактивний
9	to make updates periodically	періодично оновлюватись
10	to require	вимагати
11	a manual process to edit the text	ручний процес редагування тексту
12	a five-page website	п’ятисторінковий сайт
13	static websites	статичні вебсайти
14	pre-defined	заздалегідь визначені
15	to lack interactive features, personalised content, and scalability	не мають інтерактивних функцій, персоналізованого контенту та масштабованості
16	hosting	хостинг
17	to customise	налаштовувати
18	to generate dynamic web systems	створювати динамічні вебсистеми
19	web template systems	системи вебшаблонів
20	to retrieve	отримувати
21	to simulate a certain type of dynamic website	моделювати певний тип динамічного вебсайту
22	eCommerce websites, Business websites	вебсайти електронної комерції, бізнес-сайти
23	Blog websites	вебсайти блогів
24	Portfolio websites	вебсайти портфоліо
25	Personal websites	персональні сайти
26	Landing pages	цільові сторінки
27	Membership websites	членські вебсайти
28	Booking websites	вебсайти для бронювання
29	Nonprofit websites	некомерційні вебсайти
30	Online forums, School websites, Informational websites, Community websites, Consulting websites	онлайн-форуми, шкільні вебсайти, інформаційні вебсайти, вебсайти спільнот, консультаційні вебсайти
31	to store	зберегти
32	a customised domain	індивідуальний домен
33	insights into your personality	розуміння вашої особистості
34	a one-stop hub	універсальний центр

35	landing pages	цільові сторінки
36	non-gated pages	незамкнені сторінки
37	membership websites	членські сайти
38	link	посилання
39	to expand your reach	розширити свою аудиторію
40	to boost	збільшити

1.3. WEBSITE DESIGN. SECURITY OF WEBSITES

1	easy-to-use	простий у використанні
2	accessible, well-designed, easy-to-scan, easy-to-navigate	доступний, добре продуманий, легко сканується, зручний для навігації
3	to identify the purpose of your site	визначити мету вашого сайту
4	website development	розробка сайту
5	target audience	цільова аудиторія
6	to keep track of …	відстежувати ...
7	to end up serving several different purposes	в кінцевому підсумку служити декільком різним цілям
8	to simplify the initial design process	спростити початковий процес проєктування
9	building a website	створення вебсайту
10	to set up your page	налаштувати вашу сторінку
11	to reduce potential frustration	зменшити потенційне розчарування
12	to incorporate into your site design	включити в дизайн вашого сайту
13	to sketch out your website organisation	накидати ескіз організації вашого сайту
14	layout and content	макет і контент
15	the menu, the banner or logo, the navigation bar, contact information, and social network icons	меню, банер або логотип, панель навігації, контактну інформацію та іконки соціальних мереж
16	to take back to the home page	повернутися на головну сторінку
17	to keep with this tradition on your site	підтримувати цю традицію на вашому сайті
18	to depict the typical placement of common website elements	відображати типове розміщення типових елементів сайту
19	consistency	послідовність
20	to attract attention and increase readership	привернути увагу та збільшити кількість читачів
21	anything that requires scrolling	все, що вимагає прокрутки
22	an attention-grabbing heading	заголовок, що привертає увагу
23	to keep in mind	запам’ятовувати
24	navigation	навігація
25	serial position effect, within-page linking	ефект послідовного розташування, внутрішньосторінкова перелінковка
26	search engines	пошукові системи
27	visual hierarchy	візуальна ієрархія

28	too many colours can be overwhelming and distracting	надмірна кількість кольорів може перевантажувати та відволікати увагу
29	to limit yourself to no more than 3 fonts; to reduce visual clutter	обмежитися не більше ніж 3-ма шрифтами; зменшити візуальне захаращення
30	accessibility, adaptability	доступність, адаптивність
31	vulnerabilities	вразливості
32	injected spam	інжектований спам
33	digging deep into the root of your code	глибоко копатися в корені вашого коду
34	plugins	плагіни
35	outdated, updated	застарілі, оновлені
36	brute forcing programs	програми грубого перебору
37	arduous	важкий
38	restricting user permissions	обмеження прав користувачів
39	innocuous	нешкідливий
40	the expired certificate	прострочений сертифікат

1.4. WEB SERVERS. SECURITY OF WEB SERVERS

1	hardware and software components	апаратні та програмні компоненти
2	the data center, hosting provider	дата-центр, хостинг-провайдер
3	to accompany	супроводжувати
4	an accurate portrayal	точне зображення
5	an internet connected server	підключений до Інтернету сервер
6	to reinvent this concept	переосмислити цю концепцію
7	to reduce costs	зменшити витрати
8	backup	резервне копіювання
9	enough emergency power to keep running	достатнє аварійне живлення для продовження роботи
10	low powered devices	малопотужні пристрої
11	“just-enough-power” devices	пристрої достатньої потужності
12	web server	вебсервер
13	a database	база даних
14	a scripting language	скриптова мова
15	operating systems	операційні системи
16	the plethora of combinations	безліч комбінацій
17	the catch-all reference	універсальний довідник
18	to facilitate resource allocation	полегшити розподіл ресурсів
19	robust	надійний, потужний
20	to expand on	розширювати
21	to contribute to	сприяти
22	to compile	збирати
23	to track	відстежувати
24	the end user	кінцевий користувач
25	configuration files	конфігураційні файли

26	to allow us to share our web pages	дозволити нам ділитися нашими вебсторінками
27	the client's browser displays	відображати браузер клієнта
28	to view them as a destination on a network	переглядати їх як пункт призначення в мережі
29	a similar open source approach as Linux	подібний підхід з відкритим вихідним кодом, як у Linux
30	a large number of Linux-based operating systems	велика кількість операційних систем на базі Linux
31	countermeasures	контрзаходи
32	patch management	управління виправленнями
33	security tools	інструменти безпеки
34	vulnerabilities	вразливості
35	a built-in database	вбудована база даних
36	to be compromised	бути скомпрометованим
37	external systems	зовнішні системи
38	the website get defaced	вебсайт може бути пошкоджений
39	open-source web server architecture	архітектура вебсервера з відкритим вихідним кодом
40	IIS web server architecture	архітектура вебсервера IIS

2.1. CLASSICAL CRYPTOGRAPHY. CIPHERS AND CODES

1	cryptography, cryptology	криптографія, криптологія
2	plaintext, ciphertext	відкритий текст, зашифрований текст
3	eavesdropper	підслуховувач
4	to eave	підслуховувати
5	cipher, code	шифр, код
6	to encipher, decipher	шифрувати, розшифровувати
7	to encode, decode	кодувати, розшифровувати
8	to encrypt, decrypt	зашифровувати, розшифровувати
9	Kerckhoffs' Principle	принцип Керкгоффа
10	to be kept secret from sb.	тримати в таємниці від будь-кого
11	major drawbacks	основні недоліки
12	to prevent everyone from reading everyone else's messages	щоб ніхто не міг прочитати чужі повідомлення
13	to recover security	відновити безпеку
14	indecipherable	нерозбірливий
15	to be applicable	бути застосовним
16	to handle or operate	оброблювати або експлуатувати
17	the secret key	секретний ключ
18	to be concentrated in the secrecy of the key	бути сконцентрованим на секретності ключа
19	to interpret Kerckhoffs' principle	інтерпретувати принцип Керкгоффа

20	safely use the same encryption algorithm	безпечно використовувати один і той самий алгоритм шифрування
21	key generation	генерація ключів
22	to substitute different length strings of characters	підставляти рядки символів різної довжини
23	block ciphers	блокові шифри
24	symmetric key algorithms, asymmetric key algorithms	алгоритми з симетричним ключем, алгоритми з асиметричним ключем
25	public / private key	відкритий / закритий ключ
26	hiding writing	приховуване письмо
27	transposition, substitution	перестановка, заміна
28	skytale, rod	розповідь, паличка
29	scrambling	скремблювання, перестановка
30	interceptor	перехоплювач
31	to rearrange, to replace, to shift	переставляти, замінювати, зміщувати
32	a wannabe code breaker, a cunning and intelligent code breaker	зломщик коду, хитрий і розумний зломщик коду
33	monoalphabetic	моноалфавітний
34	flaw	недолік, дефект
35	treatise	трактат
36	mishmash	мішанина
37	wrench	ключ
38	misspell	помилка
39	constantly bickering	постійно сваритися
40	encrypted message	зашифроване повідомлення

2.2. CRYPTANALYSIS

1	cryptanalysis	криптоаналіз
2	defeating	злам
3	accessing the plaintext content	доступ до відкритого вмісту
4	weakness	вразливість
5	cryptanalysts	криптоаналітики
6	ciphertext	зашифрований текст
7	malicious attackers	зловмисники
8	misconception	омана
9	unbreakable	незламний
10	adversary	супротивник
11	to intercept	перехопити
12	encrypted message	зашифроване повідомлення
13	to compromise	скомпрометувати
14	ciphertext-only attack	атака тільки на зашифрований текст
15	brute force attack or exhaustive key search	атака грубою силою або вичерпний перебір ключів

16	known-plaintext attack	атака за відомим відкритим текстом
17	chosen-plaintext attack	атака за обраним відкритим текстом
18	adaptive chosen-plaintext attack	адаптивна атака відкритим текстом
19	chosen-ciphertext attack	атака по зашифрованому тексту
20	lunchtime attack or midnight attack	обідня атака або опівнічна атака
21	adaptive chosen-ciphertext attack	адаптивна атака з вибраним шифрованим текстом
22	open key model attacks	атаки за моделлю відкритого ключа
23	related-key attack	атака пов'язаного ключа
24	known-key distinguishing attack and chosen-key distinguishing attack	атака з відомим ключем та атака з обраним ключем
25	side-channel attack	атака побічного каналу
26	evil maid attack	атака злої покоївки
27	plaintext	відкритий текст
28	resistant	стійкий
29	vulnerable	вразливий
30	an arbitrary ciphertext	довільний шифротекст
31	frequency analysis	частотний аналіз
32	weaknesses	слабкі місця
33	to encrypt a message	шифрувати повідомлення
34	nonrandom	невипадковий
35	Enigma encrypted messages	зашифровані повідомлення Enigma
36	to be exponentially dependent on the key size	експоненціально залежить від розміру ключа
37	no better chance of guessing the contents	не кращі шанси вгадати вміст
38	differential cryptanalysis / linear cryptanalysis	диференціальний криптоаналіз / лінійний криптоаналіз
39	cryptanalysis tools	інструменти криптоаналізу
40	to disclose	розкрити

2.3. STEGANOGRAPHY

1	steganography	стеганографія
2	human inspection	людський контроль
3	to be concealed within another file, message, image, or video	бути прихованим в іншому файлі, повідомленні, зображенні або відео
4	digital steganographic systems	цифрові стеганографічні системи
5	carrier	носій
6	payload	корисне навантаження
7	channel	канал
8	package, stego file, or covert message	пакет, стего-файл або приховане повідомлення
9	encoding density	щільність кодування
10	suspect	підозрюваний

11	candidate	кандидат
12	a JPEG image	зображення у форматі JPEG
13	plainly visible encrypted messages	явно видимі зашифровані повідомлення
14	incriminating	що викривають
15	an innocuous image file	нешкідливий графічний файл
16	subtle	прихований
17	physical steganography	фізична стеганографія
18	invisible ink on paper	невидиме чорнило на папері
19	cultural or social steganography	культурна або соціальна стеганографія
20	an alternate meaning	альтернативне значення
21	digital or electronic steganography	цифрова або електронна стеганографія
22	a block of random data	блок випадкових даних
23	steganalysis, stego-analytical algorithms	стеганоаналіз, стегоаналітичні алгоритми
24	chosen stego attack	обрана стегоатака
25	known cover attack	відома атака прикриття
26	known stego attack	відома стего-атака
27	stego only attack	атака тільки на стего
28	chosen message attack	атака обраного повідомлення
29	known message attack	атака з відомим повідомленням
30	passive steganalysis, active steganalysis	пасивний стеганоаналіз, активний стеганоаналіз
31	ordinary-looking files	звичайні файли
32	scrambling	скремблювання
33	backmasking	маскування
34	identical	ідентичні
35	retrieved	знайдено
36	embedding	вбудовування
37	data hiding techniques	методи приховування даних
38	histograms	гістограми
39	stego version	стего-версія
40	undetectability	невиявленість

2.4. DIGITAL WATERMARKING

1	digital watermarking	цифрові водяні знаки
2	to embed	вбудовувати
3	hiding digital information	приховування цифрової інформації
4	a carrier signal	несучий сигнал
5	to verify the authenticity or integrity of the carrier signal	перевірити автентичність або цілісність несучого сигналу
6	the identity of its owners	ідентифікація власників
7	to trace copyright infringements	відстежувати порушення авторських прав
8	to distort	спотворювати
9	to change the size of the carrier signal	змінювати розмір несучого сигналу
10	a fragile watermark	крихкий водяний знак

11	to control the robustness	контролювати стійкість
12	a passive protection tool	інструмент пасивного захисту
13	the difference between the watermarked signal and the cover signal	різниця між сигналом з водяним знаком і сигналом прикриття
14	embedding, attack, and detection	вбудовування, атака та виявлення
15	to be transmitted or stored	передавати або зберігати
16	to make a modification	вносити зміни
17	to crop an image or video	обрізати зображення або відео
18	an attack	атака
19	to remove the digital watermark through modification	видаляти цифровий водяний знак шляхом модифікації
20	detection	виявлення
21	fragile digital watermarking	крихкий цифровий водяний знак
22	robust	надійний
23	imperceptible	непомітний
24	tamper detection	виявлення несанкціонованого доступу
25	after malignant transformations	після злоякісних перетворень
26	imperceptible, perceptible	непомітний, відчутний
27	transparent / translucent	прозорий / напівпрозорий
28	the embedded message	вбудоване повідомлення
29	an additive modification	адитивна модифікація
30	interference	втручання
31	visible versus invisible	видимий, невидимий
32	fragile versus robust	крихкий, міцний
33	preventive versus detective controls	превентивний, детективний контроль
34	forgery and tampering detection	виявлення підробок і несанкціонованого втручання
35	to deter errors or irregularities, verifying authenticity and integrity of files to show ownership	запобігати помилок або порушень, перевіряючи автентичність та цілісність файлів для підтвердження права власності
36	digital extraction process	процес цифрового вилучення
37	to figure out some new technology	розібратися в новій технології
38	forgery and tampering detection	виявлення підробки та втручання
39	imprinted logos and photographs	надруковані логотипи та фотографії
40	obust	об’ємний

3.1. IDENTIFICATION. VERIFICATION. AUTHENTICATION. AUTHORISATION. ACCOUNTING

1	authentication	аутентифікація
2	authorisation	авторизація
3	verification	перевірка
4	identification	ідентифікація
5	authentication factors	фактори автентифікації
6	the knowledge factors	фактори знань
7	the ownership factors	фактори власності
8	the inherence factors	фактори невід'ємності
9	the location factors	фактори місцезнаходження
10	multi-factor authentication	багатофакторна автентифікація
11	to prove one's identity	підтвердити особу
12	to transmit data automatically	передавати автоматично дані
13	mutual authentication	взаємна автентифікація
14	identity verification	перевірка особи
15	a high degree of confidence	високий ступінь довіри
16	to verify someone's identity	перевірити чиюсь особу
17	a "frictionless" onboarding process	"безпроблемний" процес приєднання до команди
18	the level of assurance	рівень впевненості
19	identity "proofing" or "vetting"	"підтвердження" або "перевірка" особи
20	to validate the personal information	перевірити особисту інформацію
21	numerous regulatory acts to prevent fraudsters	численні нормативні акти для запобігання шахрайства
22	to set up false bank accounts	створення фальшивих банківських рахунків
23	laundering money	відмивання грошей
24	verification methods	методи верифікації
25	a prerequisite to allowing access to resources in an information system	передумовою для надання доступу до ресурсів в інформаційній системі
26	to grant access	надавати доступ
27	approving a transaction request	схвалення запиту на транзакцію
28	cell phone with built-in hardware token	мобільний телефон з вбудованим апаратним токеном
29	to protect the user from an unknown person	захищати користувача від невідомої особи
30	to supply the identity	надавати ідентифікаційні дані
31	the backbone of online data protection	основа захисту даних в Інтернеті
32	granting access to information or resources	надання доступу до інформації або ресурсів
33	a verification code on your phone	код підтвердження на телефоні
34	to navigate and protect our online presence	керувати та захищати нашу присутності в Інтернеті

