Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

# МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Метод криптоаналізу на основі часткових латинських квадратів»

Виконав студент 2-го курсу, групи
1БС-23м
спеціальності 125 – Кібербезпека
та захист інформації
ОПП «Безпека інформаційних та
комунікаційних систем»
_____ Олег СЕМЕНЮК

Керівник: доц. кафедри ЗІ, к.фіз-мат.н., доцент
_____ Галина ШЕЛЕПАЛО

Опонент: к.т.н., доц., доц. каф. ПЗ
_____ Олександр ХОШАБА

**Допущено до захисту**
Завідувач кафедри ЗІ,
д.т.н., проф.
_____ Володимир ЛУЖЕЦЬКИЙ

"16" ____12____ 2024 р.

м. Вінниця – 2024

Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації
Освітній рівень – другий (магістерський)
Галузь знань – 12 «Інформаційні технології»
Спеціальність – 125 «Кібербезпека та захист інформації»
Освітньо-професійна програма – «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ
Зав. кафедри ЗІ, д.т.н., проф.
_____ Володимир ЛУЖЕЦЬКИЙ
"18" 09 2024 р.

**ЗАВДАННЯ**
**НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ**

Семенюку Олегу Андрійовичу

1) Тема: Метод криптоаналізу на основі часткових латинських квадратів. керівник роботи: Шелепало Галина Василівна, к.фіз-мат.н., доцент, доц. кафедри ЗІ затвердженні наказом № 310 ректора ВНТУ від 17.09.2024.
2) Строк подання студентом роботи 16.12.2024 р.
3) Вихідні дані до роботи:
   Метод шифрування на основі латинських квадратів для потокового шифрування на CIP-квазігрупах 4-го порядку за ізотопами групи Клейна. Секретний ключ побудований на основі латинських квадратів 3-го порядку. Формули комбінаторики та статистики і теорії ймовірностей для випадків криптографічного аналізу заданого шифру
4) Зміст розрахунково-пояснювальної записки
   Вступ.
   1. Аналіз та огляд літературних джерел
   2. Аналіз та визначення секретного ключа
   3. Розробка алгоритму криптоаналізу відновлення секретного ключа
   4. Економічний розділ

   Висновки.
   Перелік використаних джерел
   Додатки
5) Перелік ілюстративного матеріалу: Блок схема алгоритму заповнення латинського квадрата, Відновлення латинських квадратів частина 1, Відновлення латинських квадратів частина 2, Відновлення латинських квадратів частина 3, Відновлення латинських квадратів частина 4, Таблиця Келі групи Кляйна.

6) Консультанти розділів роботи

| Розділ | Прізвище, ініціали та посада консультанта | Підпис, дата | |
|---|---|---|---|
| | | завдання видав | завдання прийняв |
| 1 | Галина ШЕЛЕПАЛО., к.фіз-мат.н., доц. каф. ЗІ | 10.09.24 | 11.09 |
| 2 | Галина ШЕЛЕПАЛО., к.фіз-мат.н., доц. каф. ЗІ | 16.09.24 | 22.09 |
| 3 | Галина ШЕЛЕПАЛО., к.фіз-мат.н., доц. каф. ЗІ | 23.09.24 | 2.11 |
| 4 | Ольга РАТУШНЯК. к.т.н. доц. каф. ЕПВМ | 11.11.24 | 17.11 |

7) Дата видачі завдання 1 вересня 2024 року

КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів бакалаврської кваліфікаційної роботи | Строк виконання етапів роботи | Примітка |
|---|---|---|---|
| 1 | Аналіз завдання. Вступ | 01.09.2024 - 10.09.2024 | |
| 2 | Аналіз літературних джерел за напрямком магістерської кваліфікаційної роботи | 10.09.2024 – 15.09.2024 | |
| 3 | Вибір методів дослідження | 16.09.2024 – 22.09.2024 | |
| 4 | Виконання розрахунків та отримання результатів | 23.09.2024 – 02.11.2024 | |
| 5 | Аналіз та опис в розділах досліджень та результатів | 03.11.2024 – 10.11.2024 | |
| 6 | Розробка економічного розділу | 11.11.2024 – 17.11.2024 | |
| 7 | Аналіз виконання роботи висновки | 18.11.2024 – 24.11.2024 | |
| 8 | Оформлення пояснювальної записки | 25.11.2024 – 30.11.2024 | |
| 9 | Попередній захист та доопрацювання МКР | 28.11.2024 – 01.12.2024 | |
| 10 | Перевірка МКР на наявність плагіату | 02.12.2024 – 16.12.2024 | |
| 11 | Представлення МКР до захисту | 13.12.2024 – 16.12.2024 | |
| 12 | Захист МКР | 17.12.2024 – 20.12.2024 | |

Студент _____ Олег СЕМЕНЮК

Керівник роботи _____ Галина ШЕЛЕПАЛО

# АНОТАЦІЯ

УДК 004.056.55

Семенюк О. Метод криптоаналізу на основі часткових латинських квадратів. Магістерська кваліфікаційна робота зі спеціальності 125 – Кібербезпека та захист інформації, освітня програма – Безпека інформаційних і комунікаційних систем. Вінниця: ВНТУ, 2024. 85 с.

Укр. мовою. Бібліогр. 23 назв; рис.: 15; табл.: 41.

Магістерська кваліфікаційна робота присвячена розробці методу для зменшення апаратних витрат на реалізацію латинських квадратів шляхом використання частково заповнених латинських квадратів. Підготовлено науково-дослідне обґрунтування доцільності досліджень. У роботі здійснено аналіз відомих типів латинських квадратів, відомі методи заповнення часткових латинських квадратів. Розроблено математичну модель процесу заповнення. Розроблено метод побудови латинських квадратів на основі їх часткових заповнень.

Ілюстративна частина складається з плакатів з демонстрацією результатів проведених досліджень.

В економічному розділі оцінено витрати на науково-дослідну роботу.

*Ключові слова:* криптоаналіз, латинський квадрат, частковий латинський квадрат, трансверсаль, секретний ключ, алгоритм.

# ABSTRACT

Semeniuk O. Cryptanalysis method based on partial Latin squares. Master's qualification work in speciality 125 - Cybersecurity and information protection, educational programme - Security of information and communication systems. Vinnytsia: VNTU, 2024. 85 c.

In Ukrainian. Bibliography: 23 items; pictures: 15; tables: 41.

The master's qualification work is devoted to the development of a method for reducing hardware costs for the implementation of Latin squares by using partially filled Latin squares. Feasibility justification for the research has been conducted. The paper analyses the known types of Latin squares and the known methods of filling partial Latin squares. A mathematical model of the filling process is developed. A method for constructing Latin squares based on their partial fillings has been developed.

The illustrative part consists of posters demonstrating the results of the research.

The economic section estimates the costs of research work.



*Keywords*: cryptanalysis, Latin square, partial Latin square, transversal, secret key, algorithm.

# ЗМІСТ

# ВСТУП

У сучасному світі захист інформації посідає важливе місце. З розвитком технологій людство почало зберігати великі масиви даних у електронному вигляді. Однак постало важливе питання в захисті цієї інформації від несанкціонованого доступу. Саме тому почали використовувати методи шифрування або криптозахисту для збереження та захисту інформації.

З розвитком інформаційних технологій та криптографії важливим є забезпечення ефективного захисту даних при одночасному зниженні апаратних витрат. Одним із перспективних підходів є використання латинських квадратів у криптографічних алгоритмах, які забезпечують високий рівень стійкості до атак. Однак, реалізація повністю заповнених латинських квадратів потребує значних обчислювальних ресурсів, що ускладнює їх використання у пристроях із обмеженими обчислювальними можливостями.

Застосування частково заповнених латинських квадратів дозволяє зменшити обчислювальні витрати та апаратну складність, зберігаючи при цьому криптографічну стійкість алгоритмів. Це є особливо важливим у контексті сучасних вимог до оптимізації ресурсів і забезпечення безпеки інформації. Таким чином, розробка методів, які дозволяють ефективно відновлювати латинські квадрати з частково заповнених квадратів, є актуальним завданням, що відповідає потребам підвищення продуктивності та зменшення енергоспоживання криптографічних систем.

**Метою** роботи є пришвидшення відновлення секретного ключа для зменшення апаратних витрат на реалізацію латинських квадратів, шляхом використання частково заповнених даних.

Для досягнення мети необхідно розв’язати такі завдання:

- проаналізувати відомі типи латинських квадратів;
- проаналізувати відомі методи заповнення часткових латинських квадратів;
- проаналізувати використання латинських квадратів у криптографії

- розробити метод побудови латинських квадратів на основі їх часткових заповнень;

**Об’єкт дослідження** – процес криптоаналізу шифрів, в яких використовуються латинські квадрати.

**Предмет дослідження –** метод криптоаналізу за побудовою латинських квадратів на основі частково заповнених даних.

**Наукова новизна.** Теоретично обґрунтовано можливість відтворення латинських квадратів 3-го та 4-го порядків за їх частковим заповненням, що, на відміну від відомого підходу, забезпечує однозначне відновлення будь-яких латинських квадратів з їх повного набору. Запропоновано метод для однозначного відновлення частково заповнених латинських квадратів 3-го та 4-го порядку, який використовується для шифрування з метою зменшення апаратних витрат.

**Практична цінність** полягає в отримані чіткої кількості можливих варіантів частково заповнених латинських квадратів 3-го та 4-го порядку, для реалізації однозначного заповнення.

Проміжні результати були опубліковані у вигляді тез: «Умови відновлення секретного ключа на відкритих комірках латинського квадрата» [13].

# 1 АНАЛІЗ ТА ОГЛЯД ЛІТЕРАТУРНИХ ДЖЕРЕЛ

## 1.1 Основні поняття та вибір методів дослідження

Латинський квадрат – це квадратна матриця розміру n, в якій кожен рядок і стовпчик є перестановкою елементів кінцевої множини S, що містить n елементів. При цьому кожен елемент з'являється лише один раз у кожному рядку та стовпчику. Приклад такого латинського квадрата наведено нижче [1]:

$$L = \begin{pmatrix} 0 & 1 & \vdots & n-2 & n-1 \\ 1 & 2 & \vdots & n-1 & 0 \\ \vdots & & \ddots & & \vdots \\ n-2 & n-1 & \cdots & n-4 & n-3 \\ n-1 & 0 & \cdots & n-3 & n-2 \end{pmatrix}$$

Якщо маємо множину $S = \{A, B, C\}$, то латинський квадрат розміру 3x3 може мати вигляд. У цьому квадраті кожен елемент з множини $S$ з'являється рівно один раз у кожному рядку та стовпчику.

$$L = \begin{pmatrix} A & C & B \\ C & B & A \\ B & A & C \end{pmatrix}$$

Даний латинський квадрат виражений формулою $L(x, y) = x + y$, де $x$ та $y$ має номер рядка та стовпчику квадрата, $x, y \in \Omega = \{0,1, \dots, n-1\}$, і під складанням мається на увазі складання по модулю n (можна сказати, що формула $L(x, y) = x + y$) задає латинський квадрат над абелевой групою $Z_n$). Довільний латинський квадрат порядку $n$ над групою $Z_n$ задається формулою $L(x, y) = x + y + f(x, y)$, де $f$ – це деяка функція $Z_n * Z_n \to Z_n$ [1].

Зараз у якості множини $M$ зазвичай береться множина натуральних чисел від 1 до n, однак Леонард Ейлер (1707 – 1783) взяв букви латинського алфавіту, звідки й отримали свою назву латинські квадрати.

Врахуємо, що є безліч різних підходів до вивчення і аналізу та формування латинських квадратів, які сходять до Ейлера. Він сформував латинські квадрати з латинських прямокутників. Важливою частиною у вивченні латинських квадратів була робота А. Келлі, у якій він вивів формулу для кількості таких прямокутників з двох рядків. Наступний етап – виведення формули для числа прямокутників з трьох рядків – відбулось у 1953 році .

Формула для розрахунку $L(n)$ латинських квадратів порядку n не виведена. У таблиці 1.1 приведено відома кількість значень $L(n)$ на сьогодні [1]:

Таблиця 1.1 – Число латинських квадратів

| | |
|---|---|
| 2 | |
| 576 | |
| 161280 | Euler (1682) |
| 812851200 | Frolov (1890) |
| 61479419904000 | Sade (1948) |
| 108776032459082956800 | Wells (1967) |
| 5524751496156892842531225600 | Bammel (1975) |
| 9982437658213039871725064756920320000 | Rogoyski (1995) |
| 776966836171770144107444346734230682311065600000 | McKay (2005) |

Найкращі оцінки для L(n) дає наступна формула:

$$\prod_{k=1}^{n}(k!)^{\frac{n}{k}} \leq L(n) \leq \frac{(n!)^{2n}}{n^{n^2}}$$

Для подальшої роботи, нам необхідно обрати метод шифрування, який базується на латинських квадратах. Було обрано потоковий шифр на основі CIP-квазігруп 4-го порядку запропонований авторами Лужецьким В.А., Крайнічук Г.В., Радченко, Пилявець.

