ТЕОРЕТИЧНІ ЗАСАДИ ТА КРИПТОГРАФІЧНІ МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Шмалюк В.[1]

[1]*Харківській національний університет внутрішніх справ*

У сучасному цифровому світі, де обсяг переданої інформації зростає експоненційно, а її цінність – неоціненна, криптографія відіграє ключову роль у забезпеченні кібербезпеки. Інформаційні системи сьогодні – це не лише засіб обміну даними, а й простір для стратегічних операцій, конфіденційного спілкування, фінансових транзакцій і функціонування критичної інфраструктури. У таких умовах зростає потреба в ефективних механізмах захисту інформації від несанкціонованого доступу, підробки, перехоплення та викривлення. Саме криптографія забезпечує фундаментальні властивості безпеки – конфіденційність, цілісність, автентичність і незаперечність.

Потреба у криптографічних методах виникла з перших кроків розвитку цивілізації, однак у XXI столітті вона набула якісно нового значення. Якщо раніше шифрування використовувалося переважно у військовій сфері, то тепер його застосування стало повсюдним – від збереження медичних даних до захисту електронного голосування чи блокчейн-технологій. Криптографія є невід'ємною складовою протоколів безпечної комунікації в інтернеті, таких як HTTPS, VPN, IPsec, а також використовується в цифрових підписах, двофакторній аутентифікації, електронному документообігу та цифрових валютах.

Історія криптографії охоплює тисячоліття людського розвитку і є свідченням постійного прагнення захистити інформацію від стороннього доступу. Перші відомі приклади шифрування з'явилися ще в Давньому Єгипті, де жерці використовували ієрогліфи з прихованим значенням для передачі сакральної інформації. У Стародавній Греції було відомо про використання «скітали» – шифрувального

циліндра для перестановки букв, що забезпечував певний рівень секретності під час військових кампаній. Найвідомішим прикладом античного шифру є «шифр Цезаря», який полягав у зсуві букв алфавіту на фіксовану кількість позицій. Хоча такі методи здаються примітивними з сучасної точки зору, у свій час вони були ефективними інструментами приховування інформації.

З розвитком наук і технологій криптографія еволюціонувала. У середньовіччі застосовувалися складніші техніки, як, наприклад, шифр Віженера, який використовував поліалфавітний принцип і вважався незламним протягом століть. Проте з появою математичних методів криптоаналізу, зокрема в період арабського Ренесансу, деякі шифри було розкрито, що змусило криптографів шукати нові підходи. У XX столітті криптографія отримала стрімкий розвиток, особливо під час світових війн. Саме в цей період з'являються механічні шифрувальні пристрої, серед яких найвідомішою є «Енігма», що використовувалася німецькими військами у Другій світовій війні. Розшифрування «Енігми» союзниками, зокрема завдяки роботі Алана Тюрінга, стало важливим кроком не лише у розвитку криптоаналізу, а й у формуванні перших комп'ютерів.

З початком комп'ютерної епохи криптографія вступила у фазу стрімкої математизації. У 1970-х роках виникла сучасна симетрична та асиметрична криптографія. Широке поширення отримали алгоритми DES (Data Encryption Standard), а пізніше – AES (Advanced Encryption Standard), що й досі активно використовуються для шифрування даних. Проривом стало відкриття алгоритмів з відкритим ключем – зокрема RSA, який дозволяє безпечно обмінюватися даними навіть між незнайомими сторонами, не передаючи ключів у відкритому вигляді.

Криптографія, як наука про шифрування та захист інформації, включає кілька основних видів, кожен з яких має свої унікальні характеристики, принципи роботи та сфери застосування. Найбільш базовим і водночас найдавнішим типом є симетрична криптографія. У цій моделі використовується один і той самий ключ як для

шифрування, так і для розшифрування повідомлення. Це означає, що обидві сторони комунікації мають володіти спільним секретом, який повинен бути переданий безпечно ще до початку обміну даними. Симетричні алгоритми мають велику швидкість роботи, що робить їх особливо ефективними для шифрування великих обсягів даних у реальному часі. Одними з найпоширеніших симетричних шифрів є AES (Advanced Encryption Standard), який використовується в урядових та комерційних системах у всьому світі, та ChaCha20, що знайшов застосування у мобільних пристроях завдяки оптимізованій продуктивності.