35	invisible fortress	невидима фортеця
36	discretionary access control	дискреційний контроль доступу
37	mandatory access control	обов’язковий контроль доступу
38	role-based access control	рольовий контроль доступу
39	a gatekeeper	привратник
40	a verified user	верифікований користувач

3.2. PASSWORDS

1	a password-protected system	захищена паролем система
2	deterring	стримування
3	to hide passwords	приховувати паролі
4	to prevent bystanders from reading the password	запобігати зчитування пароля сторонніми особами
5	to choose weak / strong passwords	підбирати слабкі / сильні паролі
6	to acquire a password	підбір пароля
7	to make password attacks	здійснювати парольні атаки
8	brute-force attack	атака грубою силою
9	a unique password	унікальний пароль
10	reusing their password	повторне використання пароля
11	password data	дані пароля
12	have a mix of uppercase and lowercase letters, digits, symbols	мають мікс великих і малих літер, цифр, символів
13	to measure of password strength	вимірювати стійкості пароля
14	cracking passwords	злом паролів
15	stolen password sets	викрадені набори паролів
16	passcode / password	пароль
17	passphrase	парольна фраза
18	to guess	вгадати
19	to reduce the security of a system	знизити рівень безпеки системи
20	frequent password resets	часте скидання пароля
21	to gain unauthorised access to accounts or systems	отримати несанкціонований доступ до облікових записів або систем
22	dictionary attack	атака за словником
23	phishing	фішинг
24	credential stuffing	наповнення облікових даних
25	keylogging	кейлоггінг
26	password spraying	розпилення паролів
27	Man-in-the-Middle attack	атака «людина посередині»
28	cracking and sniffing	злом і перехоплення
29	unencrypted data	незашифровані дані
30	to intercept	перехоплення
31	password managers	менеджери паролів

32	monitoring login activities for suspicious behavior	моніторинг активності входу в систему на предмет підозрілої поведінки
33	conducting periodic security audits	проведення періодичних аудитів безпеки
34	graphical passwords	графічні паролі
35	click-based passwords	паролі на основі кліків
36	pattern-based passwords	паролі на основі шаблонів
37	to mitigate vulnerabilities	зменшувати вразливості
38	3D passwords	3D-паролі
39	integrating multi-dimensional authentication factors	інтеграція багатовимірних факторів автентифікації
40	robust defense	надійний захист

3.3. BIOMETRICS

1	biometrics	біометрія
2	human characteristics	людські характеристики
3	a form of identification and access control	форма ідентифікації та контролю доступу
4	to identify individuals	ідентифікувати осіб
5	physiological versus behavioral characteristics	фізіологічні та поведінкові характеристики
6	fingerprint, palm veins, face recognition, DNA	відбитки пальців, вени долоні, розпізнавання обличчя, ДНК
7	palm print, hand geometry, iris recognition, retina and odor / scent	відбиток долоні, геометрія руки, розпізнавання райдужної оболонки ока, сітківки та запаху
8	gait, keystroke, signature, behavioral profiling, and voice	хода, натискання клавіш, підпис, поведінкове профілювання та голос
9	biometric authentication	біометрична автентифікація
10	human physiology	фізіологія людини
11	assessing the suitability of any trait for use in biometric authentication	оцінка придатності будь-якої ознаки для використання в біометричній автентифікації
12	universality	універсальність
13	uniqueness	унікальність
14	permanence	постійність
15	measurability	вимірність
16	acceptability	прийнятність
17	circumvention	обхід
18	verification (or authentication) mode	режим верифікації (або автентифікації)
19	one-to-one comparison	порівняння один до одного
20	to verify the individual	верифікувати особу
21	threshold	поріг, межа
22	a smart card, username or ID number (e.g. PIN)	смарт-карта, ім’я користувача або ідентифікаційний номер (наприклад, PIN-код)

23	identification mode	режим ідентифікації
24	“positive recognition” or “negative recognition” of the person	«позитивне розпізнавання» або «негативне розпізнавання» особи
25	enrollment	реєстрація
26	the matching phase	етап зіставлення
27	biometric data	біометричні дані
28	user requirements	вимоги користувача
29	to estimate	оцінювати
30	identity theft deterrence	запобігання крадіжці особистих даних
31	replacement	заміна
32	surveillance	спостереження
33	data breaches	витоки даних
34	identification of individuals	ідентифікація осіб
35	personal data	персональні дані
36	permanently compromised	постійно скомпрометовані
37	proof of identity	підтвердження особи
38	encryption	шифрування
39	to install updates	встановлювати оновлення
40	to keep your devices up to date	підтримувати ваші пристрої в актуальному стані

3.4. SECURITY TOKEN

1	security token / authentication token / token-based authentication	токен безпеки / токен автентифікації / автентифікація на основі токенів
2	a peripheral device	периферійний пристрій
3	to gain access	отримати доступу
4	a bank-provided token	токен, наданий банком
5	to prove identity	підтверджувати особу
6	static password token	статичний токен пароля
7	synchronous dynamic password token	синхронний динамічний токен пароля
8	asynchronous password token	асинхронний токен пароля
9	challenge response token	токен відповіді на виклик
10	to replay attacks	відтворювати атаки
11	a one-time password	одноразовий пароль
12	time-synchronised one-time passwords	синхронізовані за часом одноразові паролі
13	the client’s token	токен клієнта
14	disconnected tokens	відключені токени
15	connected tokens	підключені токени
16	smart card technology	технологія смарт-карт
17	smart-card-based USB tokens	USB-жетони на основі смарт-карт
18	smart card reader	зчитувач смарт-карт
19	contactless tokens	безконтактні токени
20	keyless entry systems	системи безключового доступу

21	a keychain token	брелок-токен
22	single sign-on software tokens	програмні токени єдиного входу
23	to store software	зберігати програмного забезпечення
24	the passwords are stored on the token	на токені зберігаються паролі
25	to store a cryptographic hash of the password	зберігати криптографічний хеш пароля
26	programmable tokens	програмовані токени
27	“drop-in” replacement	«drop-in» заміна
28	to embed	вбудовувати
29	VPN access	доступ до VPN
30	email signature	підпис електронної пошти
31	email encryption	шифрування електронної пошти
32	disk encryption	шифрування диска
33	digital certificate	цифровий сертифікат
34	to unblock	розблокувати
35	to reset	скинути
36	to impersonate	видавати себе за іншу особу
37	to retrieve	отримати
38	hardware vs. software security tokens	апаратні та програмні токени безпеки
39	to plug into the computer	підключити до комп'ютера
40	to require a PIN	вимагати PIN-код

Appendix 2. Phrasal Verbs & Idioms

PHRASAL VERBS

Break

Break down = to analyse or simplify complex design elements into manageable parts.

Break through = to achieve a significant advancement or innovation in web design techniques.

Break away = to deviate from conventional design practices to create a unique user experience.

Bring

Bring up = to raise a topic for discussion, such as design ideas or feedback.

Bring together = to collaborate or combine resources, ideas, or team members for a project.

Bring in = to incorporate new features, styles, or technologies into a website.

Build

Build up = to gradually enhance or improve a website's features or user experience.

Build on = to expand or develop existing designs or ideas further.

Build out = to create additional pages or sections of a website for better functionality and content depth.

Carry

Carry on = to continue with a task or project despite challenges.

Carry out = to execute plans / sprints / tasks effectively.

Carry forward = to take lessons learned or successful practices from one iteration to the next.

Carry through = to complete a project or task.

Change

Change over = to transition from one process or tool to another one.

Change up = to modify strategies or practices.

Change back = to revert to a previous process or approach.

Change around = to reorganise team roles or tasks to enhance efficiency and collaboration.

Change in = to adapt team dynamics or workflows in response to feedback during retrospectives.

Come

Come across = to find or discover something by chance.

Come into play = to something that becomes relevant or applicable in a situation.

Come together = to join people or things.

Deal

Deal out = to distribute or allocate something.

Deal with = to handle, manage, or address a particular situation, issue, or problem.

Decide

Decide against = indicates choosing not to do something.

Decide upon = to make a choice or reach a conclusion after consideration.

Differ

Differ from = to be distinct in some way from someone / something.

Do

Do away with = to stop a certain practice; to eliminate something.

Do over = to redo something.

Do up = to enhance or improve the security features of something.

Fall

Fall back on = to rely on or turn to a backup option when the primary one fails.

Fall into = to categorise various forms of something.

Get

Get across = to effectively communicate.

Get around = to find a way to avoid an obstacle.

Go

Go through = to examine in detail.

Go over = to evaluate the accuracy of information.

Go along with = to accept a proposal.

Give

Give out = to distribute information or credentials.

Give up = to relinquish access or rights to something.

Give rise to = to cause something to happen.

Keep

Keep track of = to monitor or maintain something.

Keep up with = to maintain current knowledge.

Keep out = to prevent something.

Put

Put in place = to establish something.

Put to use = to apply something.

Put off = to delay implementing something.

Play

Play with = to experiment or test something.

IDIOMS

1.2

in the same boat

a red flag

a double-edged sword

breaking the ice

a treasure trove

on the same wavelength

biting off more than they could chew

1.4.

bite the bullet

hit the ground running

burn the midnight oil

the ball is in your court

keep our fingers crossed

cross that bridge when we come to it

the tip of the iceberg

2.2.

spill the beans

under lock and key

read between the lines

an open book

cutting edge

the weakest link

playing cat and mouse

2.4.

a picture is worth a thousand words

keeping their cards close to their chest

don’t throw the baby out with the bathwater

sticking to your guns

draw a line under the issue

an ounce of prevention is worth a pound of cure

a chain is only as strong as its weakest link

3.2.

lock up your secrets

never put all my keys in one basket

change the locks regularly

go the extra mile

leaving the front door wide open

3.4.

hedging the bet

keeping the keys close

riding the compliance wave

building a fortress

bridging the trust gap

charting the compliance waters

Appendix 3. Grammar Bank

PRESENT TENSES

PRESENT SIMPLE

FORMS	USAGE	EXAMPLES	TIME EXPRESSIONS
I work He / she / it work**s** We / you / they work Do I / we / you work? Does he / she / it work? I / we / you / they don't work He / she / it doesn't work	✓ facts and permanent states ✓ general truths ✓ habits and routines ✓ timetables ✓ programmes ✓ reviews	I **often work** on different IT projects.	✓ usually ✓ often ✓ always ✓ every day / week / month

PRESENT CONTINUOUS

FORMS	USAGE	EXAMPLES	TIME EXPRESSIONS
I am working He / she / it is working We / you / they are working Am I working? Are we / you / they working? Is he / she / it working? I'm not working He / she / it isn't working We / you / they aren't working	✓ actions at or around the moment ✓ temporary situations ✓ fixed arrangements	Now I **am working** on the IT project.	✓ now ✓ at the moment ✓ at present ✓ these days ✓ nowdays

1. **Nick is a web designer. Complete the story about him putting the verbs in brackets into the present simple.**

Nick **1)** _____ **(be)** a web designer who **2)** _____ **(enjoy)** his work. Every morning, he **3)** _____ **(arrive)** at his office with a cup of coffee. He **4)** _____ **(check)** his emails and **5)** _____ **(look)** at the latest project updates from his clients. Then he **6)** _____ **(open)** his design software and **7)** _____ **(start)** creating new layouts. Nick **8)** _____ **(focus)** on user experience. He **9)** _____ **(make)** sure that each website is not only beautiful but also functional. In the afternoon, he **10)** _____ **(collaborate)** with his team via video calls. They **11)** _____ **(exchange)** ideas and feedback. At the end of the day, Nick usually **12)** _____ **(feel)** satisfied with his progress and looks forward to tomorrow's challenges.

Borrowed and modified from: https://deepai.org/

2. **Alex is a scrum master. Read the story about him and put the verbs in brackets into the present simple or the present continuous to complete the story.**

Alex is a scrum master. He **1)** _____ **(work)** on different IT projects throughout the year. Now, his team **2)** _____ **(develop)** software for universities to improve student engagement and administrative efficiency. Every day, Alex **3)** _____ **(conduct)** stand-up meetings to check in with his developers and discuss any obstacles they face. As he **4)** _____ **(lead)** the sprint planning sessions, he **5)** _____ **(emphasis)** collaboration and ensures that everyone contributes their ideas.

At the moment, Alex **6)** _____ **(review)** the latest features with his team. They **7)** _____ **(implement)** a user-friendly dashboard that allows students to track their courses and grades easily.

Next month, Alex **8) _____ (go)** to London. He **9) _____ (prepare)** for a conference where he will present his team software. Alex **10) _____ (practice)** his presentation every evening, focusing on how their project addresses the challenges universities face.

He **11) _____ (believe)** that their hard work will make a difference in the education sector, and he feels proud of what they are achieving together.

Borrowed and modified from: https://deepai.org/

3. **You work in the IT field. Write a story (at least 12 sentences) describing your daily activities and what you are currently doing. Use the present simple for routine actions and the present continuous for ongoing tasks. Refer to any of the following IT professions:**

1. Software Developer/Engineer
2. Web Developer
3. Database Administrator
4. Systems Analyst
5. Network Administrator
6. Cybersecurity Analyst
7. Data Scientist
8. Cloud Engineer
9. DevOps Engineer
10. IT Project Manager
11. UX/UI Designer
12. Quality Assurance Tester
13. Game Developer
14. Mobile App Developer
15. Network Architect
16. Artificial Intelligence Engineer

4. Correct the mistakes.

1. Does he works on this IT project?
2. What you know about Agile project management?
3. I am believing that the project will be successful.
4. Is Sam participate in this conference now?
5. Does Kanban a visual management method that focuses on continuous delivery without fixed iterations?
6. Kanban use a board to visualise work items and their progress, allowing teams to manage workflow by limiting work in progress.
7. At the moment, they discuss the difference between Kanban and Lean.
8. Is anything wrong? I just think about our future project.

PRESENT PERFECT

FORMS	USAGE	EXAMPLES	TIME EXPRESSIONS
I have worked He / she / it has worked We / you / they have worked Have I / we / you / they worked? Has he / she / it worked? I / we / you / they haven't worked He / she / it hasn't worked	✓ actions that happened at an unstated time in the past ✓ a recently finished action	I **have already finished working** on this IT project.	✓ for ✓ since ✓ already ✓ just ✓ ever ✓ never ✓ so far

PRESENT PERFECT CONTINUOUS

FORMS	USAGE	EXAMPLES	TIME EXPRESSIONS
I / we / you / they have been working He / she / it has been working Have I been working Have we / you / they been working? Has he / she / it been working? I / we / you / they haven't been working He / she / it hasn't been working	✓ emphasis on the duration of an action which started in the past and continuous up to the present	I **have been working** on this IT project since September.	✓ for ✓ since ✓ how long ✓ all day

5. **Put the verbs into the correct tense. Use the present perfect or the present perfect continuous.**

1. A web developer _____ **(finish)** developing a website.
2. He _____ **(develop)** websites since he graduated from the university.
3. Website security _____ **(become)** increasingly important in the digital age.
4. Tim _____ **(use)** the Agile project methodology for 5 years, but he _____ **(stop)** now working in this field.
5. She _____ **(write)** a scientific paper about different IT project methodologies since October.
6. Businesses _____ **(invest)** in advanced security measures to protect their online assets from potential breaches.
7. Developers _____ **(update)** software to patch vulnerabilities since November. And they continue to do so.
8. Many companies _____ **(implement)** two-factor authentication to enhance user safety during login processes.
9. Security teams _____ **(monitor)** website activity since last Friday, and they are still continuing to do this.
10. Companies _____ **(realise)** the importance of conducting security audits.

6. **Put the verbs in a story into the correct tense. Use the present perfect or the present perfect continuous.**

Patricia, a DevOps engineer, finished her workday at Google feeling accomplished after implementing a new continuous integration pipeline. As she left the office, she saw her friend Ann, a network administrator, sitting in a nearby café. They greeted each other with warm smiles. And they quickly settled into a comfortable corner, eager to share their day.