Основна ідея алгоритму потокового шифрування полягає в тому, що на кожному етапі накладання гами на інформацію виконується операція, яка вибирається псевдовипадковим чином з певного набору операцій.

Відомо, що кожна бінарна квазігрупова операція має 6 парастрофів головної квазігрупової операції, а саме: головна операція; ліве ділення; праве ділення; комутування; комутування; правого ділення; комутування лівого ділення.

Нехай головна операція зображена рівністю $x \cdot y = z$, тоді парастроф лівого ділення квазігрупової операції полягає у перестановці місцями змінних x і z, що зображується рівністю $z \cdot y = x$.

Для реалізації алгоритму зашифрування можемо взяти парастроф головної операції з набору квазігруп, а для алгоритму розшифрування – відповідний парастроф лівого ділення.

Набір операцій отримано шляхом перетворень над ізотопами групи Клейна для середніх CIP-квазігруп 4-го порядку з функцією оборотності x2 [2].

Бінарні операції, що застосовуються для зашифрування, відтворений такими латинськими квадратами:

| L0 | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 3 | 1 | 2 |
| 1 | 2 | 1 | 3 | 0 |
| 2 | 3 | 0 | 2 | 1 |
| 3 | 1 | 2 | 0 | 3 |

| L1 | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 1 | 2 | 0 | 3 |
| 1 | 3 | 0 | 2 | 1 |
| 2 | 2 | 1 | 3 | 0 |
| 3 | 0 | 3 | 1 | 2 |

| L2 | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 2 | 1 | 3 | 0 |
| 1 | 0 | 3 | 1 | 2 |
| 2 | 1 | 2 | 0 | 3 |
| 3 | 3 | 0 | 2 | 1 |

| L3 | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 3 | 0 | 2 | 1 |
| 1 | 1 | 2 | 0 | 3 |
| 2 | 0 | 3 | 1 | 2 |
| 3 | 2 | 1 | 3 | 0 |

Розшифрування виконується з використанням бінарних операції, що відтворюються такими латинськими квадратами:

| L-10 | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 2 | 3 | 1 |
| 1 | 3 | 1 | 0 | 2 |
| 2 | 1 | 3 | 2 | 0 |
| 3 | 2 | 0 | 1 | 3 |

| L-11 | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 1 | 3 | 2 | 0 |
| 1 | 2 | 0 | 1 | 3 |
| 2 | 0 | 2 | 3 | 1 |
| 3 | 3 | 1 | 0 | 2 |

| L-12 | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 2 | 0 | 1 | 3 |
| 1 | 1 | 3 | 2 | 0 |
| 2 | 3 | 1 | 0 | 2 |
| 3 | 0 | 2 | 3 | 1 |

| L-13 | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 3 | 1 | 0 | 2 |
| 1 | 0 | 2 | 3 | 1 |
| 2 | 2 | 0 | 1 | 3 |
| 3 | 1 | 3 | 2 | 0 |

Для бінарної операції $x \cdot y = z$ змінні і результат подаються як дворозрядний двійковий код, тобто $x = x_1x_2$, $y = y_1y_2$ і $z = z_1z_2$. З урахуванням цього маємо такі логічні функції, що описують бінарні операції:

$$L_0(x_1, x_2, y_1, y_2) = z_1 = y_2\overline{(x_1 \oplus x_2)} + \overline{y}_2(x_1 \oplus x_2);$$

$$L_0(x_1, x_2, y_1, y_2) = z_2 = y_2\overline{(x_1 \oplus y_2)} + \overline{y}_2(x_1 \oplus y_2);$$

$$L_1(x_1, x_2, y_1, y_2) = z_1 = y_2\overline{(x_1 \oplus x_2)} + \overline{y}_2(x_1 \oplus x_2);$$

$$L_1(x_1, x_2, y_1, y_2) = z_2 = y_2(x_1 \oplus y_1) + \overline{y}_2\overline{(x_1 \oplus y_1)};$$

$$L_2(x_1, x_2, y_1, y_2) = z_1 = x_2(x_1 \oplus y_2) + \overline{x}_2\overline{(x_1 \oplus y_2)};$$

$$L_2(x_1, x_2, y_1, y_2) = z_2 = y_2(x_1 \oplus y_1) + \overline{y}_2\overline{(x_1 \oplus y_1)};$$

$$L_3(x_1, x_2, y_1, y_2) = z_1 = x_2(x_1 \oplus y_2) + \overline{x}_2\overline{(x_1 \oplus y_2)};$$

$$L_3(x_1, x_2, y_1, y_2) = z_2 = y_2(x_1 \oplus y_1) + \overline{y}_2\overline{(x_1 \oplus y_1)};$$

$$L_0^{-1}(x_1, x_2, y_1, y_2) = z_1 = x_2\overline{(y_1 \oplus y_2)} + \overline{x}_2(y_1 \oplus y_2);$$

$$L_0^{-1}(x_1, x_2, y_1, y_2) = z_2 = x_2\overline{(x_1 \oplus y_1)} + \overline{x}_2(x_1 \oplus y_1);$$

$$L_1^{-1}(x_1, x_2, y_1, y_2) = z_1 = x_2(y_1 \oplus y_2) + \overline{x}_2\overline{(y_1 \oplus y_2)};$$

$$L_1^{-1}(x_1, x_2, y_1, y_2) = z_2 = x_1(x_2 \oplus y_1) + \overline{x}_1\overline{(x_2 \oplus y_1)};$$

$$L_2^{-1}(x_1, x_2, y_1, y_2) = z_1 = x_2\overline{(y_1 \oplus y_2)} + \overline{x}_2(y_1 \oplus y_2);$$

$$L_2^{-1}(x_1, x_2, y_1, y_2) = z_2 = x_1(x_2 \oplus y_1) + \overline{x}_1\overline{(x_2 \oplus y_1)};$$

$$L_2^{-1}(x_1, x_2, y_1, y_2) = z_1 = x_2(y_1 \oplus y_2) + \overline{x}_2\overline{(y_1 \oplus y_2)};$$

$$L_2^{-1}(x_1, x_2, y_1, y_2) = z_2 = x_1(x_2 \oplus y_1) + \overline{x}_1\overline{(x_2 \oplus y_1)}.$$

Відкрита інформація М подається як послідовність двобітних елементів $M = (m_1, m_2, m_3, \ldots, m_n)$, $m_i \in \{0,1,2,3\}$.

Секретний ключ К має дві 32-розрядні складові: $K = \{K_1, K_2\}$. Перша частина $K_1$ надається як послідовність двобітних елементів $K_1 = (k_1, k_2, k_3, \ldots, k_{16})$, $k_i \in \{0,1,2,3\}$ і застосовується як початок гами.

Гама $G = (g_1, g_2, g_3, \ldots, g_n)$ формується за такими вимогами:

$$g_i = \begin{cases} k_i, \\ m_{i-16}, \end{cases} \text{для } 1 \le i \le 16;$$

$$\text{для } 16 < i \le n.$$

Друга частина $K_2$ є першим станом регістра зсуву з лінійним зворотним зв'язком, який реалізований з використанням твірного поліному $x^{32} + x^7 + x^6 + x^2 + 1$. Цей регістр гарантує генерацію послідовності псевдовипадкових чисел $J = \{j_1, j_2, j_3, \ldots, j_n\}$, $j_i \in \{0,1,2,3\}$, кожен з них є номером використовуваного латинського квадрата.

Зашифроване повідомлення подається як послідовність двобітних елементів $C = (c_1, c_2, c_3, \ldots, c_n)$, $c_i \in \{0,1,2,3\}$.

Алгоритм зашифрування.

1. Створити елемент гами $g_i$.

2. Згенерувати псевдовипадкове число $j_i$.

3. Обчислити елемент зашифрованого повідомлення $c_i$

як результат бінарної операції $L_{j_i}$:

$c_i = L_{j_i}(m_i, g_i)$.

Ці дії виконуються для і від 1 до $n$.

Алгоритм розшифрування.

1. Створити елемент гами $g_i$.

2. Згенерувати псевдовипадкове число $j_i$.

3. Обчислити елемент відкритого повідомлення $m_i$ як

результат бінарної операції $L_{j_i}^{-1}$:

$m_i = L_{j_i}^{-1}(c_i, g_i)$.

Ці дії виконуються для і від 1 до $n$.

Криптографічна стійкість даного алгоритму потокового шифрування реалізовується криптографічною стійкістю гами (секретний ключ $K_1$ і невідомі для зловмисника елементи відкритої інформації) та невизначеною послідовністю потрібних операцій (послідовність псевдовипадкових чисел, що генерується на основі секретного ключа $K_2$).

Апаратна реалізація алгоритму потокового шифрування:

Структурну схему процесора для потокового шифрування наведено на рис.1.1 До неї входять такі структурні елементи [2].

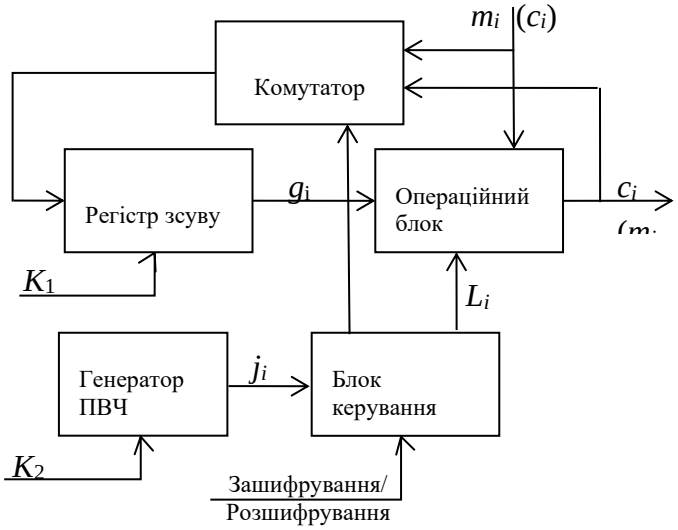



Рисунок. 1.1 – Структурна схема процесора для потокового шифрування

Регістр зсуву гарантує формування елементів гами. Для початку в нього записується код секретного ключа $K_1$, а далі на кожному етапі записується кожен наступний елемент відкритої інформації $m_i$.

Генератор псевдовипадкових чисел (ПВЧ) створений як регістр зсуву з лінійним зворотним зв’язком. Псевдовипадкові числа показані двома двійковими розрядами.

Операційний блок створює показані вище латинські квадрати.

Блок керування гарантує можливість вибору реалізації латинського квадрату залежно від потреби «Зашифрування/Розшифрування» і значення $j_i$.

Комутатор записує у регістр зсуву елементи відкритої інформації $m_i$ або з входу процесора в режимі «Зашифрування», або з виходу операційного блоку в режимі «Розшифрування».

Апаратну складність окремих структурних елементів процесора для потокового шифрування наведено в табл.1.2.

Таблиця 1.2 – Апаратна складність структурних елементів процесора

| Структурний елемент | Складність (GE) |
|---|---|
| Генератор ПВЧ | 178,57 |
| Регістр зсуву | 170,56 |
| Блок керування | 23,29 |
| Комутатор | 5,99 |
| Операційний блок | 103,98 |

Складність визначалась на базі бібліотеки UMCL18G212T3 library [2], яка має базові компоненти технології 0.18 μm виготовлення мікросхем та показує їх складність в умовних одиниць GE (Gate Equivalent).

З таблиці 1.2 виявляється, що апаратна складність створеного процесора складає 482,39 GE або з округленням – 483 GE.

Для порівняння в таблиці 1.3 показано оцінки складності апаратної реалізації відомих [3] і запропонованого алгоритму потокового шифрування.

Таблиця 1.3 – Оцінки апаратної складності реалізації алгоритмів

| Назва алгоритму | Розрядність ключа | Складність(GE) |
|---|---|---|
| Grain | 80/128 | 1294/1857 |
| Fruit-80 | 80 | 960 |
| Plantlet | 80 | 928 |
| LILLE | 80 | 911 |
| Edon-80 | 80/128 | 600/1110 |
| LKRP | 64 | 483 |

Порівняльний аналіз наведених оцінок складності показує, що запропонований алгоритм потокового шифрування на основі CIP-квазігруп 4-го порядку є досить легким в реалізації і забезпечує відповідніть вимогам LW-криптографії (апаратна складність реалізації від 100 до 2000 GE).

Складність створення запропонованого алгоритму потокового шифрування від 1,8 до 3,5 разів менше в порівнянні зі складністю реалізації існуючих алгоритмів потокового шифрування LW-криптографії.

Таким чином можна сказати, що використання CIP-квазігруп 4-го порядку є перспективним методом до побудови потокових шифрів, але існує потреба подальших досліджень.