Проте головним недоліком симетричної криптографії є складність у розповсюдженні ключів. Якщо кількість користувачів системи зростає, кількість унікальних пар ключів, які необхідно зберігати й захищати, збільшується експоненційно. Ця проблема частково вирішується завдяки асиметричній криптографії, що з'явилася в другій половині XX століття як радикально новий підхід до шифрування. Асиметричні системи базуються на використанні двох різних ключів – відкритого (public key) і закритого (private key). Відкритий ключ може бути вільно поширений і використовується для шифрування інформації, тоді як розшифрувати її можна лише за допомогою відповідного приватного ключа, який зберігається у суворій таємниці власником. Такий підхід дозволяє не передавати секретну інформацію під час обміну ключами, а також створює можливість реалізації цифрового підпису, що підтверджує справжність повідомлення та особу відправника. Найвідомішими прикладами асиметричних алгоритмів є RSA, DSA та алгоритми на еліптичних кривих (ECC), які забезпечують високий рівень безпеки навіть за умов обмежених обчислювальних ресурсів.

Попри свої переваги, асиметричні методи мають значно вищу обчислювальну складність порівняно з симетричними, що обмежує їх використання для шифрування великих масивів даних. Саме тому на практиці найчастіше використовується гібридна криптографія, яка поєднує переваги обох підходів. У гібридній схемі обмін

ключами або початкова автентифікація здійснюється за допомогою асиметричної криптографії, а сам обмін даними виконується за допомогою симетричних алгоритмів. Наприклад, під час встановлення захищеного з'єднання за протоколом HTTPS браузер спершу отримує відкритий ключ сервера та шифрує з ним випадковий симетричний ключ сесії, який далі використовується для основного обміну інформацією. Такий підхід забезпечує як високу швидкість, так і високий рівень захищеності комунікацій.

Методи шифрування та цифрового підпису є основними інструментами у криптографії, що забезпечують захист даних при передачі та зберіганні. Шифрування використовується для перетворення відкритої інформації (тексту) у зашифровану форму, яка незрозуміла стороннім особам. Принцип роботи полягає в тому, що навіть якщо зловмисник отримає доступ до зашифрованих даних, без відповідного ключа він не зможе їх розшифрувати й дізнатися зміст. Шифрування може бути симетричним або асиметричним, залежно від того, чи використовується один і той самий ключ для шифрування і дешифрування, чи пара відкритого і закритого ключів. У симетричному шифруванні широко застосовується алгоритм AES (Advanced Encryption Standard), який забезпечує надійний захист завдяки багаторівневому процесу перетворення даних із використанням блочних операцій і замін. У свою чергу, асиметричне шифрування, наприклад RSA, дозволяє захищати дані при їх пересиланні між сторонами, які не мають попередньо узгодженого секретного ключа.

Проте лише шифрування не забезпечує повного спектру криптографічних гарантій, зокрема автентичності та незаперечності. Для цього застосовується цифровий підпис – інструмент, який дозволяє перевірити, хто саме створив повідомлення, та чи не було воно змінено після підписання. Принцип цифрового підпису базується на використанні хеш-функцій та асиметричної криптографії. Коли користувач хоче підписати документ, він спочатку обчислює хеш (контрольну суму) цього документу — компактне представлення його вмісту фіксованої довжини. Потім ця хеш-сума шифрується приватним ключем

користувача, і результат додається до документа як цифровий підпис. Одержувач, отримавши підписаний документ, може обчислити хеш від отриманого тексту самостійно, розшифрувати підпис за допомогою відкритого ключа підписанта та порівняти ці значення. Якщо вони збігаються, документ є справжнім і не зміненим.