"I **1) _____ (finish)** just a big project on automating our deployment processes," Patricia said, her excitement evident. "We **2) _____ (work)** on it for weeks, and now it's finally live!" Ann nodded enthusiastically, replying, "That sounds amazing! I **3) _____ (work)** on some connectivity issues with our servers all day. It **4) _____ (be)** quite a challenge, but I think I **5) _____ (resolve)** most of them."

As they enjoyed their coffee, Patricia thought about the past few months. "Since September, I **6) _____ (focus)** on enhancing our cloud infrastructure, and I **7) _____ (join)** some training sessions on Kubernetes." Ann said, "Wow, I **8) _____ (need)** to brush up on that, too! Since then, I **9) _____ (maintain)** network security and upgrading firewalls to keep our systems safe."

Their conversation flowed smoothly into their achievements in the technology industry. "You know," Patricia said, "we **10) _____ (improve)** both really our skills this year. I **11) _____ (start)** even mentoring a new intern!" Ann smiled, "That's great! I **12) _____ (do)** some training sessions for newcomers as well. It feels rewarding to pass on what we **13) _____ (learn)**."

Borrowed and modified from: https://deepai.org/

7. **You work in the IT field. Write a diary entry detailing a typical working day at Google, incorporating at least 12 sentences that highlight your activities. You should describe what you have completed and inform about the projects you have been involved in since last year. Use the present perfect and present perfect continuous tenses. Choose from one of the following IT professions:**

1. Software Developer/Engineer
2. Web Developer

3. Database Administrator
4. Systems Analyst
5. Network Administrator
6. Cybersecurity Analyst
7. Data Scientist
8. Cloud Engineer
9. DevOps Engineer
10. IT Project Manager
11. UX/UI Designer
12. Quality Assurance Tester
13. Game Developer
14. Mobile App Developer
15. Network Architect
16. Artificial Intelligence Engineer

8. **Write a short story about a day in the life of a university student, focusing on his / her study experiences and activities. The story should incorporate at least 7–10 sentences. Use the present perfect and the present perfect continuous tenses. You may reflect on how the student has attended classes, completed assignments, and participated in group projects. Include details about what he / she has been learning, who he/she has been collaborating with, and any challenges he / she has faced throughout the day, how the experiences have contributed to his / her academic growth and engagement in his / her field of study.**

9. **Linda, a game developer at Microsoft, tells a story about her new project. Put the verbs into the correct tense: the present simple, the present continuous, the present perfect, and the present perfect continuous.**

Linda **1) _____ (work)** as a game developer at Microsoft, where she **2) _____ (create)** software aimed at helping children learn mathematics in junior classes. Every day, she **3) _____ (brainstorm)** new ideas and **4) _____ (desing)** interactive elements that make learning fun and exciting. Now, she **5) _____ (develop)** a new game that combines puzzles with basic arithmetic to improve problem-solving skills. This project started in September.

Linda **6) _____ (focus)** on this project for several months now, and she **7) _____ (collaborate)** with educators to make sure that the content aligns with the curriculum. Her team **8) _____ (receive)** great feedback from teachers who **9) _____ (appreciate)** the importance of making math enjoyable for young students. From time to time Linda **10) _____ (test)** and **11) _____ (refine)** different features, ensuring that everything runs smoothly and engages the players.

Recently, she **12) _____ (implement)** successfully a rewards system that encourages children to progress through levels by completing math challenges. Linda **13) _____ (feel)** proud of the progress she **14) _____ (make)** and is excited about sharing the game with schools soon.

Borrowed and modified from: https://deepai.org/

PAST TENSES

PAST SIMPLE

FORMS	USAGE	EXAMPLES	TIME EXPRESSIONS
I worked He worked She worked It worked We worked You worked They worked Did I / we / you / he / she / it work? I / we / you / they / he / she / it didn't work	✓ actions that happened at a definite time in the past ✓ habits in the past ✓ actions that happened immediately after one another in the past	I **worked** on the IT project yesterday.	✓ yesterday ✓ last week ✓ in 2010

PAST CONTINUOUS

FORMS	USAGE	EXAMPLES	TIME EXPRESSIONS
I was working He was working She was working It was working We were working You were working They were working Was I working? Were we / you / they working? Was he / she / it working? I / he / she / it wasn't working We / you / they weren't working	✓ actions which were in progress when another action interrupted it ✓ two or more simultaneous actions in the past ✓ actions that were in progress at a certain time in the past	At 7 o'clock last night, I **was working** on the IT project.	✓ while ✓ when ✓ all morning

10. **Put the verbs into the correct tense. Use the past simple or the past continuous.**

1. While we _____ **(decode)** the encrypted text, the computer suddenly crashed.
2. In ancient times, people _____ **(use)** simple ciphers to protect their messages.
3. During World War II, cryptographers _____ **(work)** hard to decode enemy communications.
4. Yesterday at 7 o'clock I _____ **(prepare)** a presentation on the topic "History of Cryptography".
5. They _____ **(code)** the sensitive information two days ago.
6. At three o'clock yesterday afternoon, we _____ **(try)** to understand the difference between codes and ciphers, cryptography and cryptology, public and private keys.
7. She _____ **(decode)** the message a few minutes ago.
8. Why did cryptography _____ **(become)** a growing industry during the Renaissance?
9. A. Kerckhoffs _____ **(be)** a great Dutch cryptographer, linguist, historian, and mathematician.
10. He _____ **(formulate)** general requirements for a cryptosystem and approved cryptanalysis as the only true way to test ciphers.
11. Yesterday evening, we _____ **(decode)** information from five to seven.
12. He _____ **(code)** a new message when I called him.

11. **Polin is an experienced cryptographer. She told a story that happened with her. To complete the story, put the verbs into the correct past tense: the past simple or the past continuous.**

Polin, an experienced cryptographer, **1)** _____ **(sit)** at her desk last Sunday and **2)** _____ **(think)** about the difficult week she had just had. As she **3)** _____ **(write)** a letter to her friend, she **4)** _____ **(remember)** how she had spent countless hours analysing the company's security systems. Every day, she **5)** _____ **(focus)** intensely on identifying weaknesses, poring over lines of code and testing different algorithms. While she **6)** _____ **(work)** diligently, her colleagues **7)** _____ **(engage)** in their own projects. One afternoon, while she was deep in thought, she **8)** _____ **(realise)** that a critical vulnerability had been overlooked. This discovery **9)** _____ **(push)** her to collaborate with her team, and together they **10)** _____ **(generate)** innovative solutions. On Friday, she **11)** _____ **(be)** exhausted, but a sense of achievement **12)** _____ **(fill)** her heart. Polin **13)** _____ **(end)** her letter by expressing her hope for a quieter week ahead. She couldn't wait to catch her breath and catch up with her friend.

Borrowed and modified from: https://deepai.org/

12. **Write a short story of seven sentences about your experience yesterday at your IT company. Use both the past simple and past continuous tenses to describe the events and experiences you had during the day.**

Choose one of the following professions for your story:

1. Software Developer
2. Web Developer
3. Database Administrator
4. Systems Analyst
5. Network Administrator
6. Cybersecurity Analyst

7. Data Scientist
8. Cloud Engineer
9. DevOps Engineer
10. IT Project Manager
11. UX/UI Designer
12. Quality Assurance Tester
13. Game Developer
14. Mobile App Developer
15. Network Architect
16. Artificial Intelligence Engineer

13. Correct the mistakes.

1. Did he worked for this company last year?
2. While monitoring online activity, the security team was noticing unusual patterns that pointed to a sophisticated phishing scheme.
3. Were you participate in the conference titled “Cryptography: Today and in Future” last week?
4. I was study cryptanalysis attacks at five o’clock afternoon.
5. Last year, a group of hackers successfully was executed a brute-force attack that compromised sensitive data from multiple organisations.
6. He read about the lunchtime attack when the telephone rang.
7. While the researchers analysed the network, they discovered several cryptographic attacks targeting weak encryption algorithms.
8. The analysts were investigating a recent data breach when they were uncovered that the attackers had used social engineering to gain access.
9. During the early days of the internet, many companies were underestimating the risk of cryptographic attacks and failed to secure their digital assets.
10. While they test the security protocols, they identified vulnerabilities that could lead to future cryptographic threats.

PAST PERFECT

FORMS	USAGE	EXAMPLES	TIME EXPRESSIONS
I had worked He had worked She had worked It had worked We had worked You had worked They had worked Had I / we / you / he / she / it / they worked? I / he / she / it / we / you / they hadn't worked	✓ actions that happened before another past action ✓ actions that finished in the past and the results were visible at a later point in the past	I **had finished** working **on** the IT project by 7 o'clock.	✓ for ✓ since ✓ already ✓ just ✓ before ✓ after

PAST PERFECT CONTINUOUS

FORMS	USAGE	EXAMPLES	TIME EXPRESSIONS
I had been working He had been working She had been working It had been working We had been working You had been working They had been working Had I / we / you / they / he / she / it been working? I / he / she / it / we / you / they hadn't been working	✓ emphasis on the duration of an action which started and finished in the past, before another action or stated time in the past	Alex **had been working** on this IT project for 7 days before he finished.	✓ for ✓ since ✓ how long ✓ before

14. **Put the verbs into the correct tense. Use the past perfect or the past perfect continuous.**

1. As a cryptographer John _____ **(work)** for this company for this company for three years before he left.
2. The team _____ **(complete)** the analysis of the digital files before they discovered that steganography had been used to hide illegal data.
3. The researchers _____ **(study)** historical documents for two days, before they uncovered instances where steganography had been employed by spies.
4. The experts _____ **(work)** on breaking the code for months before they finally succeeded.
5. They _____ **(finish)** writing the paper before the course started.
6. Before the digital forensics team _____ **(arrive)**, the hacker _____ **(hide)** already the secret message within the image file.
7. They _____ **(analyse)** the suspect's hard drive for two hours, before they _____ **(uncover)** evidence that steganography had been used to communicate covertly.
8. The software developers _____ **(work)** on a new detection tool for two months before they _____ **(realise)** that their previous methods were no longer effective against advanced steganography techniques.
9. The designer _____ **(embed)** a subtle watermark in the digital artwork before the client _____ **(begin)** presenting it online.
10. They _____ **(review)** the usage of images extensively that day, so they were tired.

15. **John is interested in steganography. He tells a story that happened with him. To complete the story, put the verbs into the correct tense: the past perfect or the past perfect continuous.**

John was interested in the concept of hiding information within another file or message. He **1)** _____ **(study)** steganography and its various techniques for five years, before he **2)** _____ **(start)** working for the private company. John **3)** _____ **(work)** on a very difficult case for several weeks, analysing the digital evidence from a suspected cybercrime organisation. As he got deeper into the investigation, he realised that he **4)** _____ **(miss)** an important piece of information.

John **5)** _____ **(examine)** already numerous images, but needed to find a specific piece of code that would reveal the hidden messages embedded within them. Disappointed, he **6)** _____ **(spend)** long nights at his desk, poring over data. Finally, after hours of intense work, he deciphered the method used to hide the messages. He knew that he **7)** _____ **(made)** significant progress.

Borrowed and modified from: https://deepai.org/

16. **Jane is an artist. She creates digital paintings. In addition, she tells about her experience of using watermarking. To complete the Jane's story, put the verbs into the correct tense: the past simple, the past continuous, the past perfect, or the past perfect continuous.**

Jane, an artist, **1)** _____ **(create)** several digital paintings before she **2)** _____ **(decide)** to start watermarking her work. While she **3)** _____ **(create)** a beautiful digital painting for her latest project, she realised how important it **4)** _____ **(be)** to protect her creative efforts. So Jane **5)** _____ **(decide)** to add a watermark. As she **6)** _____ **(be)** carefully the watermark, she **7)** _____ **(recognise)** that it had to be subtle yet

noticeable. And by the time Jane saved the image and shared it online, she **8)** _____ **(implement)** already her watermarking technique on her previous artwork, ensuring her signature **9)** _____ **(be)** always present on her creations.

Borrowed and modified from: https://deepai.org/

17. **Alex is a specialist in steganography. He deals with hiding sensitive information from unauthorised access. In addition, he tells about his experience of hiding information within images and texts. To complete Alex's story, put the verbs into the correct tense: the past simple, the past continuous, the past perfect, or the past perfect continuous.**

Alex **1)** _____ **(be)** a specialist in steganography for five years, focusing on hiding sensitive information from unauthorised access. When he first **2)** _____ **(join)** the company, he worked on research centred on concealing data in images. He **3)** _____ **(develop)** effective techniques for embedding messages without altering how the images **4)** _____ **(appear)**.

One day, he **5)** _____ **(attend)** an international conference where he was introduced to the exciting world of hiding information within text files. At that moment, Alex **6)** _____ **(realise)** he **7)** _____ **(explore)** yet this possibility, which intrigued him greatly. After he **8)** _____ **(complete)** several training courses and **9)** _____ **(learn)** different methods of text-based steganography, he gained enough knowledge and developed the necessary skills.

As he **10)** _____ **(become)** more involved in this new field, he **11)** _____ **(begin)** to combine his experience with images and his newly learned techniques for text files. He **12)** _____ **(spend)** hours experimenting, having already perfected his image techniques, and

13) _____ (start) to combine the two methods to achieve a higher level of security. While he **14) _____ (develop)** these innovative methods, he was also collaborating with colleagues to help refine his ideas. By the time he **15) _____ (present)** his approach, he **16) _____ (work)** on it for several months, constantly polishing each aspect to ensure its effectiveness. Finally, Alex **17) _____ (create)** a breakthrough approach that not only effectively concealed information, but also added a layer of complexity that **18) _____ (make)** detection almost impossible. His unique contributions **19) _____ (move)** the company forward, and he felt a sense of achievement as his innovations were recognised by the industry.

Borrowed and modified from: https://deepai.org/

FUTURE TENSES

FUTURE SIMPLE

FORM	USAGE	EXAMPLES	TIME EXPRESSIONS
I will work He will work She will work It will work We will work You will work They will work Will I / we / you / he / she / it work? I / we / you / he / she / it won't work	✓ Predictions about the future with verbs think, believe, adverbs probably, certainly ✓ Actions, events that will definitely happen in the future and we cannot control	I **will work** on the IT project later.	✓ tomorrow ✓ tonight ✓ soon ✓ in a week

FUTURE CONTINUOUS

FORMS	USAGE	EXAMPLES	TIME EXPRESSIONS
I will be working He / she / it will be working We / you / they will be working Will I / he / she / it / we / you / they will be working? I / he / she / it / we / you / they won't be working	✓ actions which which will be in progress at a stated future time	This time tomorrow, I **will be working** on the IT project.	✓ This time next week / month / year

18. **Put the verbs into the correct tense: the future simple or the future continuous.**

1. I probably _____ **(change)** my passphrase tomorrow.
2. This time tomorrow, I _____ **(attend)** a seminar on the latest trends in cybersecurity measures.
3. When I come back home, I _____ **(read)** the article about authorisation.
4. Sam _____ **(create)** strategies for passwords defence next week.
5. This time next month I _____ **(study)** at Hackers Academy.
6. I think that I _____ **(finish)** this project soon.
7. This time next week, security professionals _____ **(develop)** innovative strategies to combat emerging threats.
8. I hope that in the coming year, companies _____ **(prioritise)** increasingly information security in order to protect sensitive data.
9. This time tomorrow, seven employees of our company _____ **(receive)** training on how to recognise phishing attacks and maintain data security.
10. I believe that biometrics _____ **(substitute)** passwords.

19. **Jason is an ethical hacker, and together with his friends, he is going to celebrate International Ethical Hacker's Day. Jason will share some ideas about how they want to celebrate this special day. To complete the story, put the verbs into the correct future tense: the future simple or future continuous.**

Jason is an ethical hacker and his friends are ethical hackers too. Soon the 1st of October **1)** _____ **(be)** International Ethical Hacker's Day. In fact, this time next week, Jason and his friends **2)** _____ **(celebrate)** this day with great enthusiasm. His friends hope that they **3)** _____ **(gather)** at the

community center, where a series of workshops and hands-on sessions will be held to help ethical hacking communities collaborate and learn together. This day, Jason **4)** _____ **(organise)** an exciting capture-the-flag competition that will keep participants engaged throughout the day, while his friends **5)** _____ **(set)** up stands to demonstrate the latest in cybersecurity tools and techniques. They **6)** _____ **(enjoy)** delicious snacks from local vendors as they network with fellow hackers, hoping that this day **7)** _____ **(be)** perfect and filled with new ideas and partnerships. Jason believes that the atmosphere **8)** _____ **(be)** one of friendship and camaraderie.