## 1.2 Огляд літературних джерел

У роботі Нелдера (1977), в дуже короткому повідомленні, поставили запитання про частково заповнені латинські квадрати, яке на перший погляд здається простим, але вимагає детального розгляду. Розглянемо частково заповнені масиви розміром $3 \times 3$, представлені на таблиці 1.4 Бачимо, що кожен масив можна доповнити до єдиного латинського квадрата на трьох символах 0, 1, 2, але якщо будь-який один елемент видалити з будь-якого масиву, цей масив більше не буде єдиним чином доповнений до такого латинського квадрата. Нелдер назвав набір елементів із цими двома властивостями *критичним*

*набором*. Він запитав: для заданого латинського квадрата порядку $n$, яким є розмір (кількість елементів) найменшого критичного набору та найбільшого критичного набору Він позначив ці два числа як $scs(n)$ та $lcs(n)$ відповідно [4].

Таблиця 1.4 – Частково заповнена матриця 3x3

| | | |
|---|---|---|
| 0 | * | * |
| * | * | * |
| * | * | 1 |

| | | |
|---|---|---|
| 0 | 1 | * |
| 1 | * | * |
| * | * | * |

Першим несподіваним відкриттям є те, що критичні набори різних розмірів можуть існувати для одного і того ж латинського квадрата. Друге — це те, що різні латинські квадрати одного порядку $n$ мають критичні набори різних мінімальних розмірів. Ці зауваження ілюструються на Таблицях 1.5 та 1.6 Критичні набори $A$ та $B$ обидва доповнюються єдиним чином до одного і того ж латинського квадрата $L_1$, але мають різні розміри. Критичний набір $C$ доповнюється єдиним чином до латинського квадрата $L_2$. Набір $A$ є найменшим критичним набором для $L_1$, а набір $C$ — найменшим критичним набором для $L_2$, але $C$ має більший розмір (п'ять елементів), ніж $A$ (чотири елементи). Нижче наведено обґрунтування, чому $A$ та $C$ є найменшими.

Таблиця 1.5 – Критичні набори

$$\mathrm{A} = \begin{vmatrix} 0 & 1 & * & * \\ 1 & * & * & * \\ * & * & * & * \\ * & * & * & 2 \end{vmatrix} \quad \mathrm{B} = \begin{vmatrix} 0 & 1 & 2 & * \\ 1 & 2 & * & * \\ 2 & * & * & * \\ * & * & * & * \end{vmatrix} \quad \mathrm{C} = \begin{vmatrix} * & 1 & * & * \\ 1 & * & * & 2 \\ * & * & 0 & * \\ 3 & * & * & * \end{vmatrix}$$

Таблиця 1.6 – Заповнення на базі критичних наборів

$$L_1 = \begin{vmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \end{vmatrix} \quad L_2 = \begin{vmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{vmatrix} \quad L_3 = \begin{vmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 1 & 0 \\ 3 & 2 & 0 & 1 \end{vmatrix}$$

Однак найменший критичний набір для квадрата $L_3$ (який відрізняється від $L_2$ лише однією інтеркалати) містить лише чотири елементи.

**Інтеркалат** — це латинська обмінна операція найменшого можливого розміру.

Насправді латинські квадрати $L_1$ та $L_3$ є ізотопами циклічної групи $Z_4$ (і тому мають критичні набори однакового розміру), тоді як $L_2$ ізотопний 2-групі $Z_2 \times Z_2$.

Тепер пояснимо, чому $A$ і $C$ є найменшими критичними наборами для $L_1$ і $L_2$, відповідно. У будь-якій таблиці Келі циклічної групи кожен елемент належить рівно одній інтеркалаті. Усього є чотири інтеркалати, і жоден з них не має спільних клітин. Якщо клітини критичного набору не включають принаймні одну клітину з кожної інтеркалати, можна отримати два варіанти завершення цього набору: один до $L_1$ і один до латинського квадрата, який відрізняється від $L_1$ тим, що два різні символи в "непокритій" інтеркалаті поміняні місцями. Оскільки є чотири неперекриваючі інтеркалати, в критичному наборі має бути принаймні чотири клітини.

Латинський квадрат $L_2$ має інший порядок інтеркалат. Кожна клітина входить у три різні інтеркалати $L_2$. Оскільки всього є 16 клітин, але кожен інтеркалат містить чотири клітини, загальна кількість інтеркалат становить $(16 \times 3)/4 = 12$. Клітини критичного набору мають містити принаймні одну клітину з кожної з цих дванадцяти інтеркалат. Це можна забезпечити за допомогою трансверсалі квадрата. Клітини $L_2$, показані жирним шрифтом на Таблиці 1.5, формують таку трансверсаль. Однак ці клітини самі по собі (або будь-яка інша трансверсаль) не є достатніми для унікального завершення $L_2$.

**Рядковий латинський квадрат** — це квадратна матриця порядку n, кожен рядок якої є перестановкою тих самих n елементів. Аналогічно визначається стовпцевий латинський квадрат [5].

Ці поняття пов'язані з латинським прямокутником тим фактом, що об'єднання латинських прямокутників, кожен з яких має n стовпців (і таке, що загальна кількість рядків дорівнює n, очевидно, є рядковим латинським квадратом. Однак рядковий латинський квадрат не обов'язково можна розбити на латинські прямокутники, крім як у тривіальний спосіб.

Зрозуміло, що квадратна матриця, яка є одночасно і рядковим, і стовпцевим латинським квадратом, є латинським квадратом.

Також було розглянуто поняття симетричної криптографії.

Симетрична криптографія використовує один і той же ключ для шифрування та дешифрування, тому необхідно мати якийсь механізм для збереження цих ключів у секреті. Цей тип криптографії називається симетричним, оскільки учасники комунікації мають один і той же секретний ключ. Основна перевага симетричної криптографії над асиметричною полягає в тому, що вона значно швидша. Симетричну криптографію можна поділити на блочні та стрімінгові шифри.

Блочні шифри приймають на вхід блок відкритого тексту та ключ, а вихідним результатом є блок шифротексту такого ж розміру, як і відкритий текст. Стрімінгові шифри створюють довільно довгий потік ключового матеріалу, який комбінується з відкритим текстом біт за бітом. У стрімінговому шифрі вихід створюється на основі прихованого внутрішнього стану, який змінюється в процесі роботи шифру [6].

Проектування блочних шифрів спирається на два основні принципи: плутанина та дифузія. Плутанина означає, що кожна цифра шифротексту повинна залежати від кількох частин ключа. Дифузія означає, що якщо змінюється один біт відкритого тексту, то статистично половина бітів у шифротексті повинна змінитися, і навпаки.

S-блок або замісний блок є базовим компонентом алгоритмів симетричного ключа. Основною метою використання S-блоку є внесення плутанини. Властивість нелінійності S-блоків є одним з найважливіших криптографічних критеріїв, оскільки криптографічний алгоритм має бути стійким до лінійного криптоаналізу. S-блок ($n$, $m$) складається з $n$ вхідних змінних і $m$ вихідних змінних. Ці $m$ виходів можна розглядати як $m$ булевих функцій. Якщо нелінійність булевої функції дорівнює максимальному значенню, то вона називається згинальною функцією. Нелінійна межа, показана у формулі

(1.1), називається межею покриття і є строгим для згинальних булевих функцій[7].

$$N_f \leq 2^{n-1} - 2^{\frac{n}{2}-1} \quad (1.1)$$

Іншими критеріями, які враховуються в булевих або векторних функціях, є алгебраїчна ступінь, збалансованість, стійкість, алгебраїчна імунітет та інші. Якщо всі критерії використовуються одночасно, то проблема пошуку найкращої булевої функції або S-блоку є багатокритеріальною задачею.

### 1.3 Криптографічні примітиви на основі латинських квадратів

Класична схема Ель-Гамаля є криптосистемою з відкритим ключем, робота якої ґрунтується на складності обчислення дискретних логарифмів і формулюється мовою теорії чисел з використанням множення за модулем простого числа. Перед відправленням повідомлення відкритим каналом зв'язку від $A$ до $B$, перший учасник шифрує повідомлення, а другий, отримавши зашифроване повідомлення, розшифровує його. Передбачається, що канал зв'язку, який використовується для пересилання, доступний для прослуховування третіми особами. Тобто у відправника і отримувача є противник $E$, який здатний перехопити передане повідомлення. Відправника прийнято називати Бобом, отримувача — Алісою, а зловмисника — Євою. Вважається, що Єва має у своєму розпорядженні потужне обчислювальне обладнання і володіє методами криптоаналізу. Аліса та Боб, природно, зацікавлені в тому, щоб їхні повідомлення були незрозумілі Єві, і для цього використовують спеціальні шифри.

Кожна спроба зламати шифр називається атакою на шифр. У криптографії прийнято вважати, що противник може знати алгоритм шифрування, природу переданих повідомлень і перехоплений зашифрований текст, але не маючи секретного ключа, він не може зламати цей шифротекст. Основне завдання розробників сучасних криптосистем — створити шифр, максимально неуразливий до всіх відомих типів атак на відомий або обраний текст.

*Схема Ель-Гамаля*

Припустимо, є абоненти $A$ та $B$, які хочуть передавати зашифровані повідомлення один одному. Розглянемо схему, запропоновану Тахером Ель-Гамалем, яка вирішує цю проблему, використовуючи лише одну передачу повідомлень. Ця схема працює у три етапи: генерації ключів, шифрування та дешифрування.

*Етап 1. Генерація ключів.*

1) Обирається випадкове просте число $p$;

2) Обирається ціле число $g$ — первісний корінь $p$ (важливим моментом є те, що вже складені таблиці для мінімальних первісних коренів простих чисел, які можна використати, що дозволяє легко пройти цей етап без трудомістких обчислень);

Числа $p$ та $g$ передаються абонентам у відкритому вигляді.

3) Кожен абонент обирає свій секретний ключ $c_A$ і $c_B$, які задовольняють умови $1 < c_A < p - 1.1$, $1 < c_B < p - 1$, де числа $c_i$ і $p - 1$ є взаємно простими;

4) Кожен абонент, використовуючи свій секретний ключ, обчислює відповідний відкритий ключ:

$d_A \equiv g^{C_A} (mod\ p)$ та $d_B \equiv g^{C_B} (mod\ p)$.

Нехай $B$ відправляє повідомлення $m$, представлене як число $m < p$, абоненту $A$.

*Етап 2. Шифрування.*

Абонент $B$ генерує випадкове число $k$ — це сесійний ключ, $1 \leq k \leq p - 2$, при цьому $k$ і $p - 1$ є взаємно простими. Обчислюється пара чисел $(r, e)$ для передачі абоненту $A$ :$r \equiv g^k (mod\ p), e \equiv m \cdot d_B^k (mod\ p)$.

*Етап 3. Дешифрування.*

Абонент $A$, отримавши пару $(r, e)$ і знаючи свій секретний ключ $c_A$, обчислює [8]:

$$m' \equiv e \cdot r^{p-1-C_A} mod\ p).$$

Таким чином, абонент $A$ отримає повідомлення $m' = m$.

*Приклад 1.1.*

Розглянемо передачу повідомлення $m = 506$ від $B$ до $A$.

*Етап 1. Генерація ключів*

1) Візьмемо випадкове просте число $p = 719$.

2) Обираємо ціле число $g = 11$ — найменший первісний корінь 719.

3) Потім абоненти вибирають свої секретні ключі. Нехай абонент $B$ обирає секретне число $c_B = 19$, а абонент $A$ обирає секретне число $c_A = 23$.

4) Кожен абонент обчислює відповідний відкритий ключ за формулою (1):

$$dA \equiv 1123\ (mod\ 719) = 711,$$

$$dB \equiv 1119\ (mod\ 719) = 449.$$

*Етап 2. Шифрування*

Абонент $B$ випадково обирає число $k = 97$ і обчислює пару чисел $(r, e)$ за формулами (2) і (3) для передачі абоненту $A$:

$$r \equiv 1197\ (mod\ 719) = 371,$$

$$e \equiv 506 \cdot 71197(\ mod\ 719) = 506 \cdot 19\ (mod\ 719) = 267.$$

Тепер $B$ відправляє зашифроване повідомлення у вигляді пари чисел $(371, 267)$.

*Етап 3. Дешифрування*

$A$, отримавши пару $(371, 267)$ і знаючи свій секретний ключ $c_A$, обчислює:

$$m' \equiv 267 \cdot 371719 - 1 - 23\ (mod\ 719) = 267 \cdot 371695\ (mod\ 719)$$

$$= 267 \cdot 492\ (mod\ 719) = 506.$$

Отже, $A$ зміг розшифрувати передане повідомлення $m = 506$.

Противник, знаючи $p$, $g$, $dA$, $r$ і $e$, не може обчислити $m$. Лише $A$ може розшифрувати повідомлення за допомогою свого секретного ключа $cA$, відомого тільки йому.

Схему Ель-Гамаля через випадковий вибір числа $k$ називають схемою імовірнісного шифрування або шифром багатозначної заміни. Імовірнісний

характер шифрування є її перевагою. У схемі Ель-Гамаля необхідно використовувати різні значення випадкової величини k для шифрування різних повідомлень. Недоліком схеми є подвоєння довжини зашифрованого тексту порівняно з початковим текстом.

