НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра математичних методів захисту інформації

«До захисту допущено»
В.о. завідувача кафедри
_____ Сергій ЯКОВЛЄВ
«__» _____ 2022 р.

Дипломна робота

на здобуття ступеня бакалавра

зі спеціальності: 113 Прикладна математика
на тему: **«Аналіз ефективності і стійкості криптографічних систем з використанням математичних сейфів»**

Виконала: студентка 4 курсу, групи ФІ-84
Котович Анна Валентинівна _____

Керівник:
Професор, доктор фізико-математичних наук, Савчук М.М.

_____

Рецензент: звання, степінь, посада Прізвище І.П. _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент _____

Київ — 2022

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра математичних методів захисту інформації

Рівень вищої освіти — перший (бакалаврський)
Математичні методи криптографічного захисту інформації -
113 Прикладна математика,
ОПП «Математичні методи криптографічного захисту інформації»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ Сергій ЯКОВЛЄВ
«__» _____ 2022 р.

ЗАВДАННЯ
на дипломну роботу

Студент: Котович Анна Валентинівна

1. Тема роботи: «*ДОСЛІДЖЕННЯ І АНАЛІЗ СТІЙКОСТІ МАТЕМАТИЧНИХ СЕЙФІВ*»,

керівник:

професор, доктор фізико-математичних наук, Савчук Михайло Миколайович,

затверджені наказом по університету №__ від «__» _____ 2022 р.

2. Термін подання студентом роботи: «__» _____ 2022 р.

3. Вихідні дані до роботи: *Задачі про математичний сейф, криптографічні системи з використанням математичного сейфу, оцінки скалдності*

4. Зміст роботи: *Задачі про математичний сейф, системи автентифікації, системи шифрування та розшифрування, підстановка Віженера та підстановка М,*

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо): *3 рисунки: шялх з N вершин рис.1.1, контур з N вершин рис. 1.2, неорієнтований граф рис. 2.1*

6. Дата видачі завдання: 10 вересня 2021 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання	Примітка
1	Узгодження теми роботи із науковим керівником	01-15 вересня 2021 р.	Виконано
2	Огляд опублікованих джерел за тематикою дослідження	Вересень-жовтень 2021 р.	Виконано
3	Опрацювання основних теорем	Листопад-грудень 2021 р.	Виконано
4	Вивчення систем автентифікації, шифрування, підстановки Віженера	Березень - квітень 2021 р.	Виконано
5	Оцінювання ефективності та стійкості криптосистем	Квітень - травень 2021 р.	Виконано
6	Підведення підсумків	Травень - червень 2021 р.	Виконано

Студент _____ Котович А.В.

Керівник _____ Савчук М.М.

РЕФЕРАТ

Задачі, де необхідно, виходячи з початкового стану об'єкту, за певними правилами і мінімальними втрата и досягнути іншого, наперед заданого стану. Такі задачі мають загальну назву позиційні ігри, а в математичній постановці задачі – задачі про математичний сейф. Загальна постановка задачі про математичний сейф зводиться до розв'язання лінійної системи порівнянь. У даному дослідження проводитиметься аналіз ефективності та стійкості таких криптографічних систем.

Мета роботи: Провести аналіз ефективності та стійкості криптографічних систем з використанням математичних сейфів

Об'єкт дослідження: Інформаційні процеси в системах криптографічного захисту інформації

Предмет дослідження: Стійкість та ефективність криптографічних систем шифрування та автентифікації з використанням математичних сейфів

У роботі розглянуто теоретичні відомості про побудову та використання математичних сейфів та складність їх реалізації на скінченних кільцях. Проаналізована ефективність та стійкість деяких запропонованих криптографічних систем з використанням математичних сейфів: системи автентифікації та систем шифрування. Аналіз та отримані оцінки складності реалізації та стійкості показав, що ці криптографічні системи з використанням математичних сейфів є менш ефективними і не більш стійкими серед існуючих систем автентифікації та шифрування.

МАТЕМАТИЧНТЙ СЕЙФ, СИСТЕМИ ЛІНІЙНИЇ РІВНЯНЬ НАД СКІНЧЕННИМИ КІЛЬЦЯМИ І ПОЛЯМИ, КРИПТОГРАФІЧНІ СИМЕТРИЧНОГО ШИФРУВАННЯ, СИСТЕМИИ АВТЕНТИФІКАЦІЇ, АНАЛІЗ СТІЙКОСТІ ТА ЕФЕКТИВНОСТІ

ABSTRACT

Tasks, where necessary, based on the initial state of the object, according to certain rules and the minimum loss and achieve a different, predetermined state. Such problems are commonly called positional games, and in the mathematical formulation of the problem - problems about the mathematical safe. The general formulation of the problem of a mathematical safe comes down to solving a linear system of comparisons. This study will analyze the efficiency and stability of such cryptographic systems.

Purpose: To analyze the efficiency and stability of cryptographic systems using mathematical safes

Object of study: Information processes in cryptographic information security systems

Research subject: Stability and efficiency of cryptographic encryption and authentication systems using mathematical safes

The paper considers theoretical information about the construction and use of mathematical safes and the complexity of their implementation on finite rings. The efficiency and stability of some proposed cryptographic systems using mathematical safes are analyzed: authentication systems and encryption systems. Analysis and evaluations of implementation complexity and stability have shown that these cryptographic systems using mathematical safes are less efficient and no more stable among existing authentication and encryption systems.

MATHEMATICAL SAFE, SYSTEMS OF LINEAR EQUATIONS OVER FINISHED RINGS AND FIELDS, CRYPTOGRAPHIC SYMMETRIC ENCRYPTION, SYSTEMISTS SYSTEMS

ЗМІСТ

ВСТУП

Дослідження задач дискретної оптимізації є основою вдалого моделювання важливих соціальних, природних та інших процесів. Серед класу комбінаторних оптимізаційних задач особливе місце займають задачі на графах. Аналіз використання результатів досліджень дозволяє зробити висновок про актуальність нових підходів і методів комбінаторної оптимізації. Задачі з галузі теорії ігор, в яких необхідно виходячи з початкового стану об'єкту, за певними правилами і мінімальними втратами досягнути іншого, наперед заданого стану. Подібні задачі мають відношення комп'ютерних іграх, загально кажучи позиційні ігри, проте в математичній постановці їх назва хвучить як задачі про математичний сейф. У даному дослідженні розглядається розв'язання задачі про математичний сейф. Розкривається математична постановка задачі про математичний сейф, де продемонстровано, що її розв'язання зводиться до розв'язання систем лінійних рівнянь у скінченних кільцях та полях. Розкриваються методи та алгоритми розв'язання такого типу систем, де наводяться методи та алгоритми побудови базису множини розв'язків систем лінійних рівнянь для цих областей. Розглядається підстановка Віженера та М, а наприкінці проводиться аналіз криптосистем математичних сефів: автентифікації, шифрування. Більшк 20 років математичні сейфи використовуються для побудови криптографічних систем, зокрема систем автентифікації, шифрування. При цьому як правило не проводиться повний і детальний криптоаналіз таких систем щодо їх стійкості та можливості криптоатак на них. Дана робота присвячена перш за все вивченню теоретичних засад математичних сейфів, проведення криптоаналізу криптографічнмх систем, які застосову.ть математичні сейфи. Для цього потрібно провести криптоаналіз та зробити порівняння з аналогічними існуючими системами без використання мс.

Мета: Провести аналіз ефективності та стійкості криптографічних систем з використанням математичних сейфів

Для виконання мети необхідно:

1) Зробити огляд існуючої літератури, в яких вивчаються математичні сейфи та будуються криптографічні системи з їх використанням.

2) Освоїти математичні алгоритми використання математичних сейфів і описати оцінки кладності виконання операцій в математичних сейфах на скінченних кільцях.

3) Розглянути відомі криптосистеми з використанням мс і провести їх криптоаналіз: системи автентифікації, шифрування та симетрична система.

4) Оцінити ефективність та стійкість криптографічних систем з використаннямм мс і виконати порівняння з відомим криптосистемами з симетричними алгоритмами.

5) Зробити висновки щодо ефективності та стійкості.

У наступниих озділах описується виконання птсавлених завдань

1 ЗАДАЧА ПРО МАТЕМАТИЧНИЙ СЕЙФ

У роботі С.Л. Кривого, Г.І. Гогерчака «Кібернетика та комп'ютерні технології», 2020 розглянемо неформально термін математичний сейф як систему $Z = (z_1, z_2,...,z_n)$ взаємнопов'язаних між собою засувів так, що коли виконується поворот певного ключа в одному із засувів, то такий же поворот виконується і у всіх інших засувах, які пов'язані з ним. Задача про математичний сейф виникла в теорії комп'ютерних ігр, а також у криптографічних застосуваннях. Математичний сейф задається двома способами:

- за допомогою прямокутної матриці, елементи якої відповідають засувам, а значення її елементів – позиціям засувів, тобто у вигляді матриці $Z = ||z_{ij}||$, $i = 1,...,m, j = 1,...,n, i$

- за допомогою графа $G(V, E)$, де вершини відповідають засувам.