Borrowed and modified from: https://deepai.org/

20. **Work in pairs. Fill in the table below with sentences related to a working day of IT security specialists. Write sentences in the future simple column and the related sentences in the future continuous column. After completing the table, create your story about a day in the life of IT security specialists that will happen this time next week. Use both the future simple and future continuous sentences. Then share the stories with your classmates.**

Future Simple	Future Continuous
1. The team will start the day with a briefing.	**1. The team will be discussing the daily tasks.**
2.	**2.**
3.	**3.**
4.	**4.**
5.	**5.**

FUTURE PERFECT

FORMS	USAGE	EXAMPLES	TIME EXPRESSIONS
I will have worked He / she / it will have worked We / you / they will have worked Will I / we / you / he / she / it / they have worked? I / we / you / he / she / it / they won't have worked	✓ actions that will be finished before a stated future time	Alex **will have finished** his project by five o'clock this afternoon.	✓ by ✓ by the time ✓ before ✓ until ✓ by then

FUTURE PERFECT CONTINUOUS

FORMS	USAGE	EXAMPLES	TIME EXPRESSIONS
I will have been working He / she / it will have been working We / you / they will have been working Will I / we / you / they / he / she / it have been working? I / we / you / he / she / it / they won't have been working	✓ emphasis on the duration of an action up to a certain time in the future	By the time Alex finishes the project, he **will have been working** on it for two months.	✓ for ✓ by

21. **Put the verbs into the correct tense: the future perfect or the future perfect continuous.**

1. By the end of this year, users _____ **(improve)** their password security by adopting multi-factor authentication.
2. By the end of the year, users _____ **(develop)** software for universities for 10 months.
3. By next month, many individuals _____ **(use)** password managers to store their credentials safely for a year.
4. By the end of May, companies _____ **(implement)** stricter password policies to protect sensitive information.
5. By that time, employees _____ **(attend)** training sessions on creating strong passwords for several months.
6. By the end of December, cybersecurity experts _____ **(develop)** advanced algorithms that will improve password protection.
7. He _____ **(finish)** writing the article by Tuesday.
8. By 10 o'clock, they _____ **(realise)** the project for two months.
9. By next year, many organisations _____ **(integrate)** security tokens into their authentication processes to enhance security.
10. By 2025, employees _____ **(rely)** on security tokens for secure access to sensitive systems for several years.

22. Julia and Alex work together in the cyber security department. In their story, they will tell us about their future project. To complete the story, use the future simple, the future continuous, the future perfect, or the future perfect continuous.

This time next week, Julia and Alex **1)** _____ **(work)** late on a project involving the implementation of new biometric security measures. By the time they finish, they **2)** _____ **(test)** several authentication methods, making sure that the system is strong and easy to use. Julia has been researching the latest trends in biometric technology, and by next Friday, she **3)** _____ **(write)** a comprehensive report on how these advancements can improve security. Meanwhile, by the time they present their findings next Friday, Alex **4)** _____ **(develop)** a prototype that integrates both fingerprint recognition and facial scanning for several weeks.

As the days go by, they **5)** _____ **(refine)** their strategies, experimenting with different configurations. By the end of the week, they **6)** _____ **(develop)** a smooth login process that omits traditional passwords, creating a more secure environment for their clients. They both hope that by the time they present their findings to the management team, they **7)** _____ **(demonstrate)** the effectiveness of their new system through testing. By the end of the week, Julia and Alex **8)** _____ **(collaborate)** closely for countless hours, developing their skills and expertise on the project. They believe that they **9)** _____ **(eliminate)** potential vulnerabilities, making their department stronger and more effective in fighting cyber threats.

Borrowed and modified from: https://deepai.org/

Appendix 4. Tapescripts

UNIT 1

1.1. IT Project Management Methods

DEVOPS IN 5 MINUTES

Software development comprises two different departments: the development team that develops the plan, designs, and builds the system from scratch, and the operation team for testing and implementation of whatever is developed.

The operations team gave the development team feedback on any bugs that needed fixing and any rework required. Invariably the development team would be idle awaiting feedback from the operations team. This undoubtedly extended timelines and delayed the entire software development cycle.

There would be instances where the development team moves on to the next project while the operations team continues to provide feedback for the previous code. This meant weeks or even months for the project to be closed and final code to be developed.

Now what if the two departments came together and worked in collaboration with each other. What if the wall of confusion was broken and this is called the DevOps approach. The DevOps symbol resembles an infinity sign suggesting that it is a continuous process of improving efficiency and constant activity.

The DevOps approach makes companies adapt faster to updates and development changes. The teams can now deliver quickly and the deployments are more consistent and smooth. Though there may be communication challenges DevOps manages a streamlined flow between the teams and makes the software development process successful.

The DevOps culture is implemented in several phases with the help of several tools. Let’s have a look at these phases. The first phase is the planning phase where the development team puts down a plan keeping in mind the application objectives that are to be delivered to the customer. Once the plan is made the coding begins.

The development team works on the same code and different versions of the code are stored into a repository with the help of tools like get and merged when required. This process is called version control.

The code is then made executable with tools like Maven and Gradle in the build stage. After the code is successfully built, it is then tested for any bugs or errors. The most popular tool for automation testing is selenium.

Once the code has passed several manual and automated tests, we can say that it is ready for deployment and is sent to the operations team. The operations team now deploys the code to the working environment. The most prominent tools used to automate these phases are ansible, docker and kubernetes. After the deployment the product is continuously monitored.

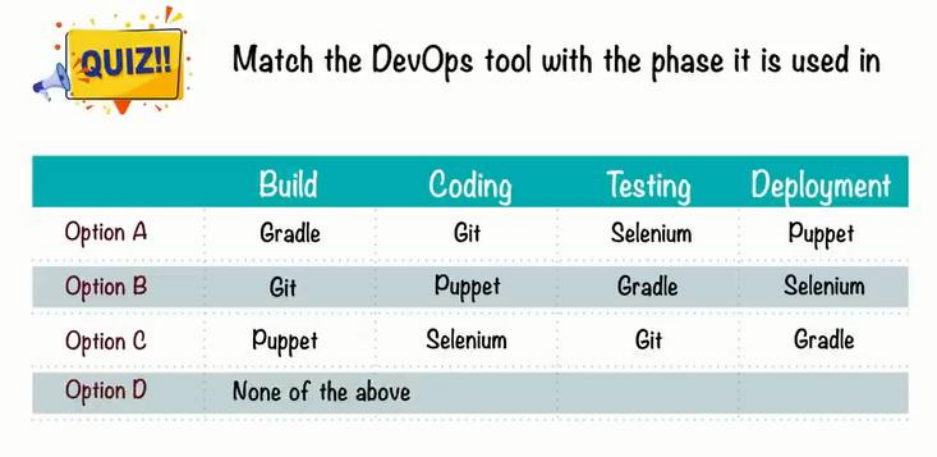
And Nagios is one of the top tools used to automate this phase. The feedback received after this phase is sent back to the planning phase and this is what forms the core of the DevOps life cycle.

That is the integration phase. Jenkins is the tool that sends the code for building and testing. If the code passes the test it is sent for deployment and this is referred to as continuous integration.

There are many tech giants and organisations that have opted for the DevOps approach. For example, Amazon, Netflix, Walmart, Facebook and Adobe. Netflix introduced its online streaming service in 2007. In 2014 it was estimated that a downtime for about an hour would cost Netflix 200 000$. However, now Netflix can cope with such issues they opted for DevOps in the most fantastic way. Netflix developed a tool called the Simian Army that continuously created bugs in the environment without affecting the users.

This chaos motivated the developers to build a system that does not fall apart when any such thing happens. So on this note here is a quiz for you.

Match the DevOps tool with the phase it is used in A, B, C, D.



None of the above.

Today more and more companies lean towards automation with the aim of reducing its delivery time and the gap between its development and operations teams. To attain all of these, there's just one gateway – DevOps.

On the base of https://www.youtube.com/watch?v=Xrgk023l4lI&t=9s

1.2. Types of Websites

POPULAR TYPES OF WEBSITES THAT YOU SHOULD KNOW

Setting up a website is no small feat, but having one is a huge asset for your business or brand. It can boost your sales, help grow your audience and give you that professional look you're going for. That's why when it comes to building your site, there are a lot of decisions to make. But the very first step before you even begin anything else, is to figure out what TYPE of site you want to build to best achieve your goals.

Hey guys, I'm Aaron, and today, we're gonna talk about 16 different types of websites – from blogs and eCommerce to online forums and portfolios – to help you understand which ones make the most sense for you. So stay tuned.

Popular Types of Websites

Before you can start building a website, you need to know what kind of site you want to build.

What are you gonna use it for?

What kind of business – if it's even for a business – do you have?

What kind of offerings will you need on this site?

And what will your audience be looking for?

These are all things you need to think about because different kinds of sites have different elements and features. That's not to say that you can't then combine some different types together, or add capabilities from other types, like having a blog site with a store, or a store with bookings. Basically, you just need to know what the core purpose of your site is. Once you've got that nailed down and you know more of what you'll need, you can really get started.

And you can always check out.

Wix's templates page. I'll throw the link in the description for you, for some great inspo for features that go well together, or to start building quickly. Now, if you already know what kind of site you want to build, just head over to Wix where you can get started. But if you're not quite sure yet, stick around, cuz I'm gonna go over a bunch of popular website types and what you should know about them.

eCommerce Websites

The best eCommerce sites give your customers a seamless shopping experience and make it really easy for them to explore, select, and purchase whatever products catch their eye. And you can either sell your own stuff or dropship products from another online store. The key to success though, comes from creating an amazing eComm site that has visually appealing product pages, captivating descriptions, and

multiple payment options. And with Wix, you can open an online store really easily with everything you need right there, like professionally designed layouts, checkout pages, shopping cart features and flexible payment options.

Business Websites

It's really important for any business to have a strong online presence, even if you're not planning on selling anything in an online store. It can help build your brand, spread your messaging and connect with your target audience. Whether that audience is other businesses or individual customers. Either way though, when you're building a site for your business it's really important to focus on your audience's needs and show them how your company can solve their unique challenges.

Blog Websites

Starting a blog is an awesome way to showcase your interests through written, visual, and digital content. They provide a platform to express yourself and share your passions with the world. And once you get your blog up and running, there are lots of opportunities to make money through things like affiliate marketing, display advertising, and selling ad space. Plus, you can share your blog posts directly on your social media to really expand your reach. And check out the link right up here to see all the blogging capabilities you get with Wix – from really cool templates to being able to choose a customised domain and even tools to help bring in more readers.

Portfolio Websites

If you're looking to showcase your skills and attract potential employers or clients, a portfolio website is definitely the way to go. Whether you're a photographer, artist, writer, or anything else it can act as your resume, putting all your best work on display. A portfolio is also a great way to establish your personal branding, giving visitors insights into your personality, interests, and values. And if you're not quite sure where to start, I'll leave a link in the description to our Wix Website Examples page. There are a bunch of really great sites made by Wix users, and you can filter by Portfolio to get some great inspo.

Event Websites

Whether it's for an in-person soiree or an online gathering, an event website is a powerful tool. And an effective one will have all the essential information people will need to know, like the date, time, and location of the event – even the lineup of speakers or a detailed agenda. Think of it as a one-stop hub for everything they need to know before they go. And by having an engaging site, you can generate buzz and excitement around your event, whether it's a conference, a concert, or just a family BBQ.

Personal Websites

Unlike a portfolio website, which showcases your work, a personal website is a space where you can truly express yourself. It's your chance to share your accomplishments, explore your interests, and develop your personal brand. Depending on your goals – like if you wanna use it to advance your career – you could add a resume, clips, and a bio. If it's more for self-expression, adding a blog or social links might be all you need.

Landing Pages

Landing pages are single page sites designed to market specific products or services. And you've got 2 types of them: non-gated and gated. Non-gated pages are open to anyone, whereas gated pages require users to fill in their details for access, like a name and email address. This type of website is perfect for introducing new offerings, generating leads, or driving targeted traffic to a specific page. And of course Wix has a ton of templates for landing pages. Check out to get ideas or to start building.

Membership Websites

Membership websites are a great option for businesses looking to create dedicated, loyal, returning customers. These sites give you the ability to create a personalised experience and offer exclusive content and valuable resources in a password-protected area. Once they log in, members can access premium services, online classes, and members-only events giving them a sense of belonging to something bigger than themselves.

Booking Websites

Booking websites offer up convenience and efficiency. So whether you're looking for classes, accommodations, or services, these platforms make it easy to sign up online. They also create a space to leave recommendations, reviews, and contact information. And I'd really suggest checking out what Wix offers for bookings pages. There's a ton of features like online scheduling, calendar management and accepting payments that make booking things really intuitive.

Nonprofit Websites

Nonprofit websites are the perfect place to put your organisation's vision and core values front and center – helping you engage with people and rally around your cause. For example, a wildlife protection organisation might be looking to raise awareness, while a food bank might be looking to recruit volunteers or donations.

Online Forums

Online forums are basically a virtual gathering place where a really diverse group of people from different backgrounds or walks of life can come together, connect and interact with each other to talk about certain topics. These forums are usually made up of different discussion threads, which make it easy for users to find the specific subject they want to focus on.

School Websites

When I say ‘school website’ I’m not only talking about elementary schools or universities. It can also be a place for online teaching and information for businesses that teach things like music or languages. And the perfect school website would be designed in a way that creates a comprehensive online database for students, parents, and faculty. It should use educational technology, like offering online lessons and assignments for students and also be a place to attract prospective students who want to enroll.

Informational Websites

Informational websites are a great place for people looking for in-depth knowledge on a specific topic, service, or product. They give valuable insights and answers to their burning questions and provide content that helps them dive deep into the subject matter. Not only that, but they also position you or your organisation as experts in your field.

Community Websites

A community website is an online space where like-minded people can come together, support each other, build strong connections and find valuable resources. By starting a community website, you can create a place that fosters trust, engagement, and a sense of belonging among your members.

Consulting Websites

If you’re an expert in a certain field, you should consider creating a consulting website to share your knowledge and even monetize it. Your site should highlight the specific services you offer, what your background is, and the target audience who could benefit from it. For example, if you’re a financial advisor, you can show how you’ll protect client’s money. If you specialise in human resources, explain how you can help businesses improve their efficiency.

Wedding Websites

Having a dedicated website can turn your special day into an unforgettable experience. And not only can you share important information with your guests like details about the festivities, but you can also add your registry or share videos, photos and stories about your relationship and even your bridal party.

Well, that about wraps it up for us today, but remember these are just 16 examples and there are more. You just need to understand what your goals are for your site, and work from there. And keep in mind, even if you start with one type of site, it's not set in stone and your site can evolve with you. It really all just depends on your needs.

On the base of https://www.youtube.com/watch?v=0tu9PjwiAwk

1.3. Website Design. Security of Websites

HOW TO PERFORM A WEBSITE SECURITY CHECK

Intro. Hey guys, it's Alisha, and today we're gonna show you how to perform a website security check.

It's no small surprise that security has become a significant concern for web developers and site owners. In this video, we can help you determine how secure your site is right now. But before we get too far, I wanna let you know that there will be links to more resources in the video's description, and remember, subscribe, and ring that bell to get notifications for future helpful content.

All right then, let's get started. One quick and easy way to check your site for malware and vulnerabilities, is **to use an online scanner**. **Use an Online Tool.** This remotely scan your site and identify common issues. It's super convenient since it doesn't require any software or plugins, and only takes a few seconds.

There are dozens of scanners to choose from online but for now let's pick a popular one that's easy to use, Sucuri SiteCheck. Once you scan your site, Sucuri will check it against block lists, look for obvious issues like injected spam, or out of date software, and briefly scan any code it can access for malware. It also offers some suggestions to harden your site against attacks. Tools like this are a great launching point for detecting hidden malware and other issues.