Цю схему можна переформулювати в термінах кільця залишків за модулем $p$ або, що те ж саме, мовою поля Галуа $GF(p)$. Нехай $(Zp, +)$ — циклічна група залишків великого простого порядку щодо додавання залишків, а $a$ — генератор групи.

*Приклад 1.2.* Шифрування на основі схеми Ель-Гамаля

*1.Генерація ключів:*

- Аліса обирає $p = 719,\ a = 11,\ m = 23$.

- Далі вона обчислює $a^m\ mod\ p$:

$$a^m = 11^{23}\ (mod\ 719) = 711.$$

- Відкритий ключ Аліси: $(p, a^m) = (719, 711)$.

- Закритий ключ Аліси: $m = 23$.

*2. Шифрування:*

- Боб хоче відправити Алісі повідомлення $S = 506$.

- Він обирає випадкове число $r = 19$ і шифрує $S$ як $a^r, a^{mr} \cdot S$.

- Обчислення Боба:

$a^r = 11^{19}\ (mod\ 719) = 449$,

$a^{mr} \cdot S = 11437 \cdot 506\ (mod\ 719) = 510 \cdot 506\ (mod\ 719) = 658.$

- Боб надсилає зашифроване повідомлення $(449, 658)$.

*3. Розшифрування:*

- Аліса отримує повідомлення $(449, 658)$ і, використовуючи свій закритий ключ $m = 23$, розшифровує його.

- Вона обчислює $a^{-mr} mod\ p$:

$449^{695}\ mod\ 719 = 86$ і далі:

$86 \cdot 658\ \backslash mod\ 719 = 506$, що відповідає початковому повідомленню $S$.

*Аналог схеми Ель-Гамаля на основі алгоритму Марковського*

*1. Генерація ключів:*

- Нехай $(Q, f)$ — бінарна квазігрупа, а$T = (\alpha, \beta, \gamma)$ — її ізотопія.

- Відкритий ключ Аліси: $(Q, f), T, T(m, n, k) = (\alpha^m, \beta^n, \gamma^k)$, де $m, n, k \in N$.

- Закритий ключ Аліси: $(m, n, k)$.

*2. Шифрування:*

- Боб хоче відправити повідомлення $b \in (Q, f)$.

- Він обирає випадкові числа $r, s, t \in N$ і обчислює $T(r, s, t)$ і $T(mr, ns, kt)$.

- Зашифроване повідомлення має вигляд: $(T(r, s, t), T(mr, ns, kt) \cdot b)$.

- Для шифрування Боб використовує відомий Алісі алгоритм Марковського.

*3. Розшифрування:*

- Аліса, знаючи $m, n, k$ і отримавши зашифроване повідомлення $(T(r, s, t), T(mr, ns, kt) \cdot b)$, обчислює $T(mr, ns, kt)^{-1}$ за допомогою $T(r, s, t)$.
- Потім вона обчислює $b$.

*Приклад 1.3*

Нехай $(Q, f)$ бінарна квазігруппа, яка задається таблицею 1.4:

Таблиця 1.8 – Бінарна квазігрупа

| ° | **1** | **2** | **3** | **4** | **5** |
|---|---|---|---|---|---|
| **1** | 1 | 5 | 3 | 4 | 2 |
| **2** | 4 | 3 | 1 | 2 | 5 |
| **3** | 3 | 1 | 2 | 5 | 4 |
| **4** | 2 | 4 | 5 | 3 | 1 |
| **5** | 5 | 2 | 4 | 1 | 3 |

$T = (\alpha, \beta, \gamma)$ її ізотопія, де $\alpha = (1\ 4\ 3)(2\ 5)$, $\beta = (5\ 3\ 2)(1\ 4)$ і $\gamma = (1\ 4\ 5\ 2\ 3)$.

Для $\gamma$ ми отримуємо зворотню підстановку $\gamma^{-1}$вигляду $\gamma^{-1} = (3\ 2\ 5\ 4\ 1)$.

Для ізотопії $T = (\alpha, \beta, \gamma)$ отримаємо таблицю 1.5:

Таблиця 1.9 – Ізотопія для $T = (\alpha, \beta, \gamma)$

| $\alpha°$ | **1** | **2** | **3** | **4** | **5** | | $\beta°$ | **1** | **2** | **3** | **4** | **5** | | $\gamma°$ | **1** | **2** | **3** | **4** | **5** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **1** | 2 | 4 | 5 | 3 | 1 | | **1** | 3 | 1 | 4 | 2 | 5 | | **1** | 1 | 4 | 5 | 3 | 2 |
| **2** | 5 | 2 | 4 | 1 | 3 | | **2** | 1 | 3 | 2 | 5 | 4 | | **2** | 4 | 1 | 3 | 2 | 5 |
| **3** | 1 | 5 | 3 | 4 | 2 | | **3** | 4 | 2 | 5 | 1 | 3 | | **3** | 5 | 3 | 2 | 4 | 1 |
| **4** | 3 | 1 | 2 | 5 | 4 | | **4** | 5 | 4 | 1 | 3 | 2 | | **4** | 2 | 5 | 4 | 1 | 3 |
| **5** | 4 | 3 | 1 | 2 | 5 | | **5** | 2 | 5 | 3 | 4 | 1 | | **5** | 3 | 2 | 1 | 5 | 4 |

*Етап 1. Генерація ключів.* Ключі Аліси: секретний ключ: m=5, n=5, k=3 і відкритий ключ це: $(Q, f), T, T^{(5,5,3)} = (\alpha^5, \beta^5, \gamma^5)$, де $\alpha^5 = (1\ 3\ 4)(5\ 2)$; $\beta^5 = (1\ 4)(2\ 3\ 5);, \gamma^5 = (1\ 5\ 3\ 4\ 2)$ та алгоритм Марковського.

*Етап 2. Шифрування.*

Щоб надіслати повідомлення $b = 221543353$, Боб знає $T = (\alpha, \beta, \gamma)$:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix};\ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{pmatrix};\ \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix}$$

вираховуємо $T^{(r,s,t)}$ для випадкових $r = 2, s = 3, t = 4$ $T^{(2,3,4)}$:

$$\alpha^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix};\ \beta^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 1 & 5 \end{pmatrix};\ \gamma^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}$$

Маємо $T^{(2,3,4)}$: $\alpha^2 = (1\ 3\ 4)$; $\beta^3 = (1\ 4)$; $\gamma^4 = (1\ 3\ 2\ 5\ 4)$

Після цього вираховуємо $T^{(mr,ns,kt)}$використовуючи відкритий ключ:

$$T^{(m,n,k)} = (\alpha^m, \beta^n, \gamma^k) = (\alpha^*, \beta^*, \gamma^*):$$

$$\alpha^* = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix};\ \beta^* = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix};\ \gamma^* = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 3 & 1 \end{pmatrix}$$

І при піднесені до степеня відповідні перестановки $r = 2, s = 3, t = 4$ маємо:

$$(\alpha^*)^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}; (\beta^*)^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix}; (\gamma^*)^4 =$$

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

$\alpha^{2m} = (1\ 4\ 3);\ \beta^{3n} = (1\ 4);\ \gamma^{4k} = (1\ 5\ 3\ 4\ 2),\ (\gamma^{4k})^{-1} = (1\ 2\ 3\ 4\ 5)$

В результаті використання нової ізотопії $T^{(2m,3n,4k)}$до квазігрупи $(Q, f)$маємо:

Таблиця 1.10 – Ізотопія $T^{(2m,3n,4k)}$

| $\alpha^{2m}\circ$ | **1** | **2** | **3** | **4** | **5** | | $\beta^{3n}\circ$ | **1** | **2** | **3** | **4** | **5** | | $(\gamma^{4k})^{-1}\circ$ | **1** | **2** | **3** | **4** | **5** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **1** | 2 | 4 | 5 | 3 | 1 | | **1** | 3 | 4 | 5 | 2 | 1 | | **1** | 5 | 3 | 1 | 4 | 2 |
| **2** | 4 | 3 | 1 | 2 | 5 | | **2** | 2 | 3 | 1 | 4 | 5 | | **2** | 4 | 5 | 2 | 3 | 1 |
| **3** | 1 | 5 | 3 | 4 | 2 | | **3** | 4 | 5 | 3 | 1 | 2 | | **3** | 3 | 1 | 5 | 2 | 4 |
| **4** | 3 | 1 | 2 | 5 | 4 | | **4** | 5 | 1 | 2 | 3 | 4 | | **4** | 1 | 2 | 4 | 5 | 3 |
| **5** | 5 | 2 | 4 | 1 | 3 | | **5** | 1 | 2 | 4 | 5 | 3 | | **5** | 2 | 4 | 3 | 1 | 5 |

Щоб отримати $(T^{(mr,ns,kt)}(Q, f)b)$, Боб використовує алгоритм Марковського відомий Алісі, знаючи значення лідера $l = 1$. Тоді шифротекст для повідомлення $b = 221543353$ буде мати вигляд:

$$v_1 = 1 \circ 2 = 3,$$
$$v_2 = 3 \circ 2 = 1,$$
$$v_3 = 1 \circ 1 = 5,$$
$$v_4 = 5 \circ 5 = 5,$$
$$v_5 = 5 \circ 4 = 1,$$
$$v_6 = 1 \circ 3 = 1,$$
$$v_7 = 1 \circ 3 = 1,$$
$$v_8 = 1 \circ 5 = 2,$$
$$v_9 = 2 \circ 3 = 2,$$

В результаті маємо шифротекст вигляду: $b` = 315511122$.

*Етап 3. Розшифрування.*

Аліса знаючи $m = 5, n = 5, k = 3$ отримав ізотопію $T^{(r,s,t)}$та шифротекст $(T^{(mr,ns,kt)}(Q, f)b = 315511122$, спочатку порахує ізотопію $T^{(mr,ns,kt)}$ використовуючи $T^{(r,s,t)} = T^{(**,**,**)}$:

$$\alpha^{**} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix};\ \beta^{**} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 1 & 5 \end{pmatrix};\ \gamma^{**} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}.$$

Вона розраховує $T^{(mr,ns,kt)}$:

$$(\alpha^{**})^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix}; (\beta^{**})^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 1 & 5 \end{pmatrix}; (\gamma^{**})^3 =$$

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

В результаті вона отримує таку саму таблицю Келі. Для $(\gamma^{4k})^{-1}$ будує парастроф (23), який використовується в алгоритмі Марковського для розшифрування.

Таблиця 1.11 – Ключ для розшифрування

| \ | **1** | **2** | **3** | **4** | **5** |
|---|---|---|---|---|---|
| **1** | 3 | 5 | 2 | 4 | 1 |
| **2** | 5 | 3 | 4 | 1 | 2 |
| **3** | 2 | 4 | 1 | 5 | 3 |
| **4** | 1 | 2 | 5 | 3 | 4 |
| **5** | 4 | 1 | 3 | 2 | 5 |

І використовуючи таблицю 1.4 для $b` = 315511122$ відновлюємо $b$:

$$u = 1\backslash 3 = 2,$$
$$u_2 = 3\backslash 1 = 2,$$
$$u_3 = 1\backslash 5 = 1,$$
$$u_4 = 5\backslash 5 = 5,$$
$$u_5 = 5\backslash 1 = 4,$$
$$u_6 = 1\backslash 1 = 3,$$
$$u_7 = 1\backslash 1 = 3,$$
$$u_8 = 1\backslash 2 = 5,$$
$$u_9 = 2\backslash 2 = 3,$$

В результаті вихідний текст був відновлений $b = 221543353$.

У цьому алгоритмі замість ізотопії [6] можна використовувати ізострофію. Замість бінарних квазигруп можна застосовувати лівосторонні і правосторонні квазигрупи або $n$-арні $n > 2$ квазигрупи [7; 8]. Як наслідок, замість алгоритму

Марковського будуть використані його узагальнені алгоритми для відповідних квазигруп. Серед усіх можливих модифікацій слід обрати варіант, найбільш стійкий до всіх відомих на даний момент видів атак.

# 2 АНАЛІЗ ТА ВИЗНАЧЕННЯ СЕКРЕТНОГО КЛЮЧА

## 2.1 Аналіз визначення умов відкритих комірок секретного ключа на основі латинських квадратів 3-го порядку

Для того, щоб реалізувати поставлену задачу встановлення криптографічного аналізу шифрів на основі квазігруп, в яких секретним ключем є латинські квадрати необхідно встановити мінімальну кількість відкритих комірок та їх найменшу кількість значень кожного латинського квадрата 2-го та 3-го порядку.

Нехай маємо $\mathbb{Z}_m: -\{Z_m; +; \cdot\}$, де $Z_m = \{0; 1; \dots m-1\}$ – кільце лишків за модулем $m$. Наприклад $Z_3 = \{0; 1; 2\}$.

Частково заповнений латинський квадрат - $\mathcal{L}$ називають латинським, якщо в кожному рядку і в кожному стовпці всі елементи різні [10].

Якщо в результаті заповнення всіх порожніх клітинок часткового латинського квадрату $\mathcal{L}$ отримуємо латинський квадрат, то таке заповнення називають латинським. В цьому випадку кажуть, що квадрат $\mathcal{L}$ має латинське заповнення.