Ці способи будемо називати матричним сейфом і графовим сейфом відповідно. В матричному сейфі кожний засув z_{ij} й в і-му стовпчику. А в графовому сейфі, пов'язаними із засувом у вершині u є ті, які відповідають засувам розміщеним у вершинах, суміжних з вершиною u. Кожний із засувів може знаходитися в одній із декількох позицій. Всіх можливих позицій скінченне число: 0,1,...,k-1. Засув відкритий, якщо він знаходиться в позиції 0. В довільній іншій позиції засув вважається закритим. Початковий стан сейфа Z при першому способі задання визначається матрицею $B = ||b_{ij}||$, а при другому - позиціями засувів у вершинах. При цьому, якщо в якомусь засуві виконується поворот ключа, то всі засуви, які пов'язані з даним засувом, збільшують свої позиції на одиницю за модулем k.

Необхідно розв'язати таку задачу: виходячи з початкового стану сейфа, знайти таку послідовність засувів і число поворотів ключа в них, щоб сейф перейшов у положення відкритого, тобто коли всі засуви будуть знаходитися в позиції 0. Розглянемо строгу математичну постановку

задачі про матричний математичний сейф.

1.1 Математична постановка задачі

Загальна постановка задачі про математичний сейф була запропонована у роботах Донця Г.П. в 2002 році.

Означення 1.1. Математичним сейфом називається система $S(Z, b, <Z>)$, яка складається з множини замків $Z = \{z_1, z_2, ..., z_N\}$, b=$(b_1, b_2, .., z_N)$, де $b_i \in \{0,1,...,k_1\text{-}1\}$ – стан і-го замка, та множини $<Z> = \{Z_1, Z_2, ..., Z_N\}, z_1 \notin Z_1, Z_1 \in 2^z (1 \leqslant i, l \leqslant N)$. У результаті одного повороту ключем в замку z_l за годинниковою стрілкою $Z_j \in Z_1$ всі замки переходять зі стану b_j у стан$(b_j + 1)(mod k_j)$. Сейф уважається відкритим, якщо він знаходиться у стані $b = (0,0,...,0) = b_{fin}$. Необхідно знайти для кожного замку z_1 таку кількість поворотів x_i ключем, щоб відкрити сейф.

Вектор $\overrightarrow{x} = (x_1, x_2, ..., x_N)$ будемо називати розв'язком задачі про сейф. Множина $< Z >$ називається множиною інцидентності. Можемо записати у вигляді матриці інцидентності $A_0 = a_{i_j}^0$ розміром $N \times N$, де на головній діагоналі стоять нулі, а $a_{i_j}^0 = 1$, якщо z_1 належить множині $Z_i (1 \leqslant i, j \leqslant N)$, і - нулю в протилежному випадку. Матриці A_0 можна поставити у відповідність орієнтований граф $G(Z)$, в якому від вершини z_i в вершину z_j заходить дуга, якщо $a_{i_j}^0 = 1$. У залежності від отриманої складності матриці виникають різні задачі про математичний сейф. Позначимо $A = A_0 + E_N$, де E_N – одинична матриця. У стовпці нашої матриці, який відповідає j-у замку, стоять одиниці навпроти тих замків, які впливають на стан j-го замка. Враховуючи кількість всіх поворотів у цих замках та кількість поворотів x_j в даному замку, отримаємо сумарну кількість поворотів ключем, яка виконувалася в j-му замку. У сумі з початковим станом j-го замку це має дорівнювати $0(mod k_j)$. Тоді загальна задача про математичний сейф зводиться до розв'язання

лінійної системи порівнянь:

$\overrightarrow{xa_i} + b \equiv 0(modk_i), (1 \leqslant i \leqslant N)$, де $\overrightarrow{a_i}$ – і-й стовпчик матриці .

1.2 Алгоритм розв'язання задачі

Розглянемо приклад у дисертації ї Агі Аг Якуба Розв'язок задачі про математичний сейф на матрицях Якщо $k_i = K = const \ \forall \ 1 \leqslant i \leqslant N$, то такі замки називаються однотиповими. У цьому розділі розглянуто задачі з однотиповими замками для $K = 2$, тобто $b_i \in 0{,}1, (1 \leqslant i \leqslant N)$. Нехай граф утворює шлях (рис. 1.1)

Компонента – шлях з N вершин

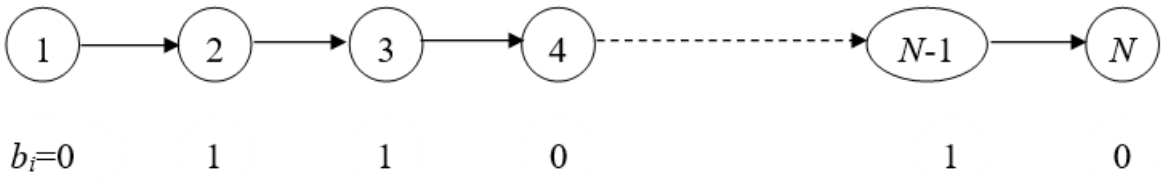

рис. 1.1

1. Припустимо, що $i = 1$

2. Якщо $b_i = 0$, то переходимо до вершини $i + 1$

3. Якщо $b_i = 1$, то робимо поворот в замку z_i , переводячи його стан в 0, а b_{i+1} переходить у стан $(b_{i+1})(mod2)$.

4.Тепер переходимо до вершини $i + 1$.

5. Урешті-решт приходимо до вершини N, стан якої переводимо в $b_N = 0$. У результаті для всієї компоненти отримаємо стани $b_i = 0(1 \leqslant i \leqslant N)$.

Розглянемо цикл з односторонньою орієнтацією – контур (рис. 1.2).

Контур з N вершин

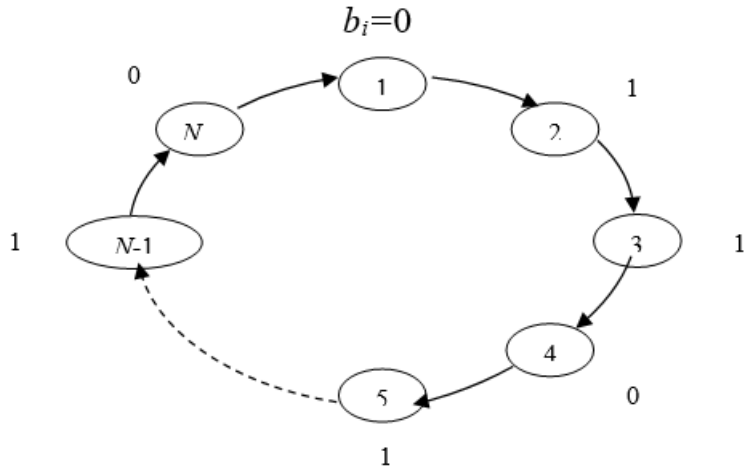

рис. 1.2

Лема 1.1. *Для того, щоб задача про математичний сейф для контура довжиною N мала розв'язок, необхідно і достатньо:*

$$\sum_{i-1}^{N} b_i \equiv 0(mod 2).$$

Такий же алгоритм, як і для шляху, застосовується і для циклу, у якого орієнтація неоднозначна, тому що він розпадається на декілька незалежних шляхів.

Для складніших орієнтованих графів доведені такі твердження:

Теорема 1.1. *Задача про сейф, заданий на транспортній мережі, завжди має розв'язок для довільного початкового стану.*

Теорема 1.2. *Задача про сейф, заданий на орієнтованому графі з незалежними контурами, має розв'язок для довільного початкового стану, якщо канонічний стан кожного контура задовольняє умову.*

Лема 1.2. *Задача про сейф, заданий на двох зв'язних контурах, має розв'язок для довільних початкових станів.*

Теорема 1.3. *Система рівнянь, записана для регулярного орієнтованого графа степеня 3, який складається з гамільтонового*

контура з діагоналями, є залежною тоді і тільки тоді, коли знайдеться такий підконтур, куди заходить парна кількість дуг, які можна розбити на спряжені пари.

Це останній результат для орієнтованих графів. Для неорієнтованих графів кількість залежних замків збільшується. Система порівнянь для ланцюга довжиною N, має вигляд:

$x_1 + x_2 ... \equiv b_1 mod 2$

$x_1 + x_2 + x_3 ... \equiv b_2 mod 2$

$. + x_2 + x_3 + x_4 ... \equiv b_3 mod 2$

. . . . . .

$. . . + x_{NP_{-1}} + x_N \equiv b_3 mod 2$

Лема 1.3. *Система порівнянь лінійно залежна тільки для* $N - 1(mod 3)$.