Серед найпоширеніших алгоритмів цифрового підпису варто відзначити RSA (Digital Signature Algorithm) та алгоритми на еліптичних кривих (ECDSA), які забезпечують високий рівень безпеки при меншій довжині ключа. У деяких випадках використовується також GOST-підпис, що є стандартом в окремих країнах пострадянського простору. Цифрові підписи стали важливою складовою інфраструктури електронного документообігу, електронної пошти, банківських систем та блокчейн-технологій. Наприклад, у криптовалюті Bitcoin цифровий підпис дозволяє підтвердити право власності на кошти та санкціонувати їх передачу в мережі без централізованої перевірки.

Криптографія є основою сучасних протоколів безпеки, які забезпечують захищене з'єднання в Інтернеті, захист мережевого трафіку, а також гарантують цілісність і достовірність транзакцій у децентралізованих системах. Одним із найважливіших і найпоширеніших прикладів є протокол TLS (Transport Layer Security), що використовується для забезпечення захищеної передачі даних у мережі. Коли користувач заходить на вебсайт із захищеним з'єднанням (https://), саме TLS забезпечує шифрування переданої інформації між браузером і сервером. Основна роль криптографії тут полягає у встановленні безпечного каналу зв'язку між сторонами, які раніше не обмінювались ключами. Для цього використовуються методи асиметричної криптографії на етапі встановлення з'єднання (так зване TLS-handshake), під час якого генерується симетричний ключ сесії. Надалі цей ключ використовується для шифрування даних із високою швидкістю.

Особливо помітна роль криптографії у блокчейн-технологіях, які є основою криптовалют,

децентралізованих додатків та смарт-контрактів. У блокчейні криптографія використовується для забезпечення цілісності транзакцій, підтвердження автентичності учасників мережі та створення незмінної структури даних. Одним з ключових криптографічних інструментів тут є геш-функції – вони дозволяють кожному блоку містити унікальний хеш, який залежить від вмісту самого блоку та хешу попереднього, утворюючи ланцюг, який неможливо змінити заднім числом без помітного втручання. Це забезпечує властивість незмінності (immutability), що є критичною для довіри у системі без централізованого контролю. Цифрові підписи, зокрема на основі алгоритмів ECDSA, гарантують, що лише власник відповідного приватного ключа може ініціювати транзакцію. Також криптографічні алгоритми відіграють роль у механізмах консенсусу, наприклад у процесі майнінгу, де складні обчислення хешів забезпечують захист мережі від шахрайства.

Попри надзвичайну важливість криптографії як одного з найнадійніших інструментів захисту інформації, її практична реалізація супроводжується низкою складних проблем, які суттєво впливають на ефективність і безпеку систем. Однією з головних проблем є так званий «людський фактор», який часто виявляється найслабшою ланкою в захищених системах. Навіть найсучасніші криптографічні алгоритми можуть бути скомпрометовані внаслідок неправильного зберігання ключів, слабких паролів, або через фішингові атаки, що змушують користувача розкрити свої облікові дані. Неправильне налаштування програмного забезпечення або недосвідченість адміністратора системи можуть призвести до ситуацій, коли криптографічний захист лише ілюзорно присутній, але насправді не виконує своїх функцій.

Ще одним критично важливим аспектом є складність управління ключами. У великих організаціях існує потреба в централізованому зберіганні, обміні, оновленні та відкликанні криптографічних ключів. Недостатньо налагоджені або застарілі механізми керування ключами призводять до численних вразливостей. Наприклад, якщо

ключі не змінюються регулярно або якщо після компрометації одного з них немає оперативного процесу його відкликання, вся система може бути скомпрометована. Особливо складною є ситуація, коли ключі передаються між різними системами або зберігаються на кінцевих пристроях без належного захисту, що створює ризики втрати або викрадення.