Нормалізованим називають латинський квадрат у якому перший рядок та перший стовпець має розташування комірок у лексико-графічному порядку.

Розглянемо латинський квадрат $\mathcal{L}$ 2-го порядку та визначимо всі діагоналі та трансверсалі

Діагоналлю квадрату називають максимальну сукупність $m$ комірок взятих з різних рядків та різних стовпців.

Транверсалль – це сукупність клітинок, взятих з різних рядків і різних стовпців, що містять попарно різні елементи [11].

Іншими словами трансверсаль – це діагональ в якої всі елементи різні.

Нехай маємо латинський квадрат $\mathcal{L}$ 2-го порядку який записано у вигляді таблиці Келі (табл. 2.1). де елементи $k_{ij}$ – це матричні індекси відповідного рядка $i$ та відповідного стовпця $j$, на перетині яких знаходиться елемент $k$.

Таблиця 2.1 – Латинський квадрат 2-го порядку загального вигляду

| | 0 | 1 |
|---|---|---|
| 0 | $k_{00}$ | $k_{01}$ |
| 1 | $k_{10}$ | $k_{11}$ |

Для визначення діагоналі, нехай зафіксуємо $k_{00}$, тоді другий елемент визначається автоматично

$$\{k_{00}; k_{11}\} \tag{2.1}$$

Аналогічним чином, зафіксувавши $k_{01}$, другий елемент визначається автоматично

$$\{k_{01}; k_{10}\} \tag{2.2}$$

Отже зробимо висновок, що в латинських квадратах другого порядку маємо лише 2 діагоналі.

Нехай маємо заповнений нормалізований латинський квадрат 2-го порядку (табл. 2.2) для визначення чи є серед визначених діагоналей трансверсалі

Таблиця 2.2 – Нормалізований латинський квадрат 2-го порядку

| | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

При перевірці $\{k_{00}; k_{11}\} \longrightarrow \{0; 0\}$ та $\{k_{01}; k_{10}\} \longrightarrow \{1; 1\}$, маємо, що в латинських квадратах 2-го порядку не існує трансверсалі, але для однозначного заповнення достатньо мати будь яку з двох його діагоналей.

**Лема 1.** Існує точно три трансверсалі для нормалізованого латинського квадрату 3-го порядку[13].

**Доведення.** Нехай маємо латинський квадрат $\mathcal{L}$ 3-го порядку записаний у вигляді квадратної таблиці 2.3, де елементи $k_{ij}$ – це матричні індекси відповідного рядка $i$ та відповідного стовпця $j$, на перетині яких знаходиться елемент $k$.

Таблиця 2.3 – Латинський квадрат 3-го порядку загального вигляду

| | 0 | 1 | 2 |
|---|---|---|---|
| 0 | $k_{00}$ | $k_{01}$ | $k_{02}$ |
| 1 | $k_{10}$ | $k_{11}$ | $k_{12}$ |
| 2 | $k_{20}$ | $k_{21}$ | $k_{22}$ |

Визначимо всі можливі множини діагоналей та які з діагоналей є трансверсалі.

Нехай зафіксуємо перший елемент $k_{00}$, тоді другий елемент маємо право обирати починаючи з 2-го рядка та з 2-го стовпця. Обираємо другий елемент з множини $\{k_{11}; k_{12}\}$. Нехай другий елемент $k_{11}$, тоді третій елемент визначається однозначно.

$$\{k_{00}; k_{11}; k_{22}\} \tag{2.3}$$

Аналогічним чином, якщо другий елемент $k_{12}$, маємо :

$$\{k_{00}; k_{12}; k_{21}\} \tag{2.4}$$

Нехай зафіксуємо перший елемент $k_{01}$, тоді другий елемент маємо право обирати починаючи з 2-го рядка та за виключенням 2-го стовпця. Обираємо другий елемент з множини $\{k_{10}; k_{12}\}$. Нехай другий елемент $k_{10}$, тоді третій елемент визначається однозначно.

$$\{k_{01}; k_{10}; k_{22}\} \tag{2.5}$$

Аналогічним чином, якщо другий елемент $k_{12}$, маємо :

$$\{k_{01}; k_{12}; k_{20}\} \tag{2.6}$$

Нехай зафіксуємо перший елемент $k_{02}$, тоді другий елемент маємо право обирати починаючи з 2-го рядка та за виключенням 3-го стовпця. Обираємо другий елемент з множини $\{k_{10}; k_{11}\}$. Нехай другий елемент $k_{10}$, тоді третій елемент визначається однозначно.

$$\{k_{02}; k_{10}; k_{21}\} \tag{2.7}$$

Аналогічним чином, якщо другий елемент $k_{11}$, маємо :

$$\{k_{02}; k_{11}; k_{20}\} \tag{2.8}$$

Розглянемо заповнений нормалізований латинський квадрат 3-го, для визначення трансверсалей, тоді маємо (табл. 2.4)

Таблиця 2.4 – Заповнений нормалізований латинський квадрат 3-го порядку

| | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

Нехай фіксуємо перший елемент $k_{00} = 0$, тоді другий елемент маємо право обирати починаючи з 2-го рядка та за виключенням 1-го та 3-го стовпця. Тоді другий та третій елемент обираються однозначно.

$$\{0; 2; 1\}$$

Нехай фіксуємо перший елемент $k_{01} = 1$, тоді другий елемент маємо право обирати починаючи з 2-го рядка та за виключенням 1-го та 2-го стовпця. Тоді другий та третій елемент обираються однозначно.

$$\{1; 0; 2\}$$

Нехай фіксуємо перший елемент $k_{02} = 2$, тоді другий елемент маємо право обирати починаючи з 2-го рядка та за виключенням 2-го та 3-го стовпця. Тоді другий та третій елемент обираються однозначно.

$$\{2; 1; 0\}$$

Отже можна стверджувати, що у нормалізованому латинському квадраті 3-го порядку маємо 3 трансверсалі. ■

Дослідивши латинські квадрати 3-го порядку можна довести такі 4 твердження та виокремити з них відповідні наслідки для застосування .

**Твердження 2.1.1.** *Якщо в частковому латинському квадраті 3-го порядку заповнені 3 комірки, які утворюють трансверсаль, то такий латинський квадрат має однозначне латинське заповнення.*

**Доведення.**

Нехай маємо частковий латинський квадрат (табл. 2.5) у якому заповнено три комірки, наприклад маючи трансверсаль у вигляді множини $\{1; 0; 2\}$, то

латинський квадрат має однозначене латинське доповнення. Дійсно виконуючи доповнення отримаємо що комірки мають такі елементи: $k_{00} = 0, k_{02} = 2, k_{10} = 1, k_{11} = 2, k_{21} = 0, k_{22} = 1$.

Таблиця 2.5 – Частково заповнений латинський квадрат 3-го порядку

| | 0 | 1 | 2 |
|---|---|---|---|
| 0 | | 1 | |
| 1 | | | 0 |
| 2 | 2 | | |

У результаті доповнення дійсно отримаємо латинський квадрат, який відповідає квадрату у таблиці 2.4.■

**Наслідок 2.1.1.** Кількість заповнень трьох комірок латинського квадрату 3-го порядку, які утворюють трансверсаль, всього точно три [13].

**Доведення**. Оскільки трансверсалей згідно Леми 1 всього точно три, то враховуючи Твердження 1, маємо що кількість заповнень комірок точно буде три.

**Твердження 2.1.2.** *Якщо в частковому латинському квадраті заповнені три комірки, які утворюють діагональ одного елемента, то однозначне доповнення латинського квадрату стає можливе коли відомо* ∀ *довільна порожня комірка будь якого іншого елемента.*

**Доведення.** Нехай отримали латинський квадрат у якому діагональ утворена з одного елемента $k_{00} = 0, k_{12} = 0, k_{21} = 0$, (див табл. 2.6)

Таблиця 2.6 – Частково заповнений одним елементом латинський квадрат

| | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | | |
| 1 | | | 0 |
| 2 | | 0 | |

| | 0 | 1 | 2 |
|---|---|---|---|
| 0 | | 1 | |
| 1 | 1 | | |
| 2 | | | 1 |

| | 0 | 1 | 2 |
|---|---|---|---|
| 0 | | | 2 |
| 1 | | 2 | |
| 2 | 2 | | |

тоді, отримавши ще одну довільну комірку нехай $k_{01} = 1$. За такої умови стверджуємо, що латинський квадрат має однозначне доповнення наприклад таблиця 2.4.■

**Наслідок 2.1.2.** Кількість заповнень 4-ьох довільних комірок латинського квадрату 3-го порядку три з яких утворюють діагональ одного елемента, а четвертий довільний елемент, становить точно 18.

**Доведення.** Оскільки всього довільних комірок 9, чотири з яких заповнені, де 3 комірки утворюють діагональ одного елемента, то для вибору 4-го елементу залишається $9 - 3 = 6$ комірок. Оскільки всього є три різних елементів, тому і діагоналей одного елемента теж 3. Маємо загальну кількість $6 \cdot 3 = 18$.

**Твердження 2.1.3.** *Якщо в частковому латинському квадраті заповнені 3 комірки (довільного рядка або стовпця), то однозначне заповнення стає можливе, коли стає відома* $\forall$ *довільна порожня клітинка* $\forall$ *іншого елемента.*

**Доведення.** Нехай отримали латинський квадрат у якому заповнено 3 комірки в один ряд $k_{10} = 1, k_{11} = 2, k_{12} = 0$, (див. табл. 2.7)

Таблиця 2.7 – Частково заповнений довільним рядком чи стовпцем

| | 0 | 1 | 2 |
|---|---|---|---|
| 0 | | | |
| 1 | 1 | 2 | 0 |
| 2 | | | |

| | 0 | 1 | 2 |
|---|---|---|---|
| 0 | | | |
| 1 | | | |
| 2 | 2 | 1 | 0 |

| | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | | | |
| 2 | | | |

| | 0 | 1 | 2 |
|---|---|---|---|
| 0 | | | 2 |
| 1 | | | 0 |
| 2 | | | 1 |

| | 0 | 1 | 2 |
|---|---|---|---|
| 0 | | 1 | |
| 1 | | 2 | |
| 2 | | 0 | |

| | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | | |
| 1 | 1 | | |
| 2 | 2 | | |

тоді, отримавши ще одну довільну комірку нехай $k_{00} = 0$. За такої умови стверджуємо, що латинський квадрат має однозначне доповнення наприклад таблиця 2.4.■

**Наслідок 2.1.3.** Кількість заповнень 4-ьох довільних комірок латинського квадрату 3-го порядку три з яких утворюють заповнений рядок або стовпець, а четвертий довільний елемент, становить точно 36.

**Доведення.** Оскільки всього довільних комірок 9, чотири з яких заповнені, де 3 комірки утворюють заповнений рядок або стовпець, то для вибору 4-го елементу залишається $9 - 3 = 6$ комірок. Оскільки маємо три рядки та три стовпці, то загальна кількість становить $3 + 3 = 6$. Маємо загальну кількість $6 \cdot 6 = 36$.■

**Твердження 2.1.4.** *Якщо в частковому латинському квадраті 3-го порядку відомо довільні три комірки, дві з яких однин і той самий елемент, а одна комірка довільний інший елемент, який не повторюється, то такий латинський квадрат має однозначне латинське доповнення.*

**Доведення.** Нехай отримали частково заповнений латинський квадрат з двома довільними однаковими елементами та одним довільним елементом, який не повторюється. Тоді наприклад взявши латинський квадрат з відомими елементами $k_{00} = 0, k_{01} = 1, k_{12} = 0,$ (див. табл. 2.8). За такої умови стверджуємо, що можна однозначно доповнити латинський квадрат наприклад табл. 2.4.

Таблиця 2.8 – Частково заповнений двома однаковими елементами та один довільний

| | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | |
| 1 | | | 0 |
| 2 | | | |

| | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | |
| 1 | | | |
| 2 | | 0 | |

| | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | | |
| 1 | 1 | | |
| 2 | | 0 | |

| | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | | |
| 1 | 1 | | 0 |
| 2 | | | |

| | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | | |
| 1 | | | |
| 2 | | 0 | 1 |

| | 0 | 1 | 2 |
|---|---|---|---|
| 0 | | | |
| 1 | | | 0 |
| 2 | | 0 | 1 |

| | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | | |
| 1 | | | 0 |
| 2 | | | 1 |

| | 0 | 1 | 2 |
|---|---|---|---|
| 0 | | | |
| 1 | 1 | | 0 |
| 2 | | 0 | |

| | 0 | 1 | 2 |
|---|---|---|---|
| 0 | | 1 | |
| 1 | | | 0 |
| 2 | | 0 | |

Аналогічним чином отримавши будь який з довільних часткових доповнень маючи два однакові елементи та один довільний який не повторюється можна стверджувати про однозначне доповнення.■

**Наслідок 2.1.4.** Кількість заповнень 3-ьох довільних комірок латинського квадрату 3-го порядку, дві з яких однин і той самий елемент, а одна комірка довільний інший елемент, який не повторюється, то таких елемента 54.