У цьому випадку система має розв'язок тільки при умові:

$$\sum_{j=1}^{l} (b_{3i-2} + b_{3i-1}) \equiv 0(mod 2).$$

де $l = \frac{N+1}{3}$

Теорема 1.4. *Якщо* $N \neq -1(mod 3)$, *то розв'язком задачі про сейф, заданий на неорієнтованому ланцюгу, є*

$x_\alpha \equiv \sum_{j=1}^{l} (b_{3i-2} + b_{3i-1})(mod 2), \alpha \equiv 0(mod 3); l = \frac{\alpha}{3};$

$x_\alpha \equiv \sum_{j=1}^{l} (b_{\alpha+3i+1} + b_{\alpha+3i+2})(mod 2), \alpha \equiv (N-2)(mod 3); l = \frac{N-2-\alpha}{3};$

$x_\alpha \equiv \sum_{j=1}^{l} (x_{\alpha-1} + b_\alpha + x_{\alpha+1})(mod 2), (x_0 = x_{n+1} = 0), \alpha \equiv (N-1)(mod 3);$

Лема 1.4. *Якщо цикл має довжину* $N \equiv 0(mod 3)$, *то ранг системи порівнянь для нього дорівнює* $N - 2$. *Це витікає з таких рівностей, які можна отримати безпосередньо:*

$\sum_{j=1}^{l} (b_{3i-1} + b_{3i-2}) = \sum_{j=1}^{l} (b_{3i} + b_{3i-1}) \equiv 0(mod 2); l = \frac{N}{3}$

З них випливають такі залежності

$b_{N-1} \equiv (\sum_{j=1}^{N-2} (b_i + \sum_{j=1}^{l-1} b_{3i})(mod 2)$

$b_{N-1} \equiv (\sum_{j=1}^{N-2} (b_i + \sum_{j=1}^{l-1} b_{3i-1})(mod 2)$

Якщо ці умови не виконуються, відповідна система порівнянь і сама задача не мають розв'язків.

Позначимо $R(i)$ *множину індексів* $i, i+1, i+3, i+4, ..., i+3j, i+3j=1$, *де* $l \leqslant i \leqslant Nj = |\frac{N}{3}$, *і суми індексів обчислюються за* $modN$

Теорема 1.5. *Якщо* $N \neq 0(mod3)$, *то задача про сейф, записана для циклу довжиною* N, *має розв'язок*

$x_\alpha \equiv \sum_{i \in R(\alpha-\theta}(b_i + b_\alpha - \theta)(mod2), l \leqslant \alpha \leqslant N$, *де* $\theta \equiv (N^2+N+1)(mod3)$;

Аналогічні результати одержані для складніших графів типу зірки, або колеса. Відповідні системи порівнянь, складені для них, мають подібну структуру, яка дозволяє обчислити визначники матриць. Наводяться формули розв'язків задач для цих графів.

1.3 Математичні сейфи на графах з різними типами замків

У дисертації [2] типи замків описуються вектором $K = k_1, k_2, \ldots, k_N$, де деякі компоненти можуть збігатися. Позначимо вектор $b(modK) = (b_1(modk1), b_2(modk2), \ldots, b_N(modkN))$. Тоді загальна задача про сейф на графах зводиться до розв'язування системи лінійних порівнянь $A\overrightarrow{x} \equiv -b(modK)$ (4)

Якщо існує обернена матриця A^{-1}, то звідси $\overrightarrow{x} \equiv A^{-1}b(modK)$

Алгоритм розв'язання задачі:

1) Припустимо, що $i = 1$.

2) Якщо $b_i \equiv 0(modk_i)(1 \leqslant i \leqslant N)$, то припускаємо $i = i + 1$.

3) Інакше припустимо $b'_{i \equiv (k_i - b_i)(modk_i),}$ $b'_{i_{+1} \equiv (b_i + 1 + k_i - b_i)(modk_{i+1}),}$ і переходимо до наступного замка. В результаті N кроків всі замки перейдуть в нульовий стан.

Можна побудувати інший, загальний алгоритм розв'язання цієї задачі. Він ґрунтується на локальному перемиканню одного замка, при

цьому стан залежного сусіднього замка не змінюється. Це зводиться до розв'язання системи з двох порівнянь:

$x \equiv a(modk_1), x \equiv 0(modk_2)$

де $k_1 \neq k_2$. Якщо найбільший спільний дільник (НСД) (k_1,k_2) = 1, то спочатку знаходимо $t \equiv k_2^{-1}(modk_1)$, тоді $xatk_2(modk_1k_2)$.

Якщо НСД(k_1,k_2) = $c < 1$, то при $a \neq 0(modc)$ система не має розв'язків. В протилежному випадку

$x \equiv (\frac{a}{c}\frac{k_2}{c}t(mod\frac{k_1k_2}{c}, t \equiv (\frac{k_2}{c})^{-1}(mod\frac{k_1}{c})$

Поступово застосовуючи цю формулу до вершин шляху в їх послідовності, отримаємо розв'язок задачі. Розглянемо контур (рис. 1.2) і запишемо для нього систему

$x_1 + ... + x_N \equiv -b_1(modk_1)$

$x_1 + x_2 + ... \equiv -b_2(modk_2)$

$. + x_2 + x_3 + ... \equiv -b_3(modk_3)$

. . . . . .

$. . . + x_{N-1} + x_N \equiv -b_N(modk_N)$ (6)

Визначник цієї системи $detA = 1(1)^N$. Для $N \equiv 1(mod2) detA = 2$, а для $N \equiv 0(mod2) detA = 0$. В іншому випадку один рядок матриці A лінійно залежний від інших, і для того, щоб система (6) мала розв'язок, необхідне виконання умови

$$\sum_{j=1}^{N} (-1)^i b_i \equiv 0(modk_1, k_2,...,k_N),$$

В цьому випадку, відкидаючи одне залежне порівняння із системи (наприклад, останнє), отримаємо систему для шляху, розв'язок якої відомий. Якщо не існує двох послідовних замків із взаємно простими числами $k1$ і $k2$, то задача не завжди має розв'язок.

Лема 1.5. *Задача для сейфів на контурі завжди має розв'язок, якщо*

$$\sum_{j=1}^{N} b_i \equiv 0(mod2)$$

Для неорієнтованих графів задача розв'язується складніше. Система порівнянь для ланцюга має вигляд

$$\sum_{j=1}^{N} b_i \equiv 0(mod2)$$

$x_1 + x_2 ... \equiv -b_1(modk_1)$

$x_1 + x_2 + x_3 ... \equiv -b_2(modk_2)$

$. + x_2 + x_3 + x_4 ... \equiv -b_3(modk_3)$

. . . . . .

$x_{N-2} + x_{N-1} + x_N \equiv -b_{N-1}(modk_{N-1})$ $x_{N-1} + x_N \equiv -b_N(modk_N)$

Теорема 1.6. *Визначник цієї системи дорівнює* $detA = C_N = -\frac{2}{\sqrt{3}} sin\frac{\pi(N-2)}{3}$ *(10) . Якщо* $N \equiv 2(mod3)$*, то оберненої матриці не існує. Тоді для існування розв'язку системи (9) необхідно виконання умови* $b_N - b_{N-1} + b_{N-3} - b_{N-4} + ... + b_2 - b_1 \equiv 0mod(K)$ *(11)*

Тоді N*-е порівняння та змінну* x_N *відкидаємо і переходимо до системи, визначник якої відмінний від нуля. Нема необхідності знаходити повністю обернену матрицю* A^{-1}*. Достатньо знайти вираз її першого рядка, це дозволить знайти значення* x_1*. Потім, подставляючи його в систему (9), послідовно знаходимо всі значення вектора* $\overrightarrow{x}$*.*

Теорема 1.7. *Для сейфа, заданого на зірці, для* $N > 2$

$$A^{-1} = \frac{1}{N-2} \begin{pmatrix} 1 & 1 & 1 & 1...1 \\ 1 & 1 & 0 & 0...0 \\ 1 & 0 & 1 & 0...0 \\ 1 & 0 & 0 & 1...0 \\ ..... & & & \\ 1 & 0 & 0 & 0...1 \end{pmatrix},$$

$detA = -N + 2$

Для розв'язання задачі можна безпосередньо знайти обернену матрицю.

Теорема 1.8. *Для сейфа, заданого на циклі, при* $N > 3$ *справедливо* $A^{-1} = -(-1)^{N+1} 4sin^2 \frac{\pi N}{3}$

Для різних значень N *можна отримати формули, які визначають всі невідомі системи порівнянь. Та краще застосувати алгоритм, який дозволяє послідовно розв'язати задачу, тобто перевести всі замки в нульовий стан.*

Алгоритм: *Починаючи з першого замка, робимо в кожному наступному повороти ключем в напрямку, протилежному знаку стану лівого замка, доти, поки останній не перейде в нульовий стан.*

Особливість цього алгоритма полягає в тому, що в ньому не треба робити ніяких обчислень, пов'язаних з модулями.

Перша необхідна умова розв'язності системи :

$m \neq 1(modK); n \neq 1(modk); m + n \neq 1(modK)$

Для системи $A^{-1} = T_{m,n(\alpha,\beta,\gamma,\theta}$, де

$$\alpha \equiv \frac{1}{m-1} + \frac{1}{m-1} + \theta(modK)$$

$$\beta \equiv \frac{1}{n-1} + \theta(modK)$$

$$\gamma \equiv \frac{1}{m-1} + \theta(modK)$$

$$\theta \equiv -(\frac{1}{n-1} + \frac{1}{m-1})\frac{1}{m+n+1}(modK)$$

Друга умова розв'язності системи (9): а) для простого числа K розв'язок існує завжди; б) для складеного числа K розв'язок існує завжди , якщо

$(m-1, K) = (n-1, K) = (m+n-1, K) = 1$

Для сейфів з замками одного типу отримані розв'зки у явному вигляді. Для цього використовуються позначення змінних та станів замків у матричному вигляді.