While online scanners work well enough, **Scan Your Website With a WordPress** Plugin it's even better to install a plugin that's capable of digging deep into the root of your code and fishing out vulnerabilities or hard to detect malware. Some popular security plugins you might wanna try are, All in One WP Security and Firewall, and the most downloaded on the repository, Wordfence Security.

Once you've installed your plugin of choice, it will likely instruct you to run a scan immediately. The upside of these plugins over remote scanners is that they can

remove malware and make changes automatically. If you suspect or know Look for Strange Changes that your site has been infected by malware, pinpointing the source can sometimes be challenging.

Here are a few unexplained challenges you may notice as well as the files hackers are typically attracted to:

- sudden links to strange websites you didn't add yourself,
- new articles and pages you didn't create, or the content of existing pages suddenly changing,
- changes to settings you didn't make,
- a new user, especially one with high level privileges you didn't add,
- plugins or themes you didn't install,
- malware can often inject a malicious code into your files,
- check plugin and theme files, the wp-content uploads folder,
- and finally WordPress core files located in an incorrect directory, wp-config, PHP, and htaccess.

You should back up your site and have an understanding of the code before making any sensitive changes. If you connect to your site with FTP, you can sort by recently modified files for code that shouldn't be there.

If your site is infected periodically with malware and you can't find any cause in the files, the issue may be with your server or another site on your server.

Make Sure Everything Is Up to Date. As we've already mentioned, out of date software is by far the most common vector of infection in WordPress. If there's only one thing you can do to keep your site safe, it should be to keep **WordPress updated**.

The easiest way to check the status of all software on your site is to go to dashboard updates, which will alert you if your core, theme or plugins are out of date. As WordPress now performs automatic updates since version 5.5, nothing should be outdated unless you have an outdated version of WordPress. If you don't, you can update everything from this screen. If you know, there's a new version of WordPress but it isn't showing up, click the check again button below current version.

You can also check your plugins, install plugins, or appearance themes pages for updates. It's also essential to keep PHP up to date, especially if you're using a version older than 7.3 as it can present significant security vulnerabilities.

A week password on your main account makes it easy Secure Accounts and Passwords for anyone to break into your site with brute forcing programs, giving them administrator access and the ability to change anything. While a complicated password can be arduous to remember making logging in less convenient, it's even more inconvenient to have to your site from a hack.

It's definitely worth using a more secure password even if you have to keep it written down. Your password should use a mix of uppercase and lowercase letters,

numbers, and symbols. It'll be best if you did not base it on dictionary words or personal guessable information, such as your address or family member's name. In the best case scenario, your password would be a long tangled string of random characters.

We strongly recommend you use a password manager. Use a site like 1Password or LastPass to generate a secure unguessable password. You can update your password and email in WordPress by going to users, all users, or straight to users' profile. Scroll down and find email under contact info, and new password under account management.

While you're on the user's page, take a look at all your users and make sure there's no one there who you don't recognise or has inappropriate permissions. You should immediately remove any unidentified user with admin permissions.

We also encourage you look at this guide on restricting user permissions, so only your account will be able to change sensitive files on your site. If your SSL certificate is out of date, you'll usually instantly know. Check Your SSL Certificate Browsers like Google Chrome will block access to your site with a huge warning about the expired certificate. If you're not sure or already getting this error, check your SSL certificate to see if it's up to date and whether you're using the latest version of SSL TLS.

When you visit a website, you'll see a lock icon in the address bar on most browsers. If your certificate is expired, this lock may be red or have a slash through it. Click the lock icon, then click again to see certificate information including its expiration date.

You can also use an SSL certificate checker to scan your site to make sure your certificate isn't expired, and there are no vulnerabilities present in your SSL protocol. Many WordPress sites are filled with tiny vectors Common Vulnerabilities for attacks that may seem innocuous but can provide more information than you wanna share.

Having a visible WordPress version in your front-end tells hackers exactly what vulnerabilities are present on your site, especially if you're using an outdated version of WordPress. You may wanna hide this information. You'll notice file editors under appearance, theme editor and plugins. Plugin editor in your backend. While these tools are very convenient, it also makes it suitable for anyone who hacks your site to break something. So you may wanna turn them off. You can do so by adding this function to wp-config PHP.

SQL injections are a common way of breaking into a site. If you have any forms or other user input, restrict the use of special characters and allow only safe common file types to be uploaded.

Finally, for any extra layer of protection, you can password protect file directories.

On the base of https://www.youtube.com/watch?v=ENvlIBxo9Es

1.4. Web Servers. Security of Web Servers

DEMYSTIFYING WEB SERVER HACKING: TECHNIQUES, VULNERABILITIES, AND COUNTERMEASURES

Let's now talk about hacking web servers, not so much web apps. That's the topic for another module but hacking web servers.

Hacking web servers. Let's talk about our objectives. Here you'll understand some web server concepts and attacks, attack methodology, the tools, the countermeasures, patch management, security tools and pen testing.

Here's what we're going to cover, we'll talk about the concepts and the attacks. We'll talk about the methodology and the attack tools, the attack countermeasures, the patch management, the security tools and the pin testing in this order.

Starting with *understanding web server concepts*. Web servers are interesting beasts because a web server is usually a dedicated machine or dedicated virtual machine that's running a web service. And, of course, there are many web services: Apache, IIS and JINX, a variety of them. This is a service running on an operating system on a box. The service is interacting constantly with loads and loads hundreds of thousands of users either internally or from the general public. And that server service will often have web applications that do specific things. Long gone are the days of just a static web page.

Security issues with web servers.

- So a web server is software or hardware or combination that hosts websites.
- Attackers can attack vulnerabilities and configuration errors in the software.
- And we're talking about network level and operating system level attacks.
- Servers are more vulnerable because they're less secure and easily accessible via the internet. They're meant to face the internet that's their problem.

Web servers have just *sort of a hierarchy*. Here you've got web apps and third-party components. And you have a database. I mean usually web servers keep track of something but they they might have a built-in database. Typically, the database is a whole separate server: Oracle, MySQL, MS SQL who knows. Then, you've got the web server service itself: Apache, Microsoft. And you've got the operating system (Windows, Linux, OS X) and the network. And any security that you might have here: intrusion protection, intrusion detection. There's a whole sort of area and the web server is just one part of one slice of this big old layered cake. But you could possibly attack a web server at any of these layers.

Security Issues with Webservers (cont'd)

- Hierarchy:
  1. Security
  2. Network
  3. O/S
  4. Webserver
  5. Database
  6. Third-party components
  7. Custom web apps

Why web servers are compromised? Now, why is it or how is it that they're compromised.

- Well, we didn't set proper permissions for the files or the directories.
- We left defaults during the server install.
- We have services that the web server frankly doesn't need. Like it doesn't need to be a file and print server.
- There might be conflicts with security due to business ease of use. You know security is always a fight between security and everything else including ease of use.
- We just don't have a good policy. Maybe we don't have good procedures, we don't have good maintenance.
- We have improper authentication for external systems.
- We've left default accounts that have no or default passwords.
- We are keeping unnecessary files lying around that could also lead to compromise. Sample files, defaults or backups are not being stored properly or deleted properly.
- The operating system, the web server and the network are misconfigured.
- There are bugs in any of these.
- The certificates that we have or the encryption settings we have are not configured.
- Properly debugging functions which give away too much information are accessible.
- We're using just self-signed certificates that are not considered, trusted.

Consequences of web server attacks.

So what happens when a web server is attacked?

- We could have a compromise of accounts or compromise of users' data.
- We could have the website get defaced.

- The website could be used as a jump point to launch secondary attacks.
- It could give root or administrator access to other apps / servers.
- We have the potential for a theft of data or tampering with the data.

Open-source web server architecture.

Here's sort of the architecture of a classic what we call lamp stack.

When you install sort of an open source web server, it can come with a database server, some email capabilities, some applications, a web server. So this is sort of like a classic thing here.

You can see that the web server itself is this Apache service. Let me just zoom in a bit. So you can see it better. The web server itself is Apache and so that we can run web apps.

We probably have PHP which allows us to run different applications and we might have other things. Apache also talks to or uses email. The web apps are probably going to talk to some kind of database. You've got all these moving parts, not just the web server itself. Then you've got the file system of the operating system that is maintaining like html, javascript, PHP pages, text pages, pdfs, spreadsheets, images like pngs, jpegs and gifs, sound and video images swifts and mp3s, mp4s.

Then you've got all these people on the internet from normal users out in the internet to the administrator of this website to hackers like us. But these are the folks with malicious intent all making their connections through the internet to try to use or attack these services.

IIS web server architecture.

Here's IIS now. This is microsoft's version of a web server.

They have application pools and something called Svchost.exe, and external apps.

Here you've got the web server with its core components. It's got little modules that do things like authentication, certificate mapping, providing default documents, caching http, providing errors and logging. With microsoft anytime some process needs to get on a network. It usually is helped by a process called Svchost.exe. Look at task manager on a microsoft machine. If this machine is doing a bunch of different things on a network, you might see a lot of Svchost.exes here that are assisting the service. In this case, it's assisting the www service, the world wide web service.

Then you'll have other applications, configurations, applications. And what microsoft does is they run applications in what's called an app pool where a bunch of apps share resources. They mostly share policy, authentication of credentials and particularly things like memory. Then you can have your application: different things like forms or other kinds of things. Then clients / hackers / administrators are connecting through across the internet, talking to microsoft's http protocol stack, which is a driver HTTP.SYS, to talk to these components.

So that is starting basic web server concepts.

On the base of https://www.youtube.com/watch?v=5pTHvFABSzc

UNIT 2

2.1. Classical Cryptography. Ciphers and Codes

SECRET CODES: A HISTORY OF CRYPTOGRAPHY (PART 1)

Intro. The written word is the most important invention in human history but as long as humans have had the ability to share information. They've also had the need to conceal that information as well. This need led to the invention of cryptography.

Part 1: The Ancient World. The word cryptography comes from the Greek meaning hidden writing. And some of the earliest forms of secret writing come from ancient Greece as well. Herodotus, the father of history, as he is known, described a way of hiding writing by putting a message on a wooden board and then covering it with a layer of wax. During Greece's war with Persia in the 5th century BC this approach was used to send military correspondents.

This sort of concealment is known as steganography meaning covered writing. It was common all over the ancient world, from Greece to China. But as you can probably guess this approach has some issues. The main one being that if the message is discovered its contents will be easily revealed. This dilemma gave rise to cryptography which doesn't hide the existence of a message but instead hides its meaning.

Cryptography can be broken down into two subtypes: transposition and substitution. Transposition is when a document is rearranged creating an anagram and it is the earlier form of cryptography. An early historical example is once again from ancient Greece, specifically the city-state of Sparta.

The Spartans used a device called a skytale to hide their military communications. It consisted of a strip of leather wrapped around a wooden rod. The sender would write his message on the leather as it was twirled around the rod like so. When unfurled, the message would seem like a jumble of letters. But once the receiver wrapped the strip around an identical rod of their own, the message would become clear.

Transposition has some major flaws though. For one a short message has a limited number of scramblings. For instance, the word "dog" can only be rearranged five ways. And larger messages while more difficult to disentangle for an interceptor will also be too difficult for the intended receiver as well. Because of this, cryptography by way of substitution was created.

Substitution rather than rearranging the letters in a message instead replaces the letters altogether. The most famous substitution cipher is the Caesar cipher. As the name implies, it was used by the Roman dictator Julius Caesar during the Golic Wars in the 1st century AD.

The Caesar cipher also known as the Caesar shift cipher. It replaces any given letter with the letter three spaces down the alphabet. This is why it's called a shift cipher. Because the cipher alphabet is simply the plain alphabet shifted three spaces like so.

Traditionally Caesar favored a shift of three but as you can see you can shift the alphabet as many times as you want. Accordingly, there are 25 variations of the Caesar cipher. This is pretty good, but if someone knew, you were using the Caesar cipher to encrypt your message, they could brute force their way through by checking all 25 shifts. But if you scramble the alphabet at random, instead of simply shifting it over you get 400 septillion. That's 400 followed by 24 zeros different permutations. So obviously a wannabe code breaker would have no chance brute forcing his way through such an encryption. However, a totally random arrangement of the alphabet would also be difficult for the receiver of a message to remember.

One solution to this problem is a keyword cipher. Essentially, the sender and receiver of a secret message would agree on a keyword and that would be used to construct the cipher alphabet.

Let's say our keyword is *shift,* easy enough to remember, right. So the cipher alphabet would be made by spelling *shift* then filling in the alphabet according to the last letter of the word. In this case *t l*ike this. Throughout the rest of the Roman Empire's history and into the 6th century A.D. these simple ciphers broadly called mono-alphabetic substitution ciphers, were used to great success. That is until the 8th century when a group of ingenious scholars found a way to break through these puzzles.

Part 2: The Islamic Codebreakers. In the middle east about a hundred years after the death of the prophet Muhammad a new dynasty took power called the Abbasid Caliphate. This new leadership heralded what is called the Islamic Golden Age. This time of prosperity and peace was the perfect cradle for an intellectual age. Islamic scholars centered in the Baghdad house of wisdom collected works on astronomy, medicine, alchemy, music, mathematics, and more. They also added their own knowledge to the collections.

During this time muslim theologians were studying the Quran and the Hadiths. They wanted to know which revelations came earlier in the Quran and which Hadiths were genuine and which were not. They did this by using new statistical and linguistic techniques. Chief among them was called frequency analysis. Scholars saw how often words were used in the Quran and the Hadiths and this investigation would show whether the linguistic styles and etymological idiosyncrasies of the documents were in line with muhammad's. They also used this analysis on individual letters, not just words and in doing so discovered that certain letters were more frequently seen than others.

The first scholar to realise this frequency analysis could be used to break ciphers was a man named Abu Yusuf Ya'qub ibn Ishaq Al-Kindi. We'll just call him Al-Kindi. He was a very important philosopher who wrote hundreds of works on all sorts of

subjects from mathematics to music, to medicine. He also wrote a treatise on cryptanalysis the study of code breaking.

Here's a quote from his book which concisely explains his ingenious technique.

"To solve an encrypted message … find a different plain text of the same language long enough to fill one sheet or so, and then count the occurrences of each letter. Call the most frequently occurring letter the first, the next most occurring the second … and so on. Then look at the ciphertext and also classify its symbols. Find the most occurring symbol and change it to the first letter … the next most common symbol is changed to the form of the second letter … and so on, until we account for all the symbols of the cryptogram we want to solve." *Al-Kindi*

Essentially find the most occurring letter in a cipher and assume it is the most occurring letter in the normal alphabet. In English the most common letter is *e* followed by *t* and so on. The least common are *q* and z. Here's a handy chart. As you might be able to guess, this method can't be used unconditionally. Say you're deciphering a secret treatise on zebras, xylophones, and quails.

You wouldn't expect to see these letters z, x, and q very frequently and that would probably throw a wrench in your analysis. Still an intelligent cryptanalyst can break pretty much any monoalphabetic substitution cipher using frequency analysis even when letters don't line up perfectly with their statistical likelihood.

Part 3: The Renaissance. Heading back west, Europe have been going through the Dark Ages. While "the Dark Ages" is generally a term I dislike when it comes to cryptography it is fitting. As Medieval Europe had little interest in the subject. That was until the Renaissance. With the outpouring of interest and study in the arts and sciences during this time, the study of cryptography was reinvigorated too.

The political situation in Europe was also responsible for the renewed interest in keeping communication secret. This was especially true in Italy, which at the time was not a unified country but a mishmash of small kingdoms and city-states, all constantly bickering with each other. So because of this political intrigue, mixed with the leaps forward in scholarship, cryptography became a burgeoning industry. By the 15th century, almost every court in Europe had a cipher office and every ambassador – a cipher secretary. But with the islamic code breaking techniques having been brought to the west, the cryptographers were still at a disadvantage. They needed new innovations to trip up the cryptanalysts.

The first was the introduction of nulls. Nulls are symbols put into a cipher that have no meaning. Let's say, you had a cipher made from numbers1 to 50. A quick side note you may think that a cipher made from symbols or numbers instead of letters would be more difficult to solve. But they're not.