**Доведення.** Оскільки частково заповнених латинських квадратів де довільно заповнено дві комірки з однаковими елементами та одна комірка з елементом який не повторюється таких квадратів 9. Скомбінувавши значення комірок, отримали наступну кількість квадратів:

2 нулі та 1 одиниця – 9 розташувань;

2 нулі та 1 двійка – 9 розташувань;

2 одиниці та 1 нуль – 9 розташувань;

2 одиниці та 1 двійка – 9 розташувань;

2 двійки та 1 нуль – 9 розташувань;

2 двійки та 1 одиниця – 9 розташувань.

Обчисливши кількість можливих розташувань частково заповнених латинських квадратів де довільно заповнено дві комірки з однаковими елементами та одна комірка з елементом який не повторюється маємо загальну кількість $6 \cdot 9 = 54$ . ■

Отже, можна стверджувати, що частково заповненні латинські квадрати 3-го порядку мають однозначне заповнення у 111 варіантах мінімальної кількості відомих відкритих комірок.

**Теорема 1.** Оскільки всього існує 12 латинських квадратів 3-го порядку, то мінімальна кількість відновлень секретного ключа за відомими будь-якими 3-ма

чи 4-ма відкритими комірками латинських квадратів 3-го порядку становить 1332 однозначних латинських заповнень.

## 2.2 Аналіз визначення умов відкритих комірок секретного ключа на основі латинських квадратів 4-го порядку

Нехай маємо $\mathbb{Z}_m: -\{Z_m; +; \cdot\}$, де $Z_m = \{0; 1; \dots m-1\}$ – кільце лишків за модулем $m$. Наприклад $Z_4 = \{0; 1; 2; 3\}$.

**Лема 2.** Існує точно 8 трансверсалей для нормалізованого латинського квадрату 4-го порядку ізотопного групі Кляйна**.**

**Доведення.** Розглянемо частково заповнений латинський квадрат $\mathcal{L}$ 4-го порядку, тобто якщо в кожному рядку та стовпці всі елементи різні, наприклад в таблиці 2.8 х позначено часткове заповнення невідомими елементами.

Наприклад, як бачимо з табл. 2.9, множина комірок $a_{00}; a_{13}; a_{21};\ a_{32}$ – визначає одну з можливих діагоналей

Таблиця 2.9 – Частково заповнений латинський квадрат невідомими елементами

| | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | x | | | |
| 1 | | | | x |
| 2 | | x | | |
| 3 | | | x | |

Латинський квадрат (частковий латинський квадрат) порядку $m$ має $m^2$ різних комірок, тобто елементів з різними індексами. Кількість всіх діагоналей латинського квадрату (часткового латинського квадрату) обчислюється як $m!$ [7]. Тому для випадку латинського квадрату (часткового латинського квадрату) порядку $m = 4$, маємо,

$$m! = 4! = 1 \times 2 \times 3 \times 4 = 24.$$

Отже, кількість всіх можливих діагоналей латинського квадрату 4-го порядку існує 24 діагоналі.

Для початку необхідно визначити індекси елементів комірок з яких складається кожна діагональ латинського квадрату.

Нехай латинський квадрат $\mathcal{L}$ 4-го порядку записаний у вигляді квадратної табл. 2.10, де елементи $k_{ij}$ – це матричні індекси відповідного рядка $i$ та відповідного стовпця $j$, на перетині яких знаходиться елемент $k$.

Таблиця 2.10 – Латинський квадрат 4-го порядку загального вигляду

| | | | |
|---|---|---|---|
| $k_{00}$ | $k_{01}$ | $k_{02}$ | $k_{03}$ |
| $k_{10}$ | $k_{11}$ | $k_{12}$ | $k_{13}$ |
| $k_{20}$ | $k_{21}$ | $k_{22}$ | $k_{23}$ |
| $k_{30}$ | $k_{31}$ | $k_{32}$ | $k_{33}$ |

Відповідна квазігрупа (квазігрупова операція) 4-го порядку, яка записана у вигляді таблиці Келі (див табл. 2.11) з визначеною операцією $(*)$.

Таблиця 2.11 – Латинський квадрат 4-го порядку загального вигляду

| $*$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | $k_{00}$ | $k_{01}$ | $k_{02}$ | $k_{03}$ |
| 1 | $k_{10}$ | $k_{11}$ | $k_{12}$ | $k_{13}$ |
| 2 | $k_{20}$ | $k_{21}$ | $k_{22}$ | $k_{23}$ |
| 3 | $k_{30}$ | $k_{31}$ | $k_{32}$ | $k_{33}$ |

Наступний крок це визначення сукупності комірок для кожної діагоналі.

Нехай зафіксуємо перший елемент комірки $k_{00}$, тоді другий елемент маємо право брати лише з 2-го рядка та починаючи з 2-го стовпчика. Вибираємо другий елемент діагоналі з множини $\{k_{11}; k_{12}; k_{13}\}$,тобто третій елемент може бути лише з 3-го рядка та починаючи з 3-го стовпчика, якщо фіксуємо $k_{11}$. Вибираємо третій елемент діагоналі з множини $\{k_{22}; k_{23}\}$, тоді четвертий елемент визначається однозначно. Якщо третій елемент $k_{22}$, то маємо першу сукупність елементів діагоналі:

$$\{k_{00}; k_{11}; k_{22}; k_{33}\} \tag{2.9}$$

Якщо третій елемент $k_{23}$, то маємо другу сукупність елементів діагоналі

$$\{k_{00}; k_{11}; k_{23}; k_{32}\} \quad (2.10)$$

Аналогічним чином визначаються такі сукупності елементів діагоналі, якщо фіксований перший елемент, тобто:

$$\{k_{00}; k_{12}; k_{21}; k_{33}\} \quad (2.11)$$

$$\{k_{00}; k_{12}; k_{23}; k_{31}\} \quad (2.12)$$

$$\{k_{00}; k_{13}; k_{21}; k_{32}\} \quad (2.13)$$

$$\{k_{00}; k_{13}; k_{22}; k_{31}\} \quad (2.14)$$

Нехай зафіксуємо перший елемент комірки $k_{01}$, тоді другий елемент маємо право брати лише з 2-го рядка та за виключенням з 2-го стовпчика. Вибираємо другий елемент діагоналі з множини $\{k_{10}; k_{12}; k_{13}\}$,тобто третій елемент може бути лише з 3-го рядка та з 3-го стовпчика, якщо фіксуємо $k_{10}$. Вибираємо третій елемент діагоналі з множини $\{k_{22}; k_{23}\}$, тоді четвертий елемент визначається однозначно. Якщо третій елемент $k_{22}$, то маємо першу сукупність елементів діагоналі:

$$\{k_{01}; k_{10}; k_{22}; k_{33}\} \quad (2.15)$$

Якщо третій елемент $k_{23}$, то маємо другу сукупність елементів діагоналі

$$\{k_{01}; k_{10}; k_{23}; k_{32}\} \quad (2.16)$$

Аналогічним чином визначаються такі сукупності елементів діагоналі, якщо фіксований перший елемент, тобто:

$$\{k_{01}; k_{12}; k_{20}; k_{33}\} \quad (2.17)$$

$$\{k_{01}; k_{12}; k_{23}; k_{30}\} \quad (2.18)$$

$$\{k_{01}; k_{13}; k_{20}; k_{32}\} \quad (2.19)$$

$$\{k_{01}; k_{13}; k_{22}; k_{30}\} \quad (2.20)$$

Нехай зафіксуємо перший елемент комірки $k_{02}$, тоді другий елемент маємо право брати лише з 2-го рядка та за виключенням з 3-го стовпчика. Вибираємо другий елемент діагоналі з множини $\{k_{10}; k_{11}; k_{13}\}$,тобто третій елемент може бути лише з 3-го рядка та за виключенням 3-го стовпчика, якщо фіксуємо $k_{10}$. Вибираємо третій елемент діагоналі з множини $\{k_{21}; k_{23}\}$, тоді четвертий

елемент визначається однозначно. Якщо третій елемент $k_{21}$, то маємо першу сукупність елементів діагоналі:

$$\{k_{02}; k_{10}; k_{21}; k_{33}\} \quad (2.21)$$

Якщо третій елемент $k_{23}$, то маємо другу сукупність елементів діагоналі

$$\{k_{02}; k_{10}; k_{23}; k_{31}\} \quad (2.22)$$

Аналогічним чином визначаються такі сукупності елементів діагоналі, якщо фіксований перший елемент, тобто:

$$\{k_{02}; k_{11}; k_{20}; k_{33}\} \quad (2.23)$$

$$\{k_{02}; k_{11}; k_{23}; k_{30}\} \quad (2.24)$$

$$\{k_{02}; k_{13}; k_{20}; k_{31}\} \quad (2.25)$$

$$\{k_{02}; k_{13}; k_{21}; k_{30}\} \quad (2.26)$$

Нехай зафіксуємо перший елемент комірки $k_{03}$, тоді другий елемент маємо право брати лише з 2-го рядка та за виключенням з 4-го стовпчика. Вибираємо другий елемент діагоналі з множини $\{k_{10}; k_{11}; k_{12}\}$,тобто третій елемент може бути лише з 3-го рядка та за виключенням 4-го стовпчика, якщо фіксуємо $k_{10}$. Вибираємо третій елемент діагоналі з множини $\{k_{21}; k_{22}\}$, тоді четвертий елемент визначається однозначно. Якщо третій елемент $k_{21}$, то маємо першу сукупність елементів діагоналі:

$$\{k_{03}; k_{10}; k_{21}; k_{32}\} \quad (2.27)$$

Якщо третій елемент $k_{22}$, то маємо другу сукупність елементів діагоналі

$$\{k_{03}; k_{10}; k_{22}; k_{31}\} \quad (2.28)$$

Аналогічним чином визначаються такі сукупності елементів діагоналі, якщо фіксований перший елемент, тобто:

$$\{k_{03}; k_{11}; k_{20}; k_{32}\} \quad (2.29)$$

$$\{k_{03}; k_{11}; k_{22}; k_{30}\} \quad (2.30)$$

$$\{k_{03}; k_{12}; k_{20}; k_{31}\} \quad (2.31)$$

$$\{k_{03}; k_{12}; k_{21}; k_{30}\} \quad (2.32)$$

Отже, після перевірки, можна підтвердити, що кількість всіх можливих діагоналей латинського квадрату 4-го порядку існує 24 діагоналі.

Нехай маємо латинський квадрат групи Кляйна, записаний у вигляді таблиці Келі (див табл. 2.11) з визначеною операцією (⊕).

Таблиця 2.12 – Латинський квадрат групи Кляйна

| ⊕ | *0* | *1* | *2* | *3* |
|---|---|---|---|---|
| *0* | 0 | 1 | 2 | 3 |
| *1* | 1 | 0 | 3 | 2 |
| *2* | 2 | 3 | 0 | 1 |
| *3* | 3 | 2 | 1 | 0 |

Для наведеної таблиці 2.11 знайдемо та позначимо всі можливі трансверсаллі у вигляді $k_{ij}$, де $i$ - це номер рядка, $j$ - це номер стовпця, $k$ - це значення комірки.

Оскільки за умовою латинський квадрат 4-го порядку до елементи трансверсалі можливі тільки $\{0; 1; 2; 3\}$.