Також велике значення мають реалізаційні помилки у програмному коді. Навіть якщо використовується теоретично надійний алгоритм, його некоректна імплементація в програмному забезпеченні може відкрити шлях для атак. Наприклад, неправильне використання генераторів випадкових чисел у криптографічних протоколах часто призводить до слабких ключів, які зловмисник може відновити. Подібним чином, уразливості в бібліотеках, як-от OpenSSL чи libgcrypt, неодноразово ставали причиною масових інцидентів безпеки, серед яких варто згадати скандальну уразливість Heartbleed. Тому реалізація криптографічних засобів потребує найвищого рівня програмної дисципліни, перевірок, аудитів коду та незалежного тестування.

Окрему проблему становлять обчислювальні ресурси, необхідні для реалізації сучасних криптографічних алгоритмів. Асиметричні алгоритми, зокрема RSA або алгоритми на еліптичних кривих, є ресурсоємними, особливо у пристроях з обмеженими обчислювальними можливостями, таких як мобільні телефони, вбудовані системи або «інтернет речей» (IoT). Це часто змушує розробників шукати компроміси між продуктивністю та безпекою, що не завжди веде до оптимальних рішень.

Аналіз вразливостей криптосистем є одним із ключових напрямів у забезпеченні інформаційної безпеки, оскільки навіть найстійкіший теоретично криптографічний алгоритм може бути зламаний або обійдений через слабкі місця в його реалізації чи використанні. Уразливості в криптосистемах можуть виникати як на рівні алгоритмів, так і на рівні їх програмної або апаратної реалізації. Теоретичні вразливості стосуються, передусім, слабких математичних основ, на яких побудовано алгоритм.

Наприклад, шифри, що мають обмежений ключовий простір або недостатню ентропію, можуть бути піддані повному перебору (brute-force) або іншим видам криптоаналізу. Якщо алгоритм дозволяє передбачити певні шаблони у шифротексті або не забезпечує статистичну рівномірність вихідних даних, це також створює передумови для атаки.

Окрім суто математичних вразливостей, велику небезпеку становлять помилки реалізації. Навіть найнадійніший алгоритм може бути зкомпрометований, якщо він реалізований з порушенням криптографічних принципів. Прикладами таких вразливостей є використання незахищених генераторів випадкових чисел, неправильне управління пам'яттю або відсутність перевірки автентичності в протоколах шифрування.

Відомі атаки на реалізації, такі як атака таймінгу (timing attack), атака через побічні канали (side-channel attack) або атака на повторне використання ключів, демонструють, що загроза може виходити не від самого алгоритму, а від способу, яким він застосовується на практиці. Наприклад, атака Meltdown і Spectre використовували архітектурні особливості процесорів для отримання доступу до чутливих даних, у тому числі й криптографічних ключів, із пам'яті.

Ще одним критичним аспектом є людський фактор та організаційні помилки, які часто стають джерелом уразливостей.

Неправильне зберігання ключів, використання застарілих або скомпрометованих алгоритмів, відсутність регулярного аудиту безпеки, а також недбале ставлення до оновлень і патчів — усе це відкриває нові вектори атак. Наприклад, широко відома вразливість Heartbleed у бібліотеці OpenSSL дозволяла зловмисникам отримувати довільні фрагменти пам'яті з серверів, у тому числі й конфіденційні ключі. Іноді достатньо лише однієї помилки в коді або одного невчасно оновленого компонента системи, щоб створити потенційно катастрофічну загрозу.

Список використаних джерел

1. A Mathematical Proposed Model for Public Key Encryption Algorithms in Cybersecurity URL: https://www.researchgate.net/publication/354291983_A_MATHEMATICAL_PROPOSED_MODEL_FOR_PUBLIC_KEY_ENCRYPTION_ALGORITHMS_IN_CYBERSECURITY

2. Mathematical Approaches Transform Cybersecurity from Experimental to Scientific Discipline URL: https://www.mdpi.com/2076-3417/13/11/6508

3. Mathematical Models in Information Security and Cryptography URL: https://www.mdpi.com/journal/mathematics/special_issues/71516B35F0