Позначимо $\sum_{\lambda=1}^{m}\sum_{\eta=1}^{n} = \sum(b)$ $\sum_{\lambda=1}^{m} b_{\lambda j} = \lambda_j; \sum_{\eta=1}^{n} b_{\eta i} = \sigma_i$ Тоді

$x_{ij} = [b_{ij} + \frac{1}{m-1}(\frac{\sum(b)}{m+n-1} - \lambda_j) + \frac{1}{n-1}(\frac{\sum(b)}{m+n-1} - \sigma_i)](modK)$, lt $1 \leqslant i \leqslant m; 1 \leqslant j \leqslant n$. Для різних співвідношень m і n знайдено конкретні формули. Якщо в сейфі є замки різних типів, то розв'язок задачі може як ускладнитися, так і спроститися в залежності від різних відношень між кількістю замків та числами, якими описуються стани цих замків. Позначимо $M = k_1,k_2 \ldots k_N$, де k_i – прості числа. Для такого сейфа всі теоретичні висновки про розв'язання системи (4) можна отримати по аналогії.

Теорема 1.9. *Розв'язок системи (4) для довільної кількості типів замків зі взаємно простими задовольняє системі порівнянь $Ax + b$, де A – це матриця. Тоді формули (14) і (15) запишуться аналогічно, якщо замість модуля K всюди записати модуль M. Для складених чисел k_i $(1 \leqslant i \leqslant q)$ проблема ускладнюється, але не принципово, а чисто технічно через велику кількість часткових випадків.*

Висновки до розділу 1

1. Задачі про математичний сейф, на орієнтовані та неорієнтовані графи, продемонстровано зведення її до розв'язання системи лінійних порівнянь за скінченим модулем.

2. Для графів розв'язана задача про математичні сейфи, замки яких мають тільки два стани, і отримані відповідні формули у явному вигляді.

3. Розроблені методи розв'язання задачі на графах для математичних сейфах, які мають замки або однакових, або різних типів.

4. Розглянули необхідні умови існування розв'язку задачі про математичний сейф, заданих на матрицях.

2 ВИКОРИСТАННЯ МОДЕЛІ МАТЕМАТИЧНОГО СЕЙФА

Розв'язання задачі про математичний сейф зводиться до розв'язання системи лінійних однорідних рівнянь (СЛОР) за модулем k вигляду: $Bx + a \equiv 0(modk)$, де матриця B розмірності mn×mn , коефіцієнти якої 0 і 1. Складнішою постановкою задачі є: знайти розв'язок задачі про математичний сейф у вигляді розв'язання СЛОР $Bx + a - c \equiv 0(modk)$, в скінченнолму кільці типу $AKK1_k$. Це означає, що числовою областю, над якою задано МС, є кільце $AKK1_k$, побудоване нижченаведеним способом, а сейф відкривається коли позиції засувів дорівнюють значенням вектора c. Тоді в загальному випадку для побудови асоціативно-комутативного кільця k–го порядку з одиницею $AKK1_k$ у статті Кривий С.Л. Застосування комутативних кілець з одиницею для побудови системи симетичного шифрування No 3, 2022 рік, необхідно виконати такі алгоритми:

Алгоритм 2.1

ADDAB-AKK1(1,k)

1) Задекларувати масив $T + [kk]$;

2) Занести в T_+ в перші рядок і стовпчик результати додавання з нулем кільця;

3) Занести в T_+ в рядок і стовпчик з номером 2 значення операції додавання з елементом 1);

4) c:=1;

5) Взяти в T_+ елемент $c' = c + 1$;

6) Для всіх x занести в рядок і стовпчик з номером c' масиву T+ значення $c' + x = (c + 1) + x = c + (1 + x)$;

7) $c := c', c' := c + 1$; Якщо $c' = 0$ то СТОП, інакше повернутися до кроку 5).

Алгоритм 2.2

MUL-TAB-AKK1(1,k)

1) Задекларувати масив $T.[kk]$;

2) Занести в T. в рядок і стовпчик з номером 0 і 1 результати операції множення на 0 і на 1;

3) $c := 1$;

4) Взяти в T+ елемент $c' = c + 1$;

5) Для всіх x занести в рядок і стовпчик з номером c' масиву T значення $c'x = (c + 1)x = cx + x$;

6) $c := c'; c' := c + 1$; Якщо $' = 0$, то СТОП, інакше повернутися на крок 4).

Застосування моделі математичного сейфу дає змогу утворити процес автентифікації двох абонентів, які беруть участь в обміні повідомленнями.

2.1 Система автентифікація

Автентифікація полягає в даній послідовності дій: надіслати абоненту певну пару (T + [1,k],c); отримати від нього у відповідь розв'язок, який у свою чергу має відкривати сейф. Водночас кільце, в якому розв'язується задача про математичний сейф не в окжному випадку має бути кільцем G, воно може бути як і довільним скінченним кільцем, так і полем. Якщо такий розв'язок відкриває сейф, тоді наш абонент легальний, у протилежному ж випадку абонент хибний. Процес отримання підтвердження легальності абонента за отриманим розв'язком, дає дозвіл абонентам на отрмання доступу до параметрів алгоритма **RG-EN** для виконання шифрування.

Розглянемо **RG-EN** спосіб шифрування з використанням властивостей кільця:

Алгоритм 2.3

RG-EN

1) Довільним чином задати рядок додавання з одиницею T_+[1,k] (адитивна група кільця була повноциклічною), сюр'єкцію $g : G \to M$ і ключове слово p;

2)Побудувати кільце G, порядок якого km за рядком T_+[1,k];

3)Побудувати по символам шифрограму $d = d_1 d_2 ... d_3$ для $\vec{b} = n_1 n_2 ... n_3$ за правилом $d_i = k_l + g(m_i)$, де k_l – номер символа ключового слова, $g(m_i)$ – образ номера символа xi X повідомлення b, + – операція додавання кільця G (до речі, шифрування може також використовувати над кільцями операцію множення);

4) Надіслати відкритим каналом абоненту шифрограму d, а закритим – дану трійку (T_+[1,k],g, p).

Розшифрування відбувається за наступними кроками:

Алгоритм 2.4

RG-DE

1) Абонент за рядком T_+[1,k] будує кільце G;

2) За отриманою шифрограмою d і в їх цифровому зображенні ключовим словом p для кожної пари відповідних символів розв'язує рівняння за допомогою таблиці додавання або множення кільця $a_i + x_i = d_i$ або $a_i x_i = d_i$, де a_i – номер символа ключового слова, d_i - символ шифрограми;

3) Знаходить m_i номер класу, який відповідає символу відкритого тексту x_i, і таким чином відкриває оригінальний текст.

Таким чином, вищенаведені алгоритми **Алгоритм 2.3** і **Алгоритм 2.4** перетворюються в такі алгоритми:

Алгоритм 2.5

RGM-EN($T + [1,k_1],$)

1) Вислати закритим каналом рядок $T + [1,k_1]$ і вектор , які визначають кільце $AKK1_k$ (або параметри поля, де розв'язується задача про МС) і комбінацію, що відкриває сейф.

2) Вислати відкритим каналом вектор a.

3) Чекати на отримання розв'язку d задачі про МС в кільці $AKK1_k$. Якщо d відкриває сейф, то виконати крок 4, інакше СТОП(«нелегал в мережі»).

4) Виконати алгорим **GM-EN**($T + [1,k],g,$) і вислати абоненту дозвіл на роботу.

Алгоритм 2.6

RGM-DE($T + [1,k_1],$)

1) За отриманим рядком $T + [1,k_1]$ побудувати кільце AKK1k.

2) За ориманими векторами a і розв'язати систему в кольце AKK1k і знайти розв'язок d.

3) Вислати отриманий розв'язок d абонету, який прислав параметри ($T + [1,k_1],$).

4) Якщо дозвіл на роботу від абонента отриманий, то (йому відкривається доступ до шифрограми) виконати алгоритм **GMD-E**($T + [1,k],g,$).