Frequency analysis works just fine regardless of what images are used. Ciphers using things other than letters existed for centuries before this. I just hadn't mentioned them. So a cipher made from 1 to 50. Seeing as there are only 26 letters in the English alphabet, only about half of these numbers would actually correspond to letters. The rest would be nulls.

The second innovation was to simply misspell the encrypted message. So that when a cryptanalyst tried to break the cipher, he would slowly uncover misspelled words and then stop thinking he's going about it all wrong.

And lastly the introduction of codes. In cryptography codes and ciphers are two different things. Codes are words that mean other words like a code name. Codes replace words, while ciphers replace letters. Codes are obviously most useful when applied to a short message but not so good with long messages.

Because of this limitation, cryptographers started using nomenclatures. Nomenclatures are a mix between ciphers and codes. Essentially, a message would be encrypted using a cipher while also using a small list of important code words. As impressive as all these new techniques were, a cunning and intelligent code breaker could figure out the nulls, ignore them as spellings, and understand the code words through context.

For decades, cryptanalysts still had the upper hand as shown in the case of Mary Queen of Scots. While imprisoned on trumped-up charges, Queen Mary took part in the Babington Plot, a plan by English catholics, to kill Queen Elizabeth and replace her with Mary. She had corresponded with the conspirators using a cipher which was unfortunately broken by English cryptanalysts. Proving Queen Mary guilty, she was executed on February 8, 1587. So clearly cryptographers needed a better system.

And in the 16th century a frenchman named Vigineri would come up with it.

On the base of https://www.youtube.com/watch?v=9pp9YpginNg

2.2. Cryptanalysis

WHAT IS CRYPTANALYSIS?

Cryptanalysis is the process of analysing and decryption of encrypted messages without knowing the key or the algorithm used to encrypt the message. The goal of cryptanalysis is to find weaknesses in cryptographic systems that can be exploited to reveal the underlying information.

Let's understand it with an example. Suppose you receive an encrypted message that looks like this. You know that the message is encrypted using a Caesar Cipher which is a type of substitution. Cipher where each letter in the plain text is shifted a fixed number of positions down the alphabet.

For example, a Caesar Cipher with a shift of three would encode the letter "A" as "D", "B" as "E", "C" as "F", and so on. To crack the cipher and reveal the plain text message, you could use cryptanalysis techniques such as frequency analysis. This involves analysing the frequency distribution of letters in the cipher text to identify patterns that can be used to infer the key.

In this example you might notice that the letter "L" appears most frequently. In the ciphertext, this suggests that it might correspond to the letter "E" in the plain text. Since "E" is the most common letter in the English language, by applying this reasoning to the other letters in the cipher text, you can gradually deduce the key and reveal the plain text message. Therefore, the plain text message is ethical hacking.

On the base of https://www.youtube.com/watch?v=PAylKVVSW-0

THE SCIENCE OF CODES: AN INTRO TO CRYPTOGRAPHY

This probably looks like gibberish to you, and it should because it's a cryptogram, a message in code. But, if I told you that all I did was shift every letter in the sentence to the next one in the alphabet, then you'd know that it translates to this.

To encrypt a message, you need two main parts – the cypher and the key. The cipher is the set of rules that are using to encode the information. For example, shifting the alphabet by certain number of letters. The key tells you how to arrange those rules otherwise they'd be the same every time and it would be easy to decode the message in this case. The key would be one because we shifted the alphabet by one letter.

To decrypt the information, you need to know what kind of cipher was used and also have the key or you can just crack the code either by trying all possible combinations you can think of or by analysing the code and working backward from it, known as deciphering. But is it possible to come up with a combination of a cipher and key that could never be determined?

Is there such a thing as an unbreakable code? Well, people keep coming up with new and better ciphers, but it's hard to make them unbreakable. Because, no matter what, you're using a set of rules to encrypt the information and with enough time and enough data someone can usually uncover those rules. That puzzle, I just gave you, is one of the oldest and simplest ways to encrypt a message. It's usually called a Caesar cipher and in this case the key was just a number representing how many letters of the alphabet I shifted it, but it's also very easy to crack. Even if you didn't know the key, it would take you at most 25 tries to decode the message because you know the whole alphabet has to be shifted by a certain amount. Since there are 26 letters in the alphabet, there are only 25 other options.

A Caesar cipher is one simple type of monoalphabetic ciphers, a class of ciphers for the whole code is based on one letter of the alphabet standing in for another letter consistently throughout the whole message basically just scramble the alphabet in that case the key would just be a list of which letters correspond to which like this one.

There are over 400 septillion possible ways to encrypt this kind of message so you'd think it would be hard to crack and it is but only a little bit because there are lots of ways to decode messages just trying all of the possible keys to a code is probably the most obvious and least subtle and it has an equally unsubtle name – brute force.

But you can try a more sophisticated technique something called frequency analysis, which is based on the idea that every language has its own specific patterns. In English, for example, the letter "E" shows up a lot I used it seven times in just the last sentence. And some words like "the", are so common that it's hard to even use a sentence without them. Cryptographers call these words cribs. So frequency analysis looks for common words and also common letters or sets of letters like "ed" or "ing" at the end of words.

If you find that the letter "X" is showing up a lot in a message and so is the three letter word "I", "R", "X" you might guess that in the key "X" corresponds to the letter "E" and "I", "R", "X" spells "THE" and once you've figured out those letters you can figure out the rest by recognising other words and using the process of elimination. And since longer cryptograms contain more clues they're easier to crack. So monoalphabetic ciphers are fun but they're not hard to break.

If you want to get a little fancier with your encryption you can use polyalphabetic ciphers instead they're much more effective. In a polyalphabetic cipher the way you scramble the alphabet actually changes throughout the message. In the first word s might translate to "W" but in the last word s might translate to "H". It all depends on the particular encryption method you're using and on your key.

One of the earliest polyalphabetic ciphers was the VIGENERE cipher developed in the 16th century was pretty simple because the key was just a word.

So let's say you want to encrypt "SciShow is the greatest" using a VIGENERE cipher well the first thing you need to do is write out a VIGENERE square.

The alphabet goes across the top and along the left side and each row contains the letters "A" to "Z" shifted over by one. So the first line starts with "A" and ends with "Z" but the second starts with "B" goes all through the letters until "Z" and then ends with "A" and so on. You end up with 26 differently scrambled alphabets and now you're ready to encode the message. You just have to pick a key.

Let's just say your key is Michael, you write out your key multiple times until it fills the same number of letters as your message so "SciShow is the greatest" would correspond to this. Then to encrypt it, you take each letter of the message and move along its row in the VIGENERE square until you get to the column of the corresponding letter in Michael. So "scishow is the greatest" turns into this. That's much tougher to decode unless you have the key because those letter frequencies are all different now. Since the keyword Michael is seven letters long each letter of your message is encrypted using seven different scrambled alphabets.

But if your text is long enough it's still crackable using a type of frequency analysis developed in the19th century by cryptographer Charles Babbage Babbage. He realised that in a long enough message some patterns and the coded message will still show up like if your key only has seven letters. That means that there are only seven ways to encrypt the word the but if your message uses the word the eight times there are definitely going to be repeat. So he just counted how many letters separated those repeated patterns. If they were separated by 7, 14 or 21 letters, he knew that the key was probably seven letters long and from there he would just use frequency analysis to figure out the seven scrambled alphabet.

Babbages method is just one example of why it's so hard to create an unbreakable cipher. Your key creates a pattern within the encrypted message. And with enough work a spy can uncover that pattern. It turns out that the only way to have a really unbreakable cipher is to use what's known as a one-time pad encryption, which uses a key that is as long as the message itself. That way there aren't any patterns in the encrypted text. There's nothing to analyse, so there's no way to work backwards.

The sender and the recipient both have the same pad and each sheet contains a long set of random letters which is used as the key once she is used to decode a message you destroy it. Then you use the next sheet for the next message so you never repeat a key. As long as you keep the pad safe the message can't be decrypted by anyone else. But you can't always use one-time pad encryption.

Let's say you needed to get a message to someone halfway across the world whom you'd never met, you wouldn't have a chance to give them a matching pad. In warfare that sort of situation comes up a lot which is why in the early 20th century there was suddenly plenty of incentive to come up with better ciphers. Remote

communication using technology like the telegraph was incredibly valuable during wartime but it was essential that only your allies understood what you were saying.

The Germans experimented with a new more complicated mono-alphabetic cipher during World War I but eventually the French managed to crack it. Then during World War II the Germans again came up with the new cipher. And this time its security seemed perfect, maybe you've heard of it The Enigma machine.

The machine used a poly-alphabetic cipher that scrambled the alphabet in a different way each time you typed a new letter. As far as the Germans knew the only way to decipher the message, was to have your own Enigma machine and set it up using a secret key that changed every day. The machine was meant to work like a one-time pad in the sense that the alphabet was re-scrambled for every letter of the message.

But instead of having to distribute a set of sheets to everyone you could just use a key that told the users how to set up their Enigma machines. And you could change that key is often as you wanted, but it had a few flaws. For example, no letter could be encoded as itself. That might not sound like a big deal but it ended up being a fatal weakness.

British mathematician Alan Turing along with the rest of his team designed a machine of their own that could crack the Enigma code as long as they knew around 20 of the characters contained in the message – which they often did because some phrases tended to show up a lot in Nazi communicates, especially nice things about Hitler So part of the strategy of Turnings team was to look for cribs – those common words and phrases – and see where they might fit.

For instance, if they knew a message contained the word Führer, they could look for places in the text that didn't have the letter "F", since they knew that the "F" in Führer couldn't be encoded as itself. Those Clues helped them figure out how the Enigma rotors were set up to encrypt the message.

Cracking the Enigma code was a huge advantage for the Allies. Many historians attribute some of the most important victories during the war to information the Allies got from the Enigma encrypted messages.

These days, encryption is mostly important in digital computing, and that isn't perfect either. When websites announced that hackers now know everything about you that's because their encryption methods were breakable. Companies that store your data have to take into account a whole new set of considerations. Like how when you can complete billions of operations per second brute force suddenly becomes a lot more practical. So the same principles that Vigenere and Turing used are the same ones that allow you to pay your bills online and keep North Korea out of your email, most of the time.

On the base of https://www.youtube.com/watch?v=-yFZGF8FHSg

2.3. Steganography

HOW TO HIDE DATA INSIDE IMAGES (STEGANOGRAPHY)

Steganography is a way to hide secret information inside ordinary-looking files, like pictures or music. It's a bit like hiding a message in plain sight where no one expects to find it. You can hide things like passwords, codes, or IP addresses in these files. This makes it harder for people to find and access the hidden information.

Steganography isn't the same as cryptography, which is about scrambling information to make it unreadable. But sometimes, people use both methods together for extra security.

There are different ways to use steganography. Here, we'll talk about five types:

Text Steganography. This type hides a message inside a piece of text. One way to do this is by swapping letters around. For example: See? The hidden message becomes clear after swapping the letters back. It's a simple example, but steganography can be much more complex and creative!

Image steganography is one of the coolest types! It's about hiding secret messages or data inside digital images.

There are different methods to do this, like:

- *Least Significant Bit (LSB) Technique*: This method hides data in the least significant bit of each pixel in an image.
- *Masking and Filtering*: Here, you manipulate the image's colour values to hide the data.
- *Coding and Cosine Transformation*: This technique uses mathematical transformations to embed the data in the image. Check out these two images: Can you spot any difference between them? Probably not, right? But look at the file sizes: The image on the right is bigger because it's hiding a 260-word text inside it! Pretty neat, huh?

Audio steganography is all about hiding secret messages in audio files. One popular method is called Backmasking. This is where a hidden message is embedded in the audio and can only be heard when the audio is played backward. For instance, the rapper Eminem used backmasking in his song "Stimulate" released in 2002.

Network steganography is less common but intriguing. It involves hiding messages in network traffic. These hidden messages can be found in the data packets' payload or headers when examined by the receiver.

Now, let's dive into image steganography with an example using Steghide. Steghide is a free tool for image steganography that uses the least significant bit (LSB) technique.

Here's how it works: images are made of pixels, which are made of bits. The bit depth tells us how many colours are in an image. A higher bit depth means more colours. LSB changes the last bit of each byte (or pixel) in the image to hide data. This

alters the image slightly, but it's usually not noticeable. The higher the bit depth and resolution, the more data you can hide.

Ready for a little demonstration? Here's what you'll need:

1) A Linux Operating System.
2) An Internet Connection.
3) An Image.
4) and A Text File.

To start, you'll need to install Steghide. Open your terminal and type in the following command: sudo apt install steghide. After installation, you can type "steghide – help" to see a list of commands and options available.

Now, gather an image and a text file in one directory. For this example, let's use "information.txt" and image.jpg. Make sure you have some text in the text file that you want to hide in the image. Navigate to your directory using the terminal.

Now, run the following command to embed the text file into the image: Here's what each part means: steghide is the tool we're using. "embed": Tells Steghide to embed data. – EF Specifies the file you want to hide. – CF Specifies the image file you want to use as a cover. – SF: Creates a new image with the embedded data. And – V: Gives detailed information about the process.

You'll be prompted to enter a password for added security. If you don't want to set a password, just press Enter twice. Here's an example of what it might look like: And there you have it! You've successfully hidden text inside an image using Steghide. Cool, right?

Let's examine the new image we created. At first glance, they look identical, right? To be sure, you can use a tool like diffchecker.com to compare them in detail. Since the stego image has hidden data, it's slightly larger than the original. You can extract this data using the following command: Here's what each part means: - SF is the stego image containing the hidden data. and – XF is the file where the extracted data will be saved. After running this command, you should see something like this: If you see the extracted text, well done! You've successfully hidden and retrieved text from an image.

You can even hide entire books using this method. For instance, I hid a text file of Quincy Larson's book, "How to Learn to Code & Get a Developer Job", behind an image of the book using another tool called Stegcore. Here's how the original and stego images compare: And, as expected, the stego image is a bit larger than the original.

Steganography can be used both for good and bad. It's great for protecting secrets, but bad guys might use it to hide bad stuff. Always be responsible with what you learn and use it for good reasons. Stay safe online.

On the base of https://www.youtube.com/watch?v=u1oTteKYWEk

2.4. Digital Watermarking

DIGITAL WATERMARKING

What are digital watermarks?

Digital watermarks are a code added to a digital audio, video, image, or document file. In this video we will look at the three-step process that is involved with digital watermarking. We'll also look at some terminology: visible versus invisible, fragile versus robust, preventive versus detective controls and then we'll look at some examples about how digital watermarking is used.

Digital Watermarking: Three Step Process. There's a three-step process with digital watermarking is used. The first step is the embed process and this is where a file is embedded with some digital water marking code. The second part of the process is modify / copy / replace process and this is where the file is sent over the Internet posted on YouTube. It could be photocopied, anything could be done to the file. The third step in the process is the extraction process and this is where special software is used to scan the file and the digital watermark code is identified.

Let's take a look at some terminology *visible vs invisible. Visible digital watermarking* is viewable by human eye or detectable by ear. And the picture on the right is an example of a file that has a very visible digital watermark. Another example would be a black line running through a video file.

Invisible or imperceptible digital watermarking is only detectable with special software. And again the file on the right could have some digital water marking code in it that you cannot see with your eye. Another example would be a high frequency noise that you can't hear that would be added to an audio file.

Fragile versus robust. Fragile digital watermarking is corrupted if any part or even a small portion of a file is modified. And this is used for tampered detection and data security. *Robust digital watermarking* is protected and can be extracted if any part or all of a file is modified. And this is used for copyright protection and ownership protection.

Detective Control vs Preventive Control. Preventive controls by definition are processes designed to deter errors or irregularities from occurring. Digital water marking cannot do this. No file is 100% protected and tampering cannot be 100% prevented. Someone will eventually find a way to copy or tamper with a file. Another kind of control is a *detective control*. This by definition means a process designed to identify if errors or irregularities have occurred. This is something that digital watermarking can do.

So let's take a look at three applications of digital watermarking.

How is Digital Watermarking Used?

The first one is copyright protection and verifying authenticity and integrity of files to show ownership. The second application is data security of official documents and the third application is forgery and tampering detection.