Таким чином нехай зафіксуємо перший елемент комірки $k_{00} = 0$, тоді другий елемент маємо з 2-го рядка та починаючи з 2-го стовпчика, окрім $k = 0$. Обираючи другий елемент маємо множини $\{k_{12}, k_{13}\}$,якщо зафіксуємо другий елемент $k_{12} = 3$, тоді третій елемент обираємо з умовою $k \neq \{0; 3\} \wedge j \neq 0 \wedge \quad j \neq 2$, враховуючи умови можемо сказати, що третій та четвертий елемент можна визначити автоматично.

| *i* | *j* | *k* |
|---|---|---|
| *0* | *0* | *0* |
| *1* | *2* | *3* |
| *2* | *3* | *1* |
| *3* | *1* | *2* |

Якщо другий елемент $k_{13} = 2$, то маємо наступну сукупність трансверсалей

| *i* | *j* | *k* |
|---|---|---|
| *0* | *0* | *0* |
| *1* | *3* | *2* |
| *2* | *1* | *3* |
| *3* | *2* | *1* |

Нехай зафіксуємо перший елемент комірки $k_{01} = 1$, тоді другий елемент маємо з 2-го рядка та за виключення 2-го стовпчика та окрім $k = 1$. Обираючи другий елемент маємо множини $\{k_{12}, k_{13}\}$,якщо зафіксуємо другий елемент $k_{12} = 3$, тоді третій елемент обираємо з умовою $k \neq \{1; 3\} \cup j \neq 1 \cup j \neq 2$, враховуючи умови можемо сказати, що третій та четвертий елемент можна визначити автоматично.

| *i* | *j* | *k* |
|---|---|---|
| *0* | *1* | *1* |
| *1* | *2* | *3* |
| *2* | *0* | *2* |
| *3* | *3* | *0* |

Якщо другий елемент $k_{13} = 2$, то маємо наступну сукупність трансверсалей.

| *i* | *j* | *k* |
|---|---|---|
| *0* | *1* | *1* |
| *1* | *3* | *2* |
| *2* | *2* | *0* |
| *3* | *0* | *3* |

Нехай зафіксуємо перший елемент комірки $k_{02} = 2$, тоді другий елемент маємо з 2-го рядка та за виключення 3-го стовпчика та окрім $k = 2$. Обираючи другий елемент маємо множини $\{k_{10}, k_{11}\}$,якщо зафіксуємо другий елемент $k_{10} = 1$, тоді третій елемент обираємо з умовою $k \neq \{1; 2\} \cup j \neq 0 \cup j \neq 2$,

враховуючи умови можемо сказати, що третій та четвертий елемент можна визначити автоматично.

| *i* | *j* | *k* |
|---|---|---|
| *0* | *2* | *2* |
| *1* | *0* | *1* |
| *2* | *1* | *3* |
| *3* | *3* | *0* |

Якщо другий елемент $k_{11} = 0$, то маємо наступну сукупність трансверсалей

| *i* | *j* | *k* |
|---|---|---|
| *0* | *2* | *2* |
| *1* | *1* | *0* |
| *2* | *3* | *1* |
| *3* | *0* | *3* |

Нехай зафіксуємо перший елемент комірки $k_{03} = 3$, тоді другий елемент маємо з 2-го рядка та за виключення 4-го стовпчика та окрім $k = 3$. Обираючи другий елемент маємо множини $\{k_{10}, k_{11}\}$,якщо зафіксуємо другий елемент $k_{10} = 1$, тоді третій елемент обираємо з умовою $k \neq \{1; 3\} \cup j \neq 0 \cup j \neq 3$, враховуючи умови можемо сказати, що третій та четвертий елемент можна визначити автоматично.

| *i* | *j* | *k* |
|---|---|---|
| *0* | *3* | *3* |
| *1* | *0* | *1* |
| *2* | *2* | *0* |
| *3* | *1* | *2* |

Якщо другий елемент $k_{11} = 0$, то маємо наступну сукупність трансверсалей

| *i* | *j* | *k* |
|---|---|---|
| *0* | *3* | *3* |
| *1* | *1* | *0* |
| *2* | *0* | *2* |
| *3* | *2* | *1* |

Отже, можна зробити висновок, що латинські квадрати групи Клейна мають 8 трансверсалей.■

**Твердження 2.2.1.** *Якщо в частковому латинському квадраті 4-го порядку, ізотопного групі Кляйна, заповнені* $\forall$ *5 комірок, 4 з яких утворюють трансверсаль, то такий латинський квадрат має однозначне латинське заповнення.*

**Доведення.** Нехай отримали частково заповнений латинський квадрат 4-го порядку у якому довільно заповнені 5 комірок, 4 з яких утворили трансверсль $k_{03} = 3, k_{11} = 0, k_{20} = 2, k_{32} = 1$ (табл. 2.13).

Таблиця 2.13 – Частково заповнений латинський квадрат

| | *0* | *1* | *2* | *3* |
|---|---|---|---|---|
| *0* | | | | 3 |
| *1* | | 0 | | |
| *2* | 2 | | | |
| *3* | | | 1 | |

Тоді отримавши довільну 5-ту комірку, нехай $k_{00} = 0$ (табл. 2.14)

Таблиця 2.14 – Частково заповнений латинський квадрат

| | *0* | *1* | *2* | *3* |
|---|---|---|---|---|
| *0* | 0 | | | 3 |
| *1* | | 0 | | |
| *2* | 2 | | | |
| *3* | | | 1 | |

Можна стверджувати, що такий латинський квадрат має однозначне латинське заповнення, наприклад табл. 2.12.■

**Наслідок 2.2.1.** *Кількість заповнень часткового латинського квадрату 4-го порядку ізотопного групі Кляйна точно 96 розташувань.*

**Доведення.** Оскільки всього довільних комірок 16, п’ять з яких заповнені, де 4 комірки утворюють трансверсаль, то для вибору 5-го елементу залишається $16-4=12$ комірок. Оскільки з Леми 2 доведено, що латинський квадрат 4-го порядку ізотопний групі Кляйна має 8 трансверсалей. Тоді маємо загальну кількість $12\cdot 8=96$ заповнень.■

**Твердження 2.2.2.** *Якщо в частковому нормалізованому латинському квадраті 4-го порядку, ізотопного групі Кляйна у якому заповнені 6 комірок, типу 2+2+1+1, кожен з яких не з’являються в комірку фіксованої трансверсалі то такий латинський квадрат має однозначне заповнення.*

**Доведення.** Нехай маємо частково заповнений латинський квадрат 4-го порядку, де отримали 6 комірок, нехай $k_{11}=0, k_{22}=0, k_{01}=1, k_{23}=1, k_{31}=2, k_{03}=3$.(табл. 2.15)

Таблиця 2.15 – Частково заповнений латинський квадрат 6-ма комірками

| | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | | 1 | | 3 |
| 1 | | 0 | | |
| 2 | | | 0 | 1 |
| 3 | | 2 | | |

Оскільки відповідні відкриті комірки не утворюють трансверсалей то можна стверджувати, що латинський квадрат має однозначне латинське заповнення табл. 2.12.■

**Наслідок 2.2.2.** *Кількість заповнень часткового латинського квадрату 4-го порядку ізотопного групі Кляйна у якому заповнені 6 комірок, типу 2+2+1+1, кожен з яких не з’являються в комірку фіксованої трансверсалі то такий латинський квадрат має однозначне заповнення точно 3888 варіантів.*

**Доведення.** Нехай частковий латинський квадрат у якому 6 комірок заповнені, але 4 з яких не утворюють фіксовану трансверсаль, тоді маючи появу 2+2+1+1 комірок, отримаємо, що кожен з представлених елементів містить по 3 різних варіанти розташування комірок, окрім тих які утворять фіксовану трансверсаль, отже отримуємо, що $3 \cdot 3 \cdot 3 \cdot 3 = 81$ варіант.

Скомбінувавши значення комірок отримали наступну кількість можливих квадратів:

2 нулі, 2 одиниці, 1 двійка, 1 трійка – 81 розташування;

2 нулі, 1 одиниця, 2 двійки, 1 трійка – 81 розташування;

2 нулі, 1 одиниця, 1 двійка, 2 трійки – 81 розташування;

1 нуль, 2 одиниці, 2 двійки, 1 трійка – 81 розташування;

1 нуль, 1 одиниця, 2 двійки, 2 трійки – 81 розташування;

1 нуль, 2 одиниці, 1 двійка, 2 трійки – 81 розташування;

Обчисливши кількість можливих варіантів розташувань частково заповнених латинських квадратів маємо кількість $81 \cdot 6 = 486$. Оскільки кількість варіантів була розрахована для однієї трансверсалі, а згідно Леми 2 для нормалізованого латинського квадрату групи Кляйна їх кількість становить 8, то необхідно отриманий результат помножити на кількість трансверсалей $486 \cdot 8 = 3888$ можливих варіантів часткових заповнень.■

**Твердження 2.2.3.** *Якщо в нормалізованому латинському квадраті 4-го порядку, ізотопного групі Кляйна, заповнені 7 комірок з появами всіх 4-ьох елементів типу 3+2+1+1 або 2+2+2+1, кожен з яких не потрапляє в комірку фіксованої трансверсалі, то такий латинський квадрат має однозначне латинське заповнення.*

**Доведення.** Нехай отримали частково заповнений латинський квадрат 4-го порядку у якому заповнені 7 комірок жоден з яких не потрапляє у фіксовану трансверсаль $k_{00} = 0, k_{12} = 3, k_{23} = 1, k_{31} = 2$ з появою всіх 4-ьох елементів типу 3+2+1+1, де отримали нехай $k_{11} = 0, k_{22} = 0, k_{33} = 0, k_{10} = 1, k_{32} = 1, k_{02} = 2, k_{30} = 3$. (табл. 2.16)

Таблиця 2.16 – Частково заповнений латинський квадрат за схемою 3+2+1+1

| | *0* | *1* | *2* | *3* |
|---|---|---|---|---|
| *0* | x | | 2 | |
| *1* | 1 | 0 | x | |
| *2* | | | 0 | x |
| *3* | 3 | x | 1 | 0 |

Або нехай заповнені 7 комірок з появою всіх 4-ьох елементів типу 2+2+2+1, де отримали нехай $k_{22} = 0,, k_{33} = 0, k_{10} = 1, k_{01} = 1, k_{13} = 2, k_{20} = 2, k_{03} = 3.$ (табл. 2.17)

Таблиця 2.17 – Частково заповнений латинський квадрат за схемою 3+2+1+1

| | *0* | *1* | *2* | *3* |
|---|---|---|---|---|
| *0* | x | 1 | | 3 |
| *1* | 1 | | x | 2 |
| *2* | 2 | | 0 | x |
| *3* | | x | | 0 |

Оскільки відповідні відкриті комірки не утворюють фіксовану трансверсаль то можна стверджувати, що латинський квадрат має однозначне латинське заповнення таблиця 2.12.■

**Наслідок 2.2.3.1.** *Кількість заповнень часткового латинського квадрату 4-го порядку ізотопного групі Кляйна у якому заповнені 7 комірок, типу 3+2+1+1, кожен з яких не з'являються в комірку фіксованої трансверсалі то такий латинський квадрат має однозначне заповнення точно 2592 варіантів.*

**Доведення.** Нехай частковий латинський квадрат у якому 7 комірок заповнені, але 4 з яких не утворюють фіксовану трансверсаль, тоді маючи появу 3+2+1+1 комірок, отримаємо, що елемент який повторюється 3 рази має 1 можливий варіант розташування, а решта у 3 можливих варіантах розташування. Для одного з можливих варіантів розташувань отримуємо $1 \cdot 3 \cdot 3 \cdot 3 = 27$ варіантів.

Скомбінувавши значення комірок, отримали наступну кількість квадратів:

3 нулі, 2 одиниці, 1 двійка, 1 трійка – 27 розташувань;

3 нулі, 2 двійки, 1 одиниця, 1 трійка – 27 розташувань;

3 нулі, 2 трійки, 1 двійка, 1 одиниця – 27 розташувань;

3 одиниці, 2 нулі, 1 двійка, 1 трійка – 27 розташувань;

3 одиниці, 2 двійки, 1 нуль, 1 трійка – 27 розташувань;

3 одиниці, 2 трійки, 1 нуль, 1 двійка – 27 розташувань;

3 двійки, 2 нулі, 1 одиниця, 1 трійка – 27 розташувань;

3 двійки, 2 одиниці, 1 нуль, 1 трійка – 27 розташувань;

3 двійки, 2 трійки, 1 нуль, 1 одиниця – 27 розташувань;

3 трійки, 2 нулі, 1 одиниця, 1 двійка – 27 розташувань;

3 трійки, 2 одиниці, 1 двійка, 1 нуль – 27 розташувань;

3 трійки, 2 двійки, 1 нуль, 1 одиниця – 27 розташувань;

Обчисливши кількість можливих розташувань частково заповнених латинських квадратів маємо загальну кількість $27 \cdot 12 = 324$ .

Оскільки кількість варіантів була розрахована для однієї трансверсалі, а згідно Леми 2 для нормалізованого латинського квадрату групи Кляйна їх кількість становить 8, то необхідно отриманий результат помножити на кількість трансверсалей $324 \cdot 8 = 2592$ можливих варіантів часкових заповнень. ■

**Наслідок 2.2.3.2.** *Кількість заповнень часткового латинського квадрату 4-го порядку ізотопного групі Кляйна у якому заповнені 7 комірок, типу 2+2+2+1, кожен з яких не з'являються в комірку фіксованої трансверсалі то такий латинський квадрат має однозначне заповнення точно 2592 варіантів.*

**Доведення.** Нехай частковий латинський квадрат у якому 7 комірок заповнені, але 4 з яких не утворюють фіксовану трансверсаль, тоді маючи появу 2+2+2+1 комірок, отримаємо, що кожен з представлених елементів містить по 3 різних варіанти розташування комірок, окрім тих які утворять фіксовану трансверсаль, отже отримуємо, що $3 \cdot 3 \cdot 3 \cdot 3 = 81$ варіант.