2.2 Робота алгоритмів шифрування і розшифрування з використанням моделі МС

1) 1. Розглянемо роботу алгоритмів шифрування і розшифрування з використанням моделі МС. Нехай МС заданий матрицею A, за якою будується СЛОР $Bx + a = c(mod25)$, де

$$A = \begin{pmatrix} 21 & 12 & 11 & 6 & 12 & 18 \\ 23 & 22 & 0 & 14 & 21 & 13 \end{pmatrix}$$

Матриця системи B, розширена останнім стовпчиком a-c, набуває вигляду:

$$A = \begin{bmatrix} 111111100000 & 21 \\ 111111010000 & 12 \\ 111111001000 & 11 \\ 111111000100 & 6 \\ 111111000010 & 12 \\ 111111000001 & 18 \\ 100000111111 & 23 \\ 010000111111 & 22 \\ 001000111111 & 0 \\ 000100111111 & 14 \\ 000010111111 & 21 \\ 000001111111 & 13 \end{bmatrix}$$

Розв'язуємо систему:
a=(9,7,12,4,5,21,5,4,2,17,20,20), c=(16,12,4,10,9,20,7,5,2,11,2,7) в кільці $AKK1_{25}$. Переносимо стовпчик вільних членів у ліву частину і виконуємо операції віднімання в кільці $AKK1_{25}$, тоді отримємо систему неоднорідних лінійних рівнянь. Розв'язком даної системи є вектор d = (23,16,10,18,18,7,21,9,3,2,3,15,19), який надсилається абоненту, що прислав рядок T + [1,25] і вектор . Якщо надісланий вектор d відкриває

сейф (у такому випадку отримувач є легальним), то далі відправник виконує крок 4 алгоритму **GM-EN** (T + [1,k],g,) і надсилає своєму абоненту дозвіл на майбутню роботу. Результат розв'язку для отримувача означає легальність відправника - він отримує доступ до шифрограми. Слід зазначити, що для сумісності системи лінійних рівнянь потрібно стежити за тим, щоб сума коефіцієнтів рядків матриці B' за модулем k не дорівнювала 0, а сума координат вектора d' дорівнювала 0 і навпаки - достатня умова для сумісності системи.

У даному випадку слабким місцем автентифікації є те, що матриця $'$ системи має стандартний вигляд, що спрощує шлях криптоаналітика. Для уникнення такого недоліку, є вхід задати математичний сейф на графах, оскільки структура матриці залежить від топології графа і тому є можливість бути довільною. Дана властивість передається вектором списків суміжності вершин графа, його довжина не перевищує число ребер графа $2|E|$.

2) Розглянемо МС, заданий неорієнтованим графом, який задає сейф, вектор списку суміжних вершин якого має вигляд $(1 : 2, 4 : 11; 2 : 8; 3 : 5,9; 4 : 7,10; 5 : 12; 6 : 7,9; 7 : 8; 9 : 12; 10 : 11)$, і параметрами a,c з попереднього приклада на рис.1:

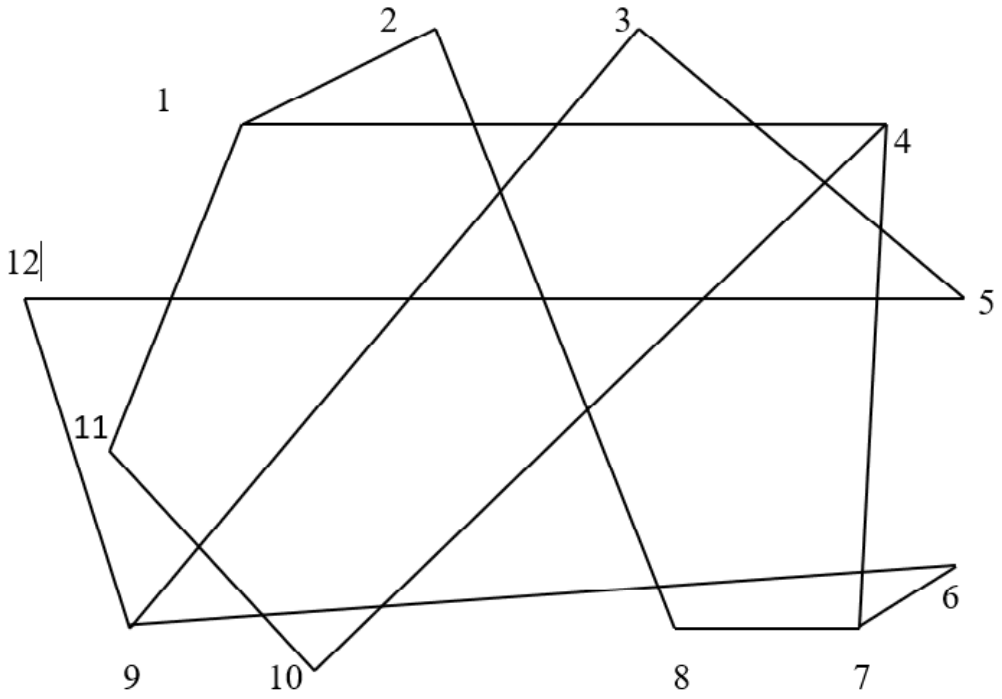

рис.2.1

Матриця системи $Bx + a - c = 0$, для заданого таким графом сейфа, має вигляд:

$$B' = \begin{bmatrix} 110100000010 & 21 \\ 110000010000 & 12 \\ 001010001000 & 11 \\ 100100100100 & 6 \\ 001010000001 & 12 \\ 000001101000 & 18 \\ 000101110000 & 23 \\ 010000110000 & 22 \\ 001001001001 & 0 \\ 000100000110 & 14 \\ 100000000110 & 21 \\ 000010001001 & 13 \end{bmatrix}$$

Розв'язком цієї системи в кільці $AKK1_{25}$ є вектор

(2,1,15,14,11,19,24,15,16,8,15,18,14), який після нормалізації (тобто множення на коефіцієнт 3, оскільки $3 \cdot 14{=}1$) дає розв'язок $d = (9,3,21,1,6,2,10,21,5,20,21,19)$, який відкраває сейф. Наступні кроки розвиваються йде у відповідності з приведеними алгоритмами **RGM-EN** $(T + [1,k_1],c)$ і **RGM-DE** $(T + [1,k1],c)$.

Таким чином, у цьому варіанті криптоаналітику серед іншого невідома також структура матриці B, що робить складнішою його роботу. Також мають місце бути інші варіації

3) Нехай задача про МС розв'язується в кільці за модулем 2 з матрицею початкових позицій засувів

$$A=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

а відкриває сейф така комбінація:

$$C=\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Матриця B’ системи має вигляд:

$$B'=\begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$Bx + a \equiv c(mod2)$

1 1 1 1 0 0 1 = 1 (mod 2)

1 1 1 0 1 0 0 = 0 (mod 2)

1 1 1 0 0 1 0 = 1 (mod 2)

1 0 0 1 1 1 0 = 0 (mod 2)

0 1 0 1 1 1 0 = 1 (mod 2)

0 0 1 1 1 1 0 = 0 (mod 2)

Розв'язком цієї системи є вектор $x = (1, 0, 1, 0, 0, 1)$, проте він не відкриває сейф. Перетворимо наш розв'язок, аби мати змогу відкрити сейф:

4) Нехай задача про МС розв'язується в кільці за модулем 27 з матрицею початкових позицій засувів

$$A = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

а відкриватиме сейф така комбінація,

$$C = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$$

Матриця B' системи має вигляд:

$$B' = \begin{bmatrix} 1 & 1 & 1 & 3 & 0 & 0 & 2 & 0 & 0 \\ 1 & 1 & 1 & 0 & 3 & 0 & 0 & 2 & 0 \\ 1 & 1 & 1 & 0 & 0 & 3 & 0 & 0 & 2 \\ 1 & 0 & 0 & 3 & 3 & 3 & 2 & 0 & 0 \\ 0 & 1 & 0 & 3 & 3 & 3 & 0 & 2 & 0 \\ 0 & 0 & 1 & 3 & 3 & 3 & 0 & 0 & 2 \\ 1 & 0 & 0 & 3 & 0 & 0 & 2 & 2 & 2 \\ 0 & 1 & 0 & 0 & 3 & 0 & 2 & 2 & 2 \\ 0 & 0 & 1 & 0 & 0 & 3 & 2 & 2 & 2 \end{bmatrix}$$

Це означає, що поворот ключа в засувах першого рядка змінить позиції засувів на 1, поворот в засувах другого рядка змінять позиції засувів на 3 одиниці, а третього рядка – позиції засувів на 2 одиниці. Тоді СЛНДР $Bx + a \equiv c(mod 27)$ набуває вигляду:

$Bx + a \equiv c(mod 27)$

1 1 1 3 0 0 2 0 0 1 = 1 (mod 27)

1 1 1 0 3 0 0 2 0 2 = 2 (mod 27)

1 1 1 0 0 3 0 0 2 0 = 3 (mod 27)

1 0 0 3 3 3 2 0 0 0 = 4 (mod 27)

0 1 0 3 3 3 0 2 0 0 = 5 (mod 27)

0 0 1 3 3 3 0 0 2 0 = 6 (mod 27)

1 0 0 3 0 0 2 2 2 0 = 7 (mod 27)

0 1 0 0 3 0 2 2 2 0 = 8 (mod 27)

0 0 1 0 0 3 2 2 2 0 = 9 (mod 27)

Розв'язком цієї системи є вектор $x = (4, 5, 18, 20, 20, 7, 24, 24, 18)$, алу він не відкриває сейф. Перетворимо наш розв'язок, аби мати змогу відкрити

сейф:

• перші три координати, які стають у відповідність з коефіцієнтами 1, залишаються незмінними;

• другі три координати, які стають у відповідність з коефіцієнтами 3, множаться на 3 за модулем 27;

• треті три координати, які стають у відповідність з коефіцієнтами 2, множаться на 2 за модулем 27.