Copyright protection now. The goal here is to detect unauthorised distribution of images, audio, video, and other documents. Owners can copyright their work by inserting digital watermarks within a file. If another person claims ownership to the file then the digital extraction process can identify the true owner.

It is claimed that owners could also control distribution of their file by inserting code that prevents copying. But this is not 100% effective. There's always someone who can figure out some new technology or some new way to bypass the code. So I'm going to cross out this particular bullet point here.

Data Security. The second way that digital water marking is used is for data security. And the goal here is to certify and authenticate a file. On the left is an example of a protected ID card. The ID number 200002144307 is written in plain text on the card. It's also barcoded and it's also hidden as a digital watermark in the photo.

This means that the key information is written three times on this ID card. If anyone tries to tamper with a card or replace the photo, it would be possible to detect the changes. Special scanning software could verify the proper links with the digital watermark hidden in the photo against the barcode and against the plain text on the card.

The third use of digital water marking is *Forgery and Tampering Detection*. And the goal here is to detect any modifications made to a file. Image A below shows an original photo of a car that has been protected with digital water marking technology.

Photo B shows the same photo with two numbers modified on the license plate. This looks like a pretty good forgery, doesn't it.

Photo C was produced after running the tampered photo through a digital watermark detection program. The tampered areas are identified in white.

Interesting Application of Digital Watermarking. Not all uses of digital watermarking is for protection and security. I thought I would would end this video on a more interesting application of digital watermarking. Bag makers Inc is a cloud-based company that sells bags with imprinted logos and photographs. They have developed a technology where they can apply a digital watermark code to a full colour photograph. The code is invisible unlike a QR code and when the photo is scanned by a cell phone or another mobile device, the digital watermark code opens a website a video or a signup sheet for membership on the mobile device. This is a great application of digital watermarking for trade shows open houses and advertising.

On the base of https://www.youtube.com/watch?v=763ELerm_rA

UNIT 3

3.1. Identification. Verification. Authentication. Authorisation. Accounting

AAA – AUTHENTICATION, AUTHORISATION, AND ACCOUNTING

Have you ever wondered how your data is protected online? In this ever evolving digital age, understanding the mechanism of safeguarding our online data is more crucial than ever.

We're surrounded by an invisible fortress, a complex architecture of security measures designed to protect our online presence. This fortress is not built of stone or steel, but of protocols and algorithms, and it's composed of three main components: Authentication, Authorisation, and Accounting.

Authentication verifies our identity, ensuring we are who we claim to be. Authorisation determines what we're allowed to do, controlling our access rights. Accounting, meanwhile, keeps track of what we do, logging our activities for further analysis. These three elements, together, form the backbone of online data protection, creating a safe environment for us to explore, interact, and innovate. So, ready to unravel the mystery? "Stay tuned as we delve deeper into these fascinating elements of cybersecurity."

Firstly, let's unlock the world of Authentication. This is the process that verifies if someone or something is, indeed, who or what it claims to be. In the digital realm, it's like a virtual handshake between a user and a system, confirming the user's identity before granting access to information or resources.

Now, how does this magic happen? Through three key factors. Think of these as the three musketeers of cybersecurity. First up, "something you know." This is the most common factor and includes passwords, PINs, or answers to secret questions. Remember when you set up your email and chose a password? That's a classic example of this factor.

Next, we have "something you have." This could be a physical or virtual object like a smart card, a security token, or even a text message with a code sent to your smartphone. Ever received a verification code on your phone to log into a social media account? That's this factor in action.

Lastly, there's "something you are." This is the most personal and hardest to fake. It includes biometrics like fingerprints, iris scans, and voice recognition. Modern smartphones using fingerprint or facial recognition to unlock? You guessed it, that's this factor at work.

These factors can work alone or in combination. When two or more of these factors are used together, it's called multi-factor authentication, upping the security game.

So, why is this important? Well, the digital world is like a bustling city, and your data is a treasure chest. Authentication is like the lock on that chest. Without a proper lock, anyone could walk up and take a peek inside. But with authentication, only you hold the key.

Remember, the strength of the lock depends on the strength of your authentication factors. A complex password, a unique security token, or a distinct biometric feature – these are your best friends in the vast digital landscape. Thus, authentication is our first line of defence in protecting our online data. The stronger it is, the safer your treasure chest remains. So let's keep our keys safe, our locks strong and our data secure onward to a safer Digital World.

Now, imagine having the keys but needing permission to enter. That's where authorisation comes in. Authorisation is a crucial component in the world of cybersecurity. It's the process that comes into play after your identity has been authenticated. It's like the bouncer at the club who checks your ID, then decides whether you're allowed in or not, based on other factors like age or dress code. In the digital world, authorisation is about determining what you, as a verified user, are allowed to do, what resources you can access, and what operations you can perform. It's the gatekeeper that ensures you only have the access you need and nothing more.

So, how does this gatekeeping work? Well, there are three main types of authorisation: discretionary Access Control (DAC), mandatory access control (MAC), and role-based access control (RBAC). Each plays a unique role in controlling access to data.

Firstly, we have discretionary access control or DAC. This method allows the owner of the information or resource to personally decide who gets access. It's like lending a friend a book from your personal library. You as the owner have the discretion to decide who gets to read your book.

Next there's mandatory access control or MAC. This is a more rigid and policy-driven approach. Access permissions are assigned by a central authority based on multiple factors such as the user's clearance level and the data's classification. Imagine a highsec government building, where access to certain floors is strictly controlled. That's MAC in action.

Finally, we have role-based access control or RBAC. In this model access rights are based on the roles users have within the system. For instance, in a company a manager may have different access rights compared to a regular employee. It's all about the role you play. Authorisation, therefore, acts as a gatekeeper deciding who gets access to what data. It's about ensuring that the right people have the right access keeping our Digital World secure.

Finally, once you're in, someone needs to keep track. Enter Accounting. In the realm of cybersecurity, accounting is the unsung hero that diligently keeps tabs on everything

that transpires once access is granted. It's like the digital equivalent of a meticulous bookkeeper, taking note of every detail and ensuring nothing slips through the cracks.

Accounting measures the resources that a user consumes during access. Think of it as a digital footprint of your activity. It records the amount of system time you've used and the data you've sent and received during a session. It's like a stopwatch and a weighing scale rolled into one carefully monitoring time and data.

But what is the purpose of all this tracking, you might ask? Well, the uses of accounting are manifold. It plays a key role in authorisation control, ensuring that users only access what they're meant to and do not overstep their boundaries.

It is used for billing purposes, calculating charges based on resource consumption. It aids in trend analysis, offering insights into user behavior and system usage patterns.

Furthermore, it assists in resource utilisation, helping to identify inefficiencies and optimise resource allocation. And, it's instrumental in capacity planning activities, ensuring that the system is equipped to handle current and future demands. Accounting, then, is our final component, maintaining a record of user activities and resource usage.

It's the silent Sentinel always watching and always recording keeping the digital world secure and orderly. As we've seen authentication, authorisation, and accounting – the AAA – form a powerful Trio in protecting our online data.

Authentication verifies our identity through something we know, have, or are. Authorisation controls access using methods like discretionary, mandatory, or role-based access control. Accounting tracks, our usage providing valuable data for Trend analysis, resource planning and more, together these three pillars of cyber security, work in unison to keep our Digital World secure. In our Digital World understanding the AAA is crucial to navigate and protect our online presence effectively.

On the base of https://www.youtube.com/watch?v=MVYswO4QI8c&t=26s

3.2. Passwords

WHAT'S WRONG WITH YOUR PA$$W0RD?

Lorrie Faith Cranor

I am a computer science and engineering professor here at Carnegie Mellon, and my research focuses on usable privacy and security, and so my friends like to give me examples of their frustrations with computing systems, especially frustrations related to unusable privacy and security.

Passwords are something that I hear a lot about. A lot of people are frustrated with passwords, and its bad enough when you have to have one really good password that you can remember but nobody else is going to be able to guess. But what do you do when you have accounts on a hundred different systems and you're supposed to have a unique password for each of these systems? It's tough.

At Carnegie Mellon, they used to make it actually pretty easy for us to remember our passwords. The password requirement up through 2009 was just that you had to have a password with at least one character. Pretty easy. But then they changed things, and at the end of 2009, they announced that we were going to have a new policy, and this new policy required passwords that were at least eight characters long, with an uppercase letter, lowercase letter, a digit, a symbol, you couldn't use the same character more than three times, and it wasn't allowed to be in a dictionary.

Now, when they implemented this new policy, a lot of people, my colleagues and friends, came up to me and they said, "Wow, now that's really unusable. Why are they doing this to us, and why didn't you stop them?"

And I said, "Well, you know what? They didn't ask me."

But I got curious, and I decided to go talk to the people in charge of our computer systems and find out what led them to introduce this new policy, and they said that the university had joined a consortium of universities, and one of the requirements of membership was that we had to have stronger passwords that complied with some new requirements, and these requirements were that our passwords had to have a lot of entropy. Now entropy is a complicated term, but basically it measures the strength of passwords. But the thing is, there isn't actually a standard measure of entropy. Now, the National Institute of Standards and Technology has a set of guidelines which have some rules of thumb for measuring entropy, but they don't have anything too specific, and the reason they only have rules of thumb is it turns out they don't actually have any good data on passwords. In fact, their report states, "Unfortunately, we do not have much data on the passwords users choose under particular rules. NIST would like to obtain more data on the passwords users actually choose, but system administrators are understandably reluctant to reveal password data to others."

This is a problem, but our research group looked at it as an opportunity. We said, "Well, there's a need for good password data. Maybe we can collect some good password data and actually advance the state of the art here."

The first thing we did is, we got a bag of candy bars and we walked around campus and talked to students, faculty and staff, and asked them for information about their passwords. Now we didn't say, "Give us your password." No, we just asked them about their password. How long is it? Does it have a digit? Does it have a symbol? And were you annoyed at having to create a new one last week? So we got results from 470 students, faculty and staff, and indeed we confirmed that the new policy was very annoying, but we also found that people said they felt more secure with these new passwords. We found that most people knew they were not supposed to write their password down, and only 13 percent of them did, but disturbingly, 80 percent of people said they were reusing their password. Now, this is actually more dangerous than writing your password down, because it makes you much more susceptible to attackers. So if you have to, write your passwords down, but don't reuse them. We also found some interesting things about the symbols people use in passwords. So CMU allows 32 possible symbols, but as you can see, there's only a small number that most people are using, so we're not actually getting very much strength from the symbols in our passwords.

This was a really interesting study, and now we had data from 470 people, but in the scheme of things, that's really not very much password data, and so we looked around to see where could we find additional password data? So it turns out there are a lot of people going around stealing passwords, and they often go and post these passwords on the Internet. So we were able to get access to some of these stolen password sets. This is still not really ideal for research, though, because it's not entirely clear where all of these passwords came from, or exactly what policies were in effect when people created these passwords. So we wanted to find some better source of data. So we decided that one thing we could do is we could do a study and have people actually create passwords for our study. So we used a service called Amazon Mechanical Turk, and this is a service where you can post a small job online that takes a minute, a few minutes, an hour, and pay people, a penny, ten cents, a few dollars, to do a task for you, and then you pay them through Amazon.com. So we paid people about 50 cents to create a password following our rules and answering a survey, and then we paid them again to come back two days later and log in using their password and answering another survey. So we did this, and we collected 5,000 passwords, and we gave people a bunch of different policies to create passwords with. So some people had a pretty easy policy, we call it Basic8, and here the only rule was that your password had to have at least eight characters. Then some people had a much harder policy, and this was very similar to the CMU policy, that it had to have eight characters including uppercase, lowercase, digit, symbol, and pass a dictionary check. And one of the other policies we tried, and there were a whole bunch more, but one of the ones

we tried was called Basic16, and the only requirement here was that your password had to have at least 16 characters.

All right, so now we had 5,000 passwords, and so we had much more detailed information. Again we see that there's only a small number of symbols that people are actually using in their passwords. We also wanted to get an idea of how strong the passwords were that people were creating, but as you may recall, there isn't a good measure of password strength. So what we decided to do was to see how long it would take to crack these passwords using the best cracking tools that the bad guys are using, or that we could find information about in the research literature.

So to give you an idea of how bad guys go about cracking passwords, they will steal a password file that will have all of the passwords in kind of a scrambled form, called a hash, and so what they'll do is they'll make a guess as to what a password is, run it through a hashing function, and see whether it matches the passwords they have on their stolen password list. So a dumb attacker will try every password in order. They'll start with AAAAA and move on to AAAAB, and this is going to take a really long time before they get any passwords that people are really likely to actually have. A smart attacker, on the other hand, does something much more clever. They look at the passwords that are known to be popular from these stolen password sets, and they guess those first. So they're going to start by guessing "password", and then they'll guess "I love you", and "monkey", and "12345678", because these are the passwords that are most likely for people to have. In fact, some of you probably have these passwords. So what we found by running all of these 5,000 passwords we collected through these tests to see how strong they were, we found that the long passwords were actually pretty strong, and the complex passwords were pretty strong too. However, when we looked at the survey data, we saw that people were really frustrated by the very complex passwords, and the long passwords were a lot more usable, and in some cases, they were actually even stronger than the complex passwords. So this suggests that, instead of telling people that they need to put all these symbols and numbers and crazy things into their passwords, we might be better off just telling people to have long passwords. Now here's the problem, though: some people had long passwords that actually weren't very strong. You can make long passwordsthat are still the sort of thing that an attacker could easily guess. So we need to do more than just say long passwords. There has to be some additional requirements, and some of our ongoing research is looking at what additional requirements we should add to make for stronger passwordsthat also are going to be easy for people to remember and type.

Another approach to getting people to have stronger passwords is to use a password meter. Here are some examples. You may have seen these on the Internet when you were creating passwords. We decided to do a study to find out whether these password meters actually work. Do they actually help people have stronger passwords, and if so, which ones

are better? So we tested password meters that were different sizes, shapes, colours, different words next to them, and we even tested one that was a dancing bunny. As you type a better password, the bunny dances faster and faster. So this was pretty fun.

What we found was that password meters do work. Most of the password meters were actually effective, and the dancing bunny was very effective too, but the password meters that were the most effective were the ones that made you work harder before they gave you that thumbs up and said you were doing a good job, and in fact we found that most of the password meters on the Internet today are too soft. They tell you you're doing a good job too early, and if they would just wait a little bit before giving you that positive feedback, you probably would have better passwords.

Now another approach to better passwords, perhaps, is to use pass phrases instead of passwords. So this was an xkcd cartoon from a couple of years ago, and the cartoonist suggests that we should all use pass phrases, and if you look at the second row of this cartoon, you can see the cartoonist is suggesting that the pass phrase "correct horse battery staple" would be a very strong pass phrase and something really easy to remember. He says, in fact, you've already remembered it. And so we decided to do a research study to find out whether this was true or not. In fact, everybody who I talk to, who I mention I'm doing password research, they point out this cartoon. "Oh, have you seen it? That xkcd. Correct horse battery staple." So we did the research study to see what would actually happen.

In our study, we used Mechanical Turk again, and we had the computer pick the random wordsin the pass phrase. Now the reason we did this is that humans are not very good at picking random words. If we asked a human to do it, they would pick things that were not very random. So we tried a few different conditions. In one condition, the computer picked from a dictionary of the very common words in the English language, and so you'd get pass phrases like "try there three come." And we looked at that, and we said, "Well, that doesn't really seem very memorable." So then we tried picking words that came from specific parts of speech, so how about noun-verb-adjective-noun. That comes up with something that's sort of sentence-like. So you can get a pass phrase like "plan builds sure power" or "end determines red drug." And these seemed a little bit more memorable, and maybe people would like those a little bit better. We wanted to compare them with passwords, and so we had the computer pick random passwords, and these were nice and short, but as you can see, they don't really look very memorable. And then we decided to try something called a pronounceable password. So here the computer picks random syllables and puts them together so you have something sort of pronounceable, like "tufritvi" and "vadasabi." That one kind of rolls off your tongue. So these were random passwords that were generated by our computer.