В результаті приходимо до розв'язку $d = ((4, 5, 18, 6, 6, 21, 21, 21, 9)$, який нарешті відкриває сейф. Демонмтруємо:

$$A = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$\rightarrow (x_{11} = 4)$

$$A = \begin{pmatrix} 5 & 6 & 4 \\ 4 & 0 & 0 \\ 4 & 0 & 0 \end{pmatrix}$$

$\rightarrow (x_{12} = 5)$

$$A = \begin{pmatrix} 10 & 11 & 9 \\ 4 & 5 & 0 \\ 4 & 5 & 0 \end{pmatrix}$$

$\rightarrow (x_{13} = 18)$

$$A = \begin{pmatrix} 1 & 2 & 0 \\ 4 & 5 & 18 \\ 4 & 5 & 18 \end{pmatrix}$$

$\rightarrow (x_{21} = 6)$

$$A = \begin{pmatrix} 7 & 8 & 0 \\ 16 & 17 & 3 \\ 10 & 11 & 18 \end{pmatrix}$$

$\rightarrow (x_{22} = 6)$

$$A = \begin{pmatrix} 7 & 8 & 21 \\ 10 & 11 & 24 \\ 10 & 11 & 12 \end{pmatrix}$$

$\rightarrow (x_{23} = 21)$

$$A = \begin{pmatrix} 1 & 8 & 21 \\ 4 & 11 & 24 \\ 4 & 5 & 6 \end{pmatrix}$$

$\rightarrow (x_{31} = 21)$

$$A = \begin{pmatrix} 1 & 2 & 21 \\ 4 & 5 & 24 \\ 25 & 26 & 0 \end{pmatrix}$$

$\rightarrow (x_{33} = 9)$

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$$

Даний метод побудови криптосистеми є можливість удосконалити, якщо розглядати прямі добутки примарних кілець. Це дозволяє виконувати автентифікацію в одному кільці, а шифрування - у другому, а передачу секретної інформації - у третьому (яке також може бути полем).

2.3 Підстановка Віженера та М

Розглянемо криптографічних систем, розрахованих на користувачів широкого кола. Серед них можна вказати на систему шифрування Віженера у дисертації Агі Аг Якуба Розв'язок задачі про математичний сейф на матрицях». На відміну від багатоалфавітної підстановки, в алгоритмі Шифрування Віженера ключ має кінцеву довжину. Таким чином, тут відсутня вимога шифрувати кожну букву вихідного тексту окремим значенням ключа.

Підстановка Віженера визначається як VIG : $(x_0, x_1, ..., x_{n-1}) \rightarrow$ $(y_0, y_1, .., y_{n-1}) = [(x_0 + k_0)\text{mod N}, (x_1 + k_1)\text{mod N}, \ldots, (x_{n-1} + k_{n-1})\text{mod N}]$, де N - кількість символів в алфавіті, а n - довжина ключа Віженера з компонентами k_i,(i=0, 1, ..., n).

Таким чином, на вихідний текст накладається періодична ключова послідовність рівної довжини, та в результаті додавання по модулю N відповідних елементів послідовностей, що виходить на виході шифрований текст Y

Розглянемо математичний сейф із однотипними замками з числом станів K. Для неї можна побудувати криптографічну систему, де шифрування

текстів пропонується.

Підстановка M, яка визначається як M : $(s_1, s_2, ..., s_N) \to (y_1, y_2, .., y_N)$ =$[(s1 + x1)modK, .., (s2 + x2)$modK, . ., $(sN + xN)$mod K], де додавання набора вихідного тексту S = [s1, s2, ..., sN] ведется по всей длине решения X = $(x_1, x_2, ..., x_N)$ задачі про математичний сейф з вихідним вектором станів $b = (b_1.,b_2,. . . . . ,b_N)$.

Відкритий текст складається в порядку нумерації елементів матриці, або вектор станів сейфа. Розглянемо спочатку приклад K = 2. Нехай n = 6, m = 4, а матриця (вектор) початкового стану сейфа дорівнює

$$B = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

$\overrightarrow{b}^T$ = (1,0,0,1,0,1,0,1,1,1,1,1,0,0,0,1,1,0,0,1,0,1,0,0,1)

Розв'язанням цього завдання буде матриця (вектор):

$$B = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

X $\equiv A \overrightarrow{b} (mod2)$

тоді X $\equiv$ (0,0,0,1,0,0,0,1,0,0,1,0,0,0,0,0,0,0,0,0,1,0,0,0).

Необхідно зашифрувати наступний текст S = (0,1,0,1,1,1,0,1,1,0,1,1,0,1,1,1,0.1,1,0,0,1,0,1).

Звідси отримаємо відповідність S = $(s_1, s_2, ..., s_N)$ + X $\to$ Y =

$(y_1, y_2, .., y_N)$, а саме S = (0,1,0,1,1,1,0,1,1,0,1,1,0,1,1,1,0.1,1,0,0,1,0,1). →
→ Y = (0,1,0,0,1,1,0,0,1,0,0,1,0,1,1,1,0.1,1,0,1,1,0,1).

Щоб криптоаналітику розшифрувати цей текст, знаючи механізм шифрування, необхідно відновлювати матрицю, для чого доведеться перебрати 2^{mn} варіантів. Для $K \geqslant 3$ проблема виглядає складніше.

Розглянемо приклад:

Нехай K = 7, n = 4, m = 3, а матриця (вектор) початкового стану сейфа дорівнює:

$$B = \begin{pmatrix} 0 & 3 & 1 & 0 \\ 5 & 6 & 0 & 2 \\ 3 & 3 & 5 & 1 \end{pmatrix}$$

$\overrightarrow{b}^T$ = (1,5,3,3,1,0,6,5,0,1,3,0)

Необхідно зашифрувати наступний текст: S = (5,4,0,2,1,6,3,2,6,5,4,1)

Обчисломо дробні значення:

$$\frac{1}{m-1} = \frac{1}{2} \equiv t_1 \,(mod 7)\,, t_1 \equiv 4\,(mod 7)$$

$$\frac{1}{n-1} = \frac{1}{3} \equiv t_2 \,(mod 7)\,, t_1 \equiv 5\,(mod 7)$$

$$\frac{1}{m+n-1} = \frac{1}{6} \equiv t_3 \,(mod 7)\,, t_1 \equiv 6\,(mod 7)$$

Обчислимо елементи оберненої матриці

$$\alpha_1 = -\,(4+5)\cdot 6 \equiv 2\,(mod 7)$$
$$\alpha_1 = 4+5-1+2 \equiv 3\,(mod 7)$$
$$\alpha_2 = 5+2 = O\,(mod 7)$$
$$\alpha_3 = 4+2 = 6\,(mod 7)$$

Звідси обернена матриця:

$$A^{-1} = \begin{pmatrix} 3 & 0 & 0 & 0 & 6 & 2 & 2 & 2 & 6 & 2 & 2 & 2 \\ 0 & 3 & 0 & 0 & 2 & 6 & 2 & 2 & 2 & 6 & 2 & 2 \\ 0 & 0 & 3 & 0 & 2 & 2 & 6 & 2 & 2 & 2 & 6 & 2 \\ 0 & 0 & 0 & 3 & 2 & 2 & 2 & 6 & 2 & 2 & 2 & 6 \\ 6 & 2 & 2 & 2 & 3 & 0 & 0 & 0 & 6 & 2 & 2 & 2 \\ 2 & 6 & 2 & 2 & 0 & 3 & 0 & 0 & 2 & 6 & 2 & 2 \\ 2 & 2 & 6 & 2 & 0 & 0 & 3 & 0 & 2 & 2 & 6 & 2 \\ 2 & 2 & 2 & 6 & 0 & 0 & 0 & 3 & 2 & 2 & 2 & 6 \\ 6 & 2 & 2 & 2 & 6 & 2 & 2 & 2 & 3 & 0 & 0 & 0 \\ 2 & 6 & 2 & 2 & 2 & 6 & 2 & 2 & 0 & 3 & 0 & 0 \\ 2 & 2 & 6 & 2 & 2 & 2 & 6 & 2 & 0 & 0 & 3 & 0 \\ 2 & 2 & 2 & 6 & 2 & 2 & 2 & 6 & 0 & 0 & 0 & 3 \end{pmatrix}.$$

$$\overrightarrow{b}^T = (-A^{-1}\overrightarrow{b}) \equiv (4,3,5,0,0,0,3,4,1,4,3,2)$$

$$B = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 4 & 3 & 0 & 0 \\ 0 & 5 & 3 & 4 \end{pmatrix}$$

Звідси отримаємо відповідність S = $(s_1, s_2, ..., s_N) \to$ Y = $(y_1, y_2, .., y_N)$, а саме S = (5,4,0,2,1,6,3,2,6,5,4,1) $\to$ Y = (0,0,4,3,5,2,3,2,6,3,0,5). Щоб криптоаналітику розшифрувати цей текст, знаючи механізм шифрування, необхідно відновлювати матрицю, для чого доведеться перебрати K^{mn} варіантів. Тут можна досягти певної гарантії навіть якщо користуватися порівняно невеликими значеннями K.

Слід зазначити, що запропонований метод шифрування розрахований на інформацію, яка втрачає свою цінність за короткий час після передачі.

Сюди можна зарахувати, наприклад, таку інформацію, яка передається по мобільних телефонах, Маючи невелике програмуюче пристрій для дешифрування та шифрування, який компактно може підключатись до телефону, можна надійно захистити необхідну інформацію від несанкціонованого її вилучення.

Висновки до розділу 2

Запропоновано спосіб побудови простої криптосистеми на основі властивостей асоціативно-комутативних кілець з одиницею і моделлю математичного сейфа, заданого матрицею або графом. Пропонована система має великий простір ключів, необхідний для стійкості системи. Для побудови такої системи необхідно реалізувати (при необхідності) алгоритми побудови таблиць операцій кільця і пошуку розв'язків систем лінійних рівнянь в кільці $_{1k}$. Знайдені розв'язки такої системи повинні відкривати сейф, а відкриття сейфа означає ідентифікацію абонентів, які обмінюються повідомленнями. З цією метою пропонуються алгоритми побудови таблиць операцій кільця з поліноміальною оцінкою складності, поліноміальні алгоритми розв'язання систем лінійних рівнянь в примарних кільцях і полях. Шифрування і розшифрування теж виконуються в поліноміальному часі від величини порядку кільця . Продемонстровано, що графовий сейф в криптографічному сенсі має певні переваги над матричним сейфом. Слід зазначити, що метод шифрування підстановка М розрахований на інформацію, яка втрачає свою цінність за короткий проміжок часу після передачі. Сюди можна зарахувати, наприклад, таку інформацію, яка передається по мобільних телефонах - можна надійно захистити необхідну інформацію від несанкціонованого її вилучення.

3 АНАЛІЗ КРИПТОСИСТЕМ З ВИКОРИСТАННЯМ МАТЕМАТИЧНИХ СЕЙФІВ

Проаналізуємо криптосистему автентифікації користувачів А і В з використанням математичних сейфів, описану в розділі 2, базуючись на статті Кривого С.Л. «Застосування комутативних кілець з одиницею для побудови системи симетричного шифрування». Користувач А проводить автентифікацію користувача В з використанням математичного сейфу на основі кільця. Зробимо порівняння з симетричною системою шифрування.

3.1 Аналіз системи автентифікації з використанням математичного сейфу.

Проаналізуємо криптосистему автентифікації користувачів А і В з використанням математичних сейфів, описану в розділі 2, базуючись на статті Кривого С.Л. «Застосування комутативних кілець з одиницею для побудови системи симетричного шифрування». Користувач А проводить автентифікацію користувача В з використанням математичного сейфу на основі кільця. Зробимо порівняння з симетричною системою шифрування.

1) Користувач А пересилає заздалегідь В по закритому каналу таємну інформацію T+[1,k1] для побудови кільця і секретні позиції засувів с. Тобто попередня передача секретної інформації іде по закритому каналу, аналогічно як це робиться в симетричних криптоалгоритмах. І можна порівняти кільце і СЛОР з алгоритмом шифрування в симетричній криптосистемі, а вектор с з секретним ключем. Складність алгоритму додавання у кільці (k^2logk), а множення - $O((klogk)^2)$, де k – порядок кільця. Арифметична складність переходу від попереднього переходу до наступного лінійних однорідних діафантових рівнянь в одній підсистемі пропорційна величині l^5, а оскільки ця дія

повторюється r разів, то отримуємо оцінку $O(l^6)$, де l=max(n, s, r), n – кількість невідомих, s – кількість рівнянь у системі. Система виявилася неефективною, стійкість буде залежати від довжини цього параметру для звичайних систем у маккоді, але складність буде більше, тому вона буде неефективна з точки зору практичності.

2) В симетричних шифрах згідно правилу Керкгоффа алгоритм шифрування повинен бути несекретним, а таємним тільки секретний ключ. Як відомо, секретність алгоритму в сучасних умовах не вважають додатковим захистом. Для системи, яка аналізується, при багатократній автентифікації, скоріше всього структура кільця буде знайдена за поліноміальний час. Тому кільце треба вважати несекретним. Складність такої системи буде базуватися на складності обчислення системи рівнянь, яка знаходить відповідно рішення цього рівняння. Арифметична складність переходу від попереднього переходу до наступного лінійних однорідних діафантових рівнянь в одній підсистемі пропорційна величині l^5, а оскільки ця дія повторюється r разів, то отримуємо оцінку $O(l^6)$, де l=max(n, s, r), n – кількість невідомих, s – кількість рівнянь у системі. Якщо не використовувати таємну передачу параметрів, тоді відповідно система автентифікації буде зовсім нестійка, ще буде неефективна у тому плані, якщо вона використовує таємний якийсь параметр, який попередньо передається, то для нової автентифікації потрібно буде і ще раз передавати таємний параметр

3) Нехай структура кільця відома, тоді оскільки початковий стан математичного сейфу вектор a і розв'язок d передаються при автентифікації по відкритому каналу, то за одну перехоплену автентифікацію зловмисник знайде таємний ключ. Для другої автентифікації користувач A повинен генерувати новий вектор c і заздалегідь передавати його по закритому каналу. Зовсім неефективна автентифікація. Добре відома автентифікація на основі симетричних криптосистем. Оскільки сучасні симетричні шифри стійкі до атак на основі ВТ, то відомі запит і відповідь при автентифікації не дадуть змоги

зловмиснику знайти секретний ключ.

3.2 Аналіз криптосистеми шифрування з використанням математичних сейфів для автентифікації.

Проаналізуємо криптосистему шифрування з використанням математичних сейфів, описану в розділі 2 на основі статті Кривого С.Л. «Застосування комутативних кілець з одиницею для побудови системи симетричного шифрування». Автор застосовує алгебраїчний апарат скінченних асоціативно-комутативних кілець з одиницею для побудови криптосистем симетричного шифрування, в якій для автентифікації використовується математичний сейф. Математичний сейф використовується в системі тільки для автентифікації і на стійкість системи шифрування запропонована процедура не впливає. Що стосується автентифікації з використанням математичних сейфів, аналіз стійкості і ефективності алгоритму проведено в пункті 3.1. Проаналізуємо алгоритм шифрування в запропонованій криптосистемі. Якщо ключове слово включається до складу секретного ключа, то отримаємо періодичний шифр, в якому заміна пари літер (букви відкритого тексту та відповідної літери ключа) на літеру шифрованого тексту відбувається за допомогою побудованих таблиць операцій у кільці. У порівнянні з шифром Віженера ускладнення в тому, що заміна такої пари буде не за допомогою модуля, а за допомогою секретних таблиць. Цей шифр складніший за шифр Віженера, але за сучасними уявленнями також не є стійким. Застосування математичного сейфу не робить систему шифрування Віженера в даному випадку більш стійким, вона буде відразу ж провально нестійкою по відношенню до атаки на основі відкритого тексту, коли відомий відкритий та шифрований текст. Вона буде нестійка і відповідно буде не дуже стійка, коли атака буде на основі тільки шифротексту. У більш загальному вигляді (у тому числі з

можливим використанням групових операцій) такі шифри під назвою «табличне гамування» описані, наприклад, у навчальному посібнику: Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А .В. Основі криптографии. - М.: Гелиос АРВ, 2001. - 480 с. Аналіз також показав, що використання бієкцій кільця з одиницею як простору секретних ключів (за наявності також бієкцій на алфавіті) не є суттєвим для побудови наведеного шифру і не робить його більш стійким, ускладнюючи при цьому його практичне використання. Стійкість криптосистем з обмеженими ключами визначається як потужністю ключового простору, так і неефективністю всіх можливих атак, а не лише методу повного перебору. Велика кількість можливих ключів криптосистеми є необхідною, але далеко не достатньою умовою для стійкості. Запропонована система шифрування є варіантом періодичних поліалфавітних шифрів з використанням асоціативно-комутативних кілець з одиницею для побудови бієктивних відображень (що можна робити й іншими способами). За сучасними поняттями така криптосистема буде мати слабкості навіть до атак на основі шифрованого тексту і зовсім нестійкою до атак на основі відкритого тексту.

3.3 Криптосистема шифрування, яка базується на математичному сейфі.

Розглянемо криптосистему шифрування, запропоновану в дисертації Агаі Аг Гаміш Якуб «Розв'язок задачі про математичний сейф на матрицях», а також описану в розділі 2.

На відміну від загальної постановки задачі на матрицях можуть виникнути задачі зі скороченими правилами:

1) кожен замок впливає тільки на замки на рядку 2) кожен замок впливає тільки на замки у стовпчику 3) кожен замок впливає тільки на інші замки в рядку і на один замок, що розташований нижче

Розглянемо перший випадок:

$$A = \begin{pmatrix} \Theta_n & 0 & 0 & ... & ... 0 \\ 0 & \Theta_n & 0 & ... & ... 0 \\ 0 & 0 & \Theta_n & ... & ... 0 \\ ... & ... & ... & ... & ... ... \\ 0 & 0 & 0 & ... & ... 0 \end{pmatrix}$$

Для перших n значень шуканий розв'язок X заишуться з основного рівняння:

$x_{11} + x_{12} + x_{13} + ... + x_{1n} = b_1$

$x_{11} + x_{12} + x_{13} + ... + x_{1n} = b_2$

$x_{11} + x_{12} + x_{13} + ... + x_{1n} = b_3$

.....