What we found in this study was that, surprisingly, pass phrases were not actually all that good. People were not really better at remembering the pass phrases than these

random passwords, and because the pass phrases are longer, they took longer to type and people made more errors while typing them in. So it's not really a clear win for pass phrases. Sorry, all of you xkcd fans. On the other hand, we did find that pronounceable passwords worked surprisingly well, and so we actually are doing some more research to see if we can make that approach work even better. So one of the problems with some of the studies that we've done is that because they're all done using Mechanical Turk, these are not people's real passwords. They're the passwords that they createdor the computer created for them for our study. And we wanted to know whether people would actually behave the same way with their real passwords.

So we talked to the information security office at Carnegie Mellon and asked them if we could have everybody's real passwords. Not surprisingly, they were a little bit reluctant to share them with us, but we were actually able to work out a system with them where they put all of the real passwordsfor 25,000 CMU students, faculty and staff, into a locked computer in a locked room, not connected to the Internet, and they ran code on it that we wrote to analyse these passwords. They audited our code. They ran the code. And so we never actually saw anybody's password.

We got some interesting results, and those of you Tepper students in the back will be very interested in this. So we found that the passwords created by people affiliated with the school of computer science were actually 1.8 times stronger than those affiliated with the business school. We have lots of other really interesting demographic information as well. The other interesting thing that we found is that when we compared the Carnegie Mellon passwords to the Mechanical Turk-generated passwords, there was actually a lot of similarities, and so this helped validate our research method and show that actually, collecting passwords using these Mechanical Turk studiesis actually a valid way to study passwords. So that was good news.

Okay, I want to close by talking about some insights I gained while on sabbatical last year in the Carnegie Mellon art school. One of the things that I did is I made a number of quilts, and I made this quilt here. It's called "Security Blanket." (Laughter) And this quilt has the 1,000 most frequent passwords stolen from the RockYou website. And the size of the passwords is proportional to how frequently they appeared in the stolen dataset. And what I did is I created this word cloud, and I went through all 1,000 words, and I categorised them into loose thematic categories. And it was, in some cases, it was kind of difficult to figure out what category they should be in, and then I colour-coded them.

Here are some examples of the difficulty. So "justin." Is that the name of the user, their boyfriend, their son? Maybe they're a Justin Bieber fan. Or "princess." Is that a nickname? Are they Disney princess fans? Or maybe that's the name of their cat. "Iloveyou" appears many times in many different languages. There's a lot of love in these passwords. If you look carefully, you'll see there's also some profanity, but it was really interesting to me to see that there's a lot more love than hate in these passwords.

And there are animals, a lot of animals, and “monkey” is the most common animal and the 14th most popular password overall. And this was really curious to me, and I wondered, “Why are monkeys so popular?” And so in our last password study, any time we detected somebody creating a password with the word “monkey” in it, we asked them why they had a monkey in their password. And what we found out – we found 17 people so far, I think, who have the word “monkey” – We found out about a third of them said they have a pet named “monkey” or a friend whose nickname is “monkey”, and about a third of them said that they just like monkeys and monkeys are really cute. And that guy is really cute.

So it seems that at the end of the day, when we make passwords, we either make something that’s really easy to type, a common pattern, or things that remind us of the word password or the account that we’ve created the password for, or whatever. Or we think about things that make us happy, and we create our password based on things that make us happy. And while this makes typing and remembering your password more fun, it also makes it a lot easier to guess your password. So I know a lot of these TED Talks are inspirational and they make you think about nice, happy things, but when you’re creating your password, try to think about something else.

On the base of
https://www.ted.com/talks/lorrie_faith_cranor_what_s_wrong_with_your_pa_w0rd/transcript?language=en#t-605173

3.3. Biometrics

WHAT IS BIOMETRICS AND HOW SAFE IS IT?

With the convenience of unlocking your phone or accessing your bank account. With a touch of your finger biometrics have now become an integral part of our lives.

What is Biometrics? The term is derived from “bio” meaning biology and “metrics” meaning units of measurement. Biometrics is the measurement of unique physical and behavioral characteristics of a living organism. The identification of individuals is made possible through biometric technology which includes fingerprint mapping, facial recognition, voice recognition, and retina scans. However, these are just some of the most well-known options. Unique identifiers such as the shape of an ear, the way someone sits and walks, body odors veins in one’s hands and facial contortions, are also being researched.

Biometric data can be divided into two types: behavioral biometrics and physiological biometrics.

Behavioral biometrics. The way we speak, type, and sign documents are all traits that are unique to every individual. Just as we are capable of recognising a person based on their voice or handwriting, behavioral biometric systems can do the same thing.

Physiological Biometrics. Physiological biometrics can recognise our unique physical attributes such as fingerprints, face, and iris.

How does biometric data improve security?

Traditional passwords have long been a weak point in security systems. Biometrics solves this issue by linking proof of identity to our bodies and behavior patterns. For instance, you can press your finger against a sensor on your phone to unlock the device. Your phone or laptop might scan your face before letting you log in. For security, biometrics works as a replacement for standard passwords when you register your biometrics on your personal devices.

The device will first ask you to complete an initial scan to build a profile around your Biometrics. After that, your biometric data will be collected and stored for future use. From that point on your device will compare all future login attempts with the data linked to your profile. For example, a fingerprint recognition system will initially ask you to scan different sides of your fingertip. Once this initial scan is complete, you can quickly log in with a tap of your finger.

The most secure biometric security systems store data directly on a device and protect it through a process known as encryption. If you erase the data from your phone or computer, it will be gone forever.

The main advantage of biometric data is its complexity. Biometric security systems are much more difficult to hack than traditional passwords due to the uniqueness of biometric data.

How safe is biometric security? Personal data can be easily collected without consent which is a major concern. Facial recognition is becoming increasingly common in everyday life. However, concerns about constant surveillance and data misuse are growing due to the massive amount of data collected and stored.

The risk of data breaches is another concern particularly for databases of personal information. It is important to note that biometric details cannot be changed like passwords. If biometric data is lost or stolen, it could be permanently compromised. Biometric scanners such as facial recognition systems are not foolproof. Fingerprint cloning is also a growing concern and is becoming increasingly common.

Here’s what you can do to protect your biometric data? To ensure the safety of your biometric data, it is important to consider where it is being stored. Storing biometric data on your device is a safer option than storing it with a service provider. There are many best practices that can be applied to various devices including mobile devices, laptops, and computers. It is recommended that you regularly take the time to install updates and change passwords often, always keep your devices up to date with the latest security updates.

On the base of https://www.youtube.com/watch?v=GytLOow-7OY

3.4. Security Token

SMART CARD INTRODUCTION

What is a Smart Card?

I'd like to talk with you about smart cards and versus SEC. If you're unfamiliar with the concept, a smart card is a plastic card that looks like a typical credit card but contains an embedded microprocessor. Many of us carry bank-issued chip cards which are credit cards with smart card capabilities. Just as chip, credit cards are preferable to magnetic strip cards because they are far more secure.

Smart cards are a much safer way for enterprises to protect their data than, for example, passwords alone. With smart cards, enterprises provide identification and authentication through strong two-factor authentication. What this means is: something you have – a smart card, and something you know – a Pin – to access that smart card.

With ever increasing threats, cyber threats companies of all sizes can use smart cards to increase their security and reduce threats. With two-factor authentication, companies significantly decrease the probability that the person requesting access to data is presenting false evidence of his or her identity.

Common uses for smart cards within businesses include: Windows smart card log on, secure VPN access, email signature, email encryption, and disk encryption. Enterprises using smart cards for strong authentication need a digital certificate which gets issued to the smart card.

The digital certificate identifies the user via the public key infrastructure which is commonly referred to as PKI. The user will use, for example, his or her digital certificate on the smart card to perform strong two-factor Windows smart card log on.

Smart cards are a smart choice for business. Each card has at a minimum two pins, typically: a user pin and an admin pin. The admin pin is used when a user needs to unblock the user pin. Anyone with the admin pin can easily reset the user pin and impersonate the user. That's where smart card management systems help.

A smart card management system protects the admin pin for each smart card that it manages ensuring that no malicious user will ever be able to retrieve the admin pin. Other benefits include certificate management, user pin management and smart card life cycle management.

On the base of https://www.youtube.com/watch?v=_iEnR6doeSA

Appendix 5. Psychological Tests

Cohen, A.D, Oxford, R., Chi, J.C. (2001) Learning Style Survey: Assessing Your Own Learning Styles Learning Style Survey*: Assessing Your Own Learning Styles A –Total
Retrieved from:
https://www.researchgate.net/publication/266356106_Learning_Style_Survey_Assessing_Your_Own_Learning_Styles_Learning_Style_Survey_Assessing_Your_Own_Learning_Styles_A_-Total

Instruction. For each item, circle the response that represents your approach. Complete all items. There are two activities representing twelve different aspects of your learning style. When you read the statements, try to think about what you generally do when learning. Do not spend too much time on any item – indicate your immediate feeling and move on to the next item

0 – never **1 – rarely** **2 – sometimes** **3 – often** **4 – always**

TEST № 1. HOW I USE MY PHYSICAL SENSES

1	I remember something better if I write it down.	0 1 2 3 4
2	I take detailed notes during lectures.	0 1 2 3 4
3	When I listen, I visualise pictures, numbers, or words in my head.	0 1 2 3 4
4	I prefer to learn with TV or video rather than other media.	0 1 2 3 4
5	I use colour-coding to help me as I learn or work.	0 1 2 3 4
6	I need written directions for tasks.	0 1 2 3 4
7	I have to look at people to understand what they say.	0 1 2 3 4
8	I understand lectures better when professors write on the board.	0 1 2 3 4
9	Charts, diagrams, and maps help me understand what someone says.	0 1 2 3 4
10	I remember peoples' faces but not their names.	0 1 2 3 4
	A – visual: TOTAL	
11	I remember things better if I discuss them with someone.	0 1 2 3 4
12	I prefer to learn by listening to a lecture rather than reading.	0 1 2 3 4
13	I need oral directions for a task.	0 1 2 3 4
14	Background sound helps me think.	0 1 2 3 4
15	I like to listen to music when I study or work.	0 1 2 3 4
16	I can understand what people say even when I cannot see them.	0 1 2 3 4
17	I remember peoples' names but not their faces.	0 1 2 3 4
18	I easily remember jokes that I hear.	0 1 2 3 4
19	I can identify people by their voices (e.g., on the phone).	0 1 2 3 4
20	20. When I turn on the TV, I listen to the sound more than I watch the screen.	0 1 2 3 4
	B – auditory: TOTAL	
21	I'd rather start to do things, rather than pay attention to directions.	0 1 2 3 4
22	I need frequent breaks when I work or study.	0 1 2 3 4
23	I need to eat something when I read or study.	0 1 2 3 4
24	If I have a choice between sitting and standing, I'd rather stand.	0 1 2 3 4
25	I get nervous when I sit still too long.	0 1 2 3 4
26	I think better when I move around (e.g., pacing or tapping my feet).	0 1 2 3 4
27	I play with or bite on my pens during lectures.	0 1 2 3 4

28	Manipulating objects helps me to remember what someone says.	0 1 2 3 4
29	I move my hands when I speak.	0 1 2 3 4
30	I draw lots of pictures (doodles) in my notebook during lectures.	0 1 2 3 4
	C – tactile / kinesthetic: TOTAL	

TEST № 2. HOW I FURTHER PROCESS INFORMATION

1	I can summarise information easily.	0 1 2 3 4
2	I can quickly paraphrase what other people say.	0 1 2 3 4
3	When I create an outline, I consider the key points first.	0 1 2 3 4
4	I enjoy activities where I have to pull ideas together.	0 1 2 3 4
5	By looking at the whole situation, I can easily understand someone.	0 1 2 3 4
	A – synthesising: TOTAL	
6	I have a hard time understanding when I don't know every word.	0 1 2 3 4
7	When I tell a story or explain something, it takes a long time.	0 1 2 3 4
8	I like to focus on grammar rules.	0 1 2 3 4
9	I'm good at solving complicated mysteries and puzzles.	0 1 2 3 4
10	I am good at noticing even the smallest details regarding some task.	0 1 2 3 4
	B – analytic: TOTAL	

Note!

This is only a general description of your learning style preferences. It does not describe you all of the time, but gives you an idea of your tendencies when you learn. Note that in some learning situations, you may have one set of style preferences and in a different situation, another set of preferences. Also, there are both advantages and disadvantages to every style preference. If on the sensory style preferences (visual, auditory, tactile / kinesthetic) you prefer two or all three of these senses (i.e., your totals for the categories are within five points or so), you are likely to be flexible enough to enjoy a wide variety of activities in the language classroom. On the other dimensions, although they appear to be in opposition, it is possible for you to have high scores on both, meaning that you do not have a preference one way or the other. Furthermore, learning style preferences change throughout your life, and you can also stretch them, so don't feel that you are constrained to one style.

TEST 1: HOW I USE MY PHYSICAL SENSES

If you come out as more visual than auditory, you rely more on the sense of sight, and you learn best through visual means (books, video, charts, pictures). If you are more auditory in preference, you prefer listening and speaking activities (discussions, lectures, audio tapes, role-plays). If you have a tactile / kinesthetic style preference, you benefit from doing projects, working with objects, and moving around (games, building models, conducting experiments).

TEST 2: HOW I FURTHER PROCESS INFORMATION

If you are a synthesising person, you can summarise material well, enjoy guessing meanings and predicting outcomes, and notice similarities quickly. If you are analytic, you can pull ideas apart and do well on logical analysis and contrast tasks, and you tend to focus on grammar rules.

Appendix 6. Roadmap for Teachers and Students on How to Use this Coursebook

1. Using the psychological tests in **Appendix 5**, the students can identify their "dominant" and "non-dominant" learning styles, such as visual, auditory, and kinesthetic modalities. Keep in mind that students may have a combination of different styles or modalities.

2. It is recommended that students initially focus on exercises aligned with their preferred, dominant learning style to maximise learning effectiveness. Over time, incorporating activities that target the "non-dominant" style can help create a more balanced approach. Students with mixed modalities can benefit from alternating between different methods. Throughout the course, students can switch between different learning styles to enhance their ability to develop various language skills more effectively.

3. Students can select exercises appropriate for different levels of foreign language proficiency – Exercise A for B1 level and Exercise B for B2 level. Exercises marked "A. & B." are designed for students working at both B1 and B2 levels, allowing for flexible practice aligned with their individual proficiency.

4. Students have opportunities to work independently, in small groups, and with the entire class, providing a diverse range of collaborative and individual practice that enhances their professional English language communication skills.

5. Each sub-unit includes sections such as Warm-up, Reading, Use of English (Vocabulary, Phrasal Verbs, Idioms, Grammar), Listening, Speaking, Writing, and Reflection and Synthesis, all aimed at developing students' professional communication skills in English.

6. The Revision Section at the end of each unit offers opportunities for students to review material and undertake engaging projects to consolidate their learning.

7. Appendices like the Mini-dictionary, Phrasal Verbs & Idioms, Grammar Bank, Tapescripts, Psychological Tests, and the Roadmap for Teachers and Students provide additional resources to support independent learning and effective coursebook usage.

8. Throughout the coursebook, exercises involving AI tools are designed to be engaging and relevant, helping students enhance their lexical and grammatical skills, analyse texts, paraphrase information, and develop critical thinking abilities.

Навчальне видання

Синекоп Оксана Степанівна
Литовченко Ірина Миколаївна
Чугай Оксана Юріївна

АНГЛІЙСЬКА МОВА ПРОФЕСІЙНОГО СПРЯМУВАННЯ. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА КІБЕРБЕЗПЕКА

Навчальний посібник

У 2-х частинах

Частина І

(Англійською мовою)

Технічне редагування *Наталії Тверезовської*

Подано в авторській редакції

Реєстр. № НП 25/26-301.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Свідоцтво про державну реєстрацію: серія ДК № 5354 від 25.05.2017 р.
просп. Берестейський, 37, м. Київ, 03056, Україна

Формат 60×84$^{1}/_{8}$. Гарнітура Times.
1 файл (4,69 Мб). Обл.-вид. арк. 15,97. Поз. 26-1-2-007.

Видавництво «Політехніка» КПІ ім. Ігоря Сікорського
вул. Політехнічна, 14, корп. 15
м. Київ, Україна, 03056
тел. (044) 204-81-78