$x_{n1} + x_{n2} + x_{n3} + ... + x_{nn} = b_n$

Рішенням системи існуватиме тоді та тільки тоді, коли

$b_1 = b_2 = b_3 = ... = b_n$

Розглнемо другий виадок:

$$A = \begin{pmatrix} E_n & E_n & E_n & ... & ... \mathrm{E}_n \\ E_n & E_n & E_n & ... & ... \mathrm{E}_n \\ E_n & E_n & E_n & ... & ... \mathrm{E}_n \\ ... & ... & ... & ... & ... ... \\ E_n & E_n & E_n & ... & ... \mathrm{E}_n \end{pmatrix}$$

Для наступних n значень шуканого розв'язку X запишуться з основного рівняння:

$\mathrm{x}_{1,n+1}$

$x_{11} + x_{1,n+1} + x_{1,2n+1} + x_{1,3n+1} + ... + x_{1,(m-1)n+1} = b_{11}$

$x_{11} + x_{1,n+1} + x_{1,2n+1} + x_{1,3n+1} + ... + x_{1,(m-1)n+1} = b_{1,n+1}$

$x_{11} + x_{1,n+1} + x_{1,2n+1} + x_{1,3n+1} + ... + x_{1,(m-1)n+1} = b_{1,2n+1}$

.....

$x_{11} + x_{1,n+1} + x_{1,2n+1} + x_{1,3n+1} + ... + x_{1,(m-1)n+1} = b_{1,(m-1)n+1}$

У даному випадку у правій частині стоть елементи першого стовпчика матриці B, а ліворуч одні йті самі доданки. Рішення існує тоді та тільки тоді, коди праві частини рівні сіж собою, тобто хп однакових замках в першому стовпчику матриці B. Знову маємо справу з n повторами онакових замків - сейф відчиниться за n незалежних поворотів замків. Ця система шифрування зводиться до системи Віженера, є нестійкою при атаці на основі шифрованого тексту при достатній довжині криптограми і зовсім нестійкою при атаці на основі відкритого тексту.

Висновки до розділу 3

У даному розділі було розглянуто системи автентифікація з використанням математичного сейфу, було виконано порівняння з симетричною системою порівняння - оскільки сучасні симетричні шифри стійкі до атак на основі відеритого тексту, то запит та відповідь при автентифікації не дадуть змоги зловмиснику знайти секретний ключ. Аналіз криптосиситеми шифрування з використанням математичних сейфів для автентифікації, був застосований алгебраїчний апарат скінченних асоціативних-комутативних кілець з одиницею для побудови криптосистем симетричного шифрування, в якій для автентифікації використовується математичний сейф - цей шифр складніший за шифр Віженера, але за сучасними уявленнями також не є стійким.
У ході дослідження проводилося порівняння з симетричною системою шифрування. Аналіз системи автентифікації з використанням математичого сейфу базувався на застосуванні комутативних кілець з одиницею для побудови симетричного шифрування. При першому

випадку, коли А пересилає заздалегідь В по закритому каналу таємну інформацію для побудови кільця і секретні позиції засувів с – система виявилася неефективною, стійкість залежатиме від довжини параметруу маккоді, але складність буде більше, тому з точки зору практичності система неефективна. У другому випадку, коли не використовувати таємну передачу параметрів, тоді система автентифікації буде зовсім нестійка та неефективна, тому що вона використовує секретний параметр, який попередньо передається і для кожної наступної автентифікації буде ще раз передавати таємний параметр. У третій розглянутій події структура кільця відома і вже за одну перехоплену автентифікацію зловмисник знайде таємний ключ. Застосування математичного сейфу не робить систему Віженера в даному випадку стійкою по відношенню до атаки на основі відкритого тексту. Така автентифікація буде неефектина,. Проте при автентифікація на основі симетричних криптосистем відомі запит і відповідь не дадуть зловмиснику знайти секретний ключ, оскільки сучасні симетричні шифри стійкі до атак на основі відкритого тексту Проводився аналіз криптосистеми шифрування з використанням математичних сейфів для автентифікація. У порівняння з шифром Віженера цей шифр складніший, але за сучасними стандартами також не є стійким. Використання бієкцій з одиницею як простору секретних ключів не є суттєвим для побудови наведеного шифру і не робить його більш стійким, ускладнюючи при цього практично застосування. За сучасними нормами така криптосистема буде мати слабкості навіть до атак на основі відкритого тексту.

ВИСНОВКИ

У ході дослідження було поставлено задачу розглянути відомі криптосистеми з використанням мс і провести їх криптоаналіз: системи автентифікації, шифрування та симетрична система, наступним кроком оцінити ефективність та стійкість криптографічних систем з використаннямм мс і виконати порівняння з відомим криптосистемами з симетричними алгоритмами, проаналізувати ефективність та стійкість. Аналіз системи автентифікації з використанням математичого сейфу базувався на застосуванні комутативних кілець з одиницею для побудови симетричного шифрування: у випадку коли А пересилає заздалегідь В по закритому каналу таємну інформацію для побудови кільця і секретні позиції засувів с – система виявилася неефективною, а стійкість залежна від довжини параметру у маккоді, складність буде більше, тому з точки зору практичності система неефективна: у другому випадку, коли не викорситовується таємна передача параметрів, то система автентифікації буде зовсім нестійка та неефективна, оскільки вона використовує секретний параметр, який попередньо передається і для кожної наступної автентифікації буде ще раз передавати таємний параметр: у третій розглянутій події структура кільця відома і вже за одну перехоплену автентифікацію зловмисник знайде таємний ключ, що дає зробити висновки про систему автентифікації як неефектину. При автентифікація на основі симетричних криптосистем відомі запит і відповідь не дадуть зловмиснику знайти секретний ключ, оскільки сучасні симетричні шифри стійкі до атак на основі відкритого тексту Проводився аналіз криптосистеми шифрування з використанням математичних сейфів для автентифікація. У порівняння з шифром Віженера цей шифр складніший, але за сучасними стандартами також не є стійким. Застосування математичного сейфу не робить систему Віженера в даному випадку стійкою по відношенню до атаки на основі відкритого тексту.

Використання бієкцій з одиницею як простору секретних ключів не є суттєвим для побудови наведеного шифру і не робить його більш стійким, ускладнюючи при цього практично застосування. За сучасними нормами така криптосистема буде мати слабкості навіть до атак на основі відкритого тексту. Аналіз задач на матрицях показав, що система шифрування зводиться до системи Віженера, є нестійкою при атаці на основі шифрованого тексту при достатній довжині криптограми і зовсім нестійкою при атаці на основі відкритого тексту.

ПЕРЕЛІК ПОСИЛАНЬ

1) С.Л. Кривого, Г.І. Гогерчака «Кібернетика та комп'ютерні технології», 2020

2) Донець Г.А. Решение задачи про математический сейф на (0,1)-матрицах». «Кибернетика и системный анализ».–2002.–№ 1.

3) Агаи Аг Гамиш Якуб «Решение задачи а математическом сейфе на матрицах» – 2016, Киев С. 23-52

4) Кривий С.Л. «Застосування комутативних кілець з одиницею для побудови системи симетичного шифрування» № 3, 2022 рік

5) Крывый С.Л. Численные методы решения задачи о математическом сейфе. ж. «Кибернетика и системный анализ».– 2016. - С.20-24

6) Агаи Аг Гамиш Якуб «Решение задачи а математическом сейфе на матрицах» – 2016, Киев С. 106-109

7) Калужнин Л.А. «Введение в общую алгебру». – М.:Наука. – 1973. – 447 с.

8) Кук Д., Бейз Г. «Компьютерная математика». – М.: Наука. – 1990. – 384 с.

9) Кривий С.Л. Криптосистема на основі абелевих груп і кілець. Ж. «Проблемы программирования». – № 2-3. – 2020. – С. 270-277.

10) Коблиц Н. «Курс теории чисел и криптографии». – М.: Изд-во ТВП. – 2001. – 260 с.

11) Черемушкин А. В. «Лекции по арифметическим алгоритмам в криптографии». – М.:МЦНМО. – 2002. – 103 с.

12) Донец Г.А. Решение задачи о сейфе на (0,1)-матрицах. ж. «Кибернетика и системный анализ».–2002.–№ 1. – С. 98-105.

13) А.Л. Гурин «Методы решения задач о математических сейфах на матрицах с разными типами замков, 2019, № 4

14) Чжань Бинь «Решение матричной задачи о математическом

сейфе с различными замками», 2006, № 4

15) Крывый С. Л. «Алгоритмы решения систем линейных диофантовых уравнений в кольцах вычетов. ж. «Кибернетика и системный анализ». – 2007. – No 6. - С. 27- 40.

16) Агаи Аг Гамиш Якуб, Г.А. Донец «Теорія оптимальних рішень», 2013