Скомбінувавши значення комірок отримали наступну кількість можливих квадратів:

2 нулі, 2 одиниці, 2 двійка, 1 трійка – 81 розташування;

2 нулі, 1 одиниця, 2 двійки, 2 трійка – 81 розташування;

1 нуль, 2 одиниці, 2 двійки, 2 трійки – 81 розташування;

2 нулі, 2 одиниці, 1 двійка, 2 трійки – 81 розташування;

Обчисливши кількість можливих варіантів розташувань частково заповнених латинських квадратів маємо кількість $81 \cdot 4 = 324$. Оскільки кількість варіантів була розрахована для однієї трансверсалі, а згідно Леми 2 для нормалізованого латинського квадрату групи Кляйна їх кількість становить 8, то необхідно отриманий результат помножити на кількість трансверсалей $324 \cdot 8 = 2592$ можливих варіантів часткових заповнень.■

**Твердження 2.2.4.** *Якщо в частковому латинському квадраті 4-го порядку ізотопного групі Кляйна заповнені* $\forall$ *7 комірок, з яких неповна діагональ одного елемента, 2 комірки довільного другого елемента та 2 комірки третього елемента, то такий латинський квадрат має однозначне латинське заповнення.*

**Доведення.** Нехай отримали частково заповнений латинський квадрат 4-го порядку у якому довільно заповнені 7 комірок, 3 з яких утворили неповну діагональ $k_{00} = 0, k_{11} = 0, k_{22} = 0$ (табл. 2.18).

Таблиця 2.18 – Частково заповнений латинський квадрат неповною діагоналлю

| | *0* | *1* | *2* | *3* |
|---|---|---|---|---|
| *0* | 0 | | | |
| *1* | | 0 | | |
| *2* | | | 0 | |
| *3* | | | | |

Також отримавши будь які 2 комірки довільного елемента та 2 комірки третього елемента, нехай $k_{03} = 3, k_{12} = 3, k_{23} = 1, k_{32} = 1$(табл. 2.19).

Таблиця 2.19 – частково заповнений латинський квадрат ∀ 7 елементами

| | *0* | *1* | *2* | *3* |
|---|---|---|---|---|
| *0* | 0 | | | 3 |
| *1* | | 0 | 3 | |
| *2* | | | 0 | 1 |
| *3* | | | 1 | |

Можна стверджувати, що такий латинський квадрат має однозначне латинське заповнення, наприклад табл. 2.12.■

**Наслідок 2.2.4.** *Кількість заповнень часткового латинського квадрату 4-го порядку ізотопного групі Кляйна у якому заповнені ∀ 7 комірок, з яких 3 неповна діагональ одного елемента, 2 комірки довільного другого елемента та 2 комірки третього елемента точно 1728 варіантів.*

**Доведення.** Оскільки частково заповнених латинських квадратів де довільно заповнено три комірки які утворюють неповну діагональ, а також дві комірки з довільним другим елементом який не повторюється і дві комірки з довільним третім елементом таких квадратів 144. Оскільки три комірки з одним елементом утворюють 4 варіанти, дві комірки з другим довільним елементом 6 варіантів та дві комірки з довільним третім елементом 6 варіантів.

Для одного з можливих варіантів розташувань отримуємо $4 \cdot 6 \cdot 6 = 144$ варіанти. Скомбінувавши значення комірок, отримали наступну кількість квадратів:

3 нулі, 2 одиниці, 2 двійки – 144 розташування;

3 нулі, 2 двійки, 2 трійки – 144 розташування;

3 нулі, 2 одиниці, 2 трійки – 144 розташування;

3 одиниці, 2 нулі, 2 двійки – 144 розташування;

3 одиниці, 2 нулі, 2 трійки – 144 розташування;

3 одиниці, 2 двійки, 2 трійки – 144 розташування;

3 двійки, 2 нулі, 2 одиниці – 144 розташування;

3 двійки, 2 одиниці, 2 трійки – 144 розташування;

3 двійки, 2 нулі, 2 трійки – 144 розташування;

3 трійки, 2 нулі, 2 одиниці – 144 розташування;

3 трійки, 2 одиниці, 2 двійки – 144 розташування;

3 трійки, 2 нулі, 2 двійки – 144 розташування;

Обчисливши кількість можливих розташувань частково заповнених латинських квадратів маємо загальну кількість $144 \cdot 12 = 1728$ . ■

**Твердження 2.2.5.** *Якщо в нормалізовано латинському квадраті 4-го порядку, ізотопного групи Кляйна, заповнені 8 елементів з появами лише 3-ьох елементів з 4-ьох можливих типу 3+3+2 або 4+2+2, то такий латинський квадрат має однозначне заповнення.*

**Доведення.** Нехай отримали частково заповнений латинський квадрат 4-го порядку, де заповнено 8 елементів типу 3+3+2, де 2 елементи різні елементи утворюють неповну діагональ, а третій довільний заповнений в 2 комірках. Тоді отримаємо $k_{11} = 0, k_{22} = 0, k_{33} = 0, k_{10} = 1, k_{32} = 1, k_{01} = 1, k_{30} = 3, k_{21} = 3.$ (табл. 2.20)

Таблиця 2.20 – Частково заповнений латинський квадрат типу 3+3+2

| | *0* | *1* | *2* | *3* |
|---|---|---|---|---|
| *0* | 0 | 1 | | 3 |
| *1* | | 0 | | |
| *2* | | 3 | 0 | |
| *3* | 1 | | 1 | |

Аналогічним чином, якщо заповнені 8 елементів за типом 4+2+2, тоді утвориться діагональ одного елемента та два довільних інших елементи будуть заповнені у 2-х комірках, тоді отримаємо $k_{11} = 0, k_{22} = 0, k_{33} = 0, k_{00} = 0, k_{32} = 1, k_{01} = 1, k_{30} = 3, k_{21} = 3.$ (табл. 2.21)

Таблиця 2.21 – Частково заповнений латинський квадрат типу 4+2+2

| | *0* | *1* | *2* | *3* |
|---|---|---|---|---|
| *0* | 0 | 1 | | 3 |
| *1* | | 0 | | |
| *2* | | 3 | 0 | |
| *3* | | | 1 | 0 |

Отже, можна стверджувати, що такий латинський квадрат має однозначне латинське заповнення, наприклад таблиця 2.12.■

**Наслідок 2.2.5.1** *Кількість заповнень 8-ми елементів типу 3+3+2 латинського квадрата 4-го порядку, ізотопного групі Кляйна становить точно 1152 варіанти.*

**Доведення.** Оскільки частково заповнених латинських квадратів де довільно заповнено три комірки які утворюють неповну діагональ, а також три комірки з довільним другим елементом який утворює неповну діагональ і дві комірки з довільним третім елементом таких квадратів 96. Оскільки три комірки з одним елементом утворюють 4 варіанти, три комірки з другим довільним елементом 4 варіанти та дві комірки з довільним третім елементом 6 варіантів.

Для одного з можливих варіантів розташувань отримуємо $4 \cdot 4 \cdot 6 = 96$ варіантів. Скомбінувавши значення комірок, отримали наступну кількість квадратів:

2 нулі, 3 одиниці, 3 двійки – 96 розташувань;

2 нулі, 3 двійки, 3 трійки – 96 розташувань;

2 нулі, 3 одиниці, 3 трійки – 96 розташувань;

2 одиниці, 3 нулі, 3 двійки – 96 розташувань;

2 одиниці, 3 нулі, 3 трійки – 96 розташувань;

2 одиниці, 3 двійки, 3 трійки – 96 розташувань;

2 двійки, 3 нулі, 3 одиниці – 96 розташувань;

2 двійки, 3 одиниці, 3 трійки – 96 розташувань;

2 двійки, 3 нулі, 3 трійки – 96 розташувань;

2 трійки, 3 нулі, 3 одиниці – 96 розташувань;

2 трійки, 3 одиниці, 3 двійки – 96 розташувань;

2 трійки, 3 нулі, 3 двійки – 96 розташувань;

Обчисливши кількість можливих розташувань частково заповнених латинських квадратів маємо загальну кількість $96 \cdot 12 = 1152$ варіанти. ■

**Наслідок 2.2.5.2** *Кількість заповнень 8-ми елементів типу 4+2+2 латинського квадрата 4-го порядку, ізотопного групі Кляйна становить точно 432 варіанти.*

**Доведення.** Оскільки частково заповнених латинських квадратів де довільно заповнено чотири комірки які утворюють діагональ, а також дві комірки з довільним другим елементом який не повторюється і дві комірки з довільним третім елементом таких квадратів 36. Оскільки чотири комірки з одним елементом утворюють 1 варіант, дві комірки з другим довільним елементом 6 варіантів та дві комірки з довільним третім елементом 6 варіантів.

Для одного з можливих варіантів розташувань отримуємо $1 \cdot 6 \cdot 6 = 36$ варіанти. Скомбінувавши значення комірок, отримали наступну кількість квадратів:

4 нулі, 2 одиниці, 2 двійки – 36 розташувань;

4 нулі, 2 двійки, 2 трійки – 36 розташувань;

4 нулі, 2 одиниці, 2 трійки – 36 розташувань;

4 одиниці, 2 нулі, 2 двійки – 36 розташувань;

4 одиниці, 2 нулі, 2 трійки – 36 розташувань;

4 одиниці, 2 двійки, 2 трійки – 36 розташувань;

4 двійки, 2 нулі, 2 одиниці – 36 розташувань;

4 двійки, 2 одиниці, 2 трійки – 36 розташувань;

4 двійки, 2 нулі, 2 трійки – 36 розташувань;

4 трійки, 2 нулі, 2 одиниці – 36 розташувань;

4 трійки, 2 одиниці, 2 двійки – 36 розташувань;

4 трійки, 2 нулі, 2 двійки – 36 розташувань;

Обчисливши кількість можливих розташувань частково заповнених латинських квадратів маємо загальну кількість $36 \cdot 12 = 432$ . ■

**Твердження 2.2.6** *Якщо в нормалізованому латинському квадраті 4-го порядку, ізотопного групі Кляйна, заповнені 8 елементів з появами типу 3+3+1+1, кожен з яких не потрапляє в комірку фіксованої трансверсалі, то такий латинський квадрат має однозначне заповнення.*

**Доведення.** Нехай отримали частково заповнений латинський квадрат у якому заповнено 8 елементів з появами 3+3+1+1 кожен з яких не потрапляє в комірки фіксованої трансерсалі, тоді нехай $k_{11} = 0, k_{22} = 0, k_{33} = 0, k_{01} = 1, k_{10} = 1, k_{23} = 1, k_{30} = 3, k_{02} = 2$.(табл. 2.22)

Таблиця 2.22 – Частково заповнений латинський квадрат типу 3+3+1+1

| | *0* | *1* | *2* | *3* |
|---|---|---|---|---|
| *0* | | 1 | 2 | |
| *1* | 1 | 0 | | |
| *2* | | | 0 | 1 |
| *3* | 3 | | | 0 |

Отже, можна стверджувати, що такий латинський квадрат має однозначне латинське заповнення, наприклад таблиця 2.12. ■

**Наслідок 2.2.6** *Кількість заповнень 8-ми елементів типу 3+3+1+1 латинського квадрата 4-го порядку, ізотопного групі Кляйна становить точно 3888 варіанти.*

**Доведення.** Нехай частковий латинський квадрат у якому 8 комірок заповнені, але 4 з яких не утворюють фіксовану трансверсаль, тоді маючи появу 3+3+1+1 комірок, отримаємо, що кожен з представлених елементів містить по 3 різних варіанти розташування комірок, окрім тих які утворять фіксовану трансверсаль, отже отримуємо, що $3 \cdot 3 \cdot 3 \cdot 3 = 81$ варіант.

Скомбінувавши значення комірок отримали наступну кількість можливих квадратів:

3 нулі, 3 одиниці, 1 двійка, 1 трійка – 81 розташування;

3 нулі, 1 одиниця, 3 двійки, 1 трійка – 81 розташування;

3 нулі, 1 одиниця, 1 двійка, 3 трійки – 81 розташування;

1 нуль, 3 одиниці, 3 двійки, 1 трійка – 81 розташування;

1 нуль, 1 одиниця, 3 двійки, 3 трійки – 81 розташування;

1 нуль, 3 одиниці, 1 двійка, 3 трійки – 81 розташування;

Обчисливши кількість можливих варіантів розташувань частково заповнених латинських квадратів маємо кількість $81 \cdot 6 = 486$. Оскільки кількість варіантів була розрахована для однієї трансверсалі, а згідно Леми 2 для нормалізованого латинського квадрату групи Кляйна їх кількість становить 8, то необхідно отриманий результат помножити на кількість трансверсалей $486 \cdot 8 = 3888$ можливих варіантів часткових заповнень.■

**Твердження 2.2.7** *Якщо в нормалізованому латинському квадраті 4-го порядку, ізотопного групі Кляйна, заповнені 8 елементів з появами типу 4+2+1+1, то такий латинський квадрат має однозначне заповнення.*

**Доведення.** Нехай маємо частково заповнений латинський квадрат 4-го порядку, де заповнено 8 комірок з появами ти 4+2+1+1, нехай маємо $k_{11} = 0, k_{22} = 0, k_{33} = 0, k_{00} = 0, k_{10} = 1, k_{23} = 1, k_{30} = 3, k_{02} = 2$.(табл. 2.23)

Таблиця 2.23 – Частково заповнений латинський квадрат типу 4+2+1+1

| | *0* | *1* | *2* | *3* |
|---|---|---|---|---|
| *0* | 0 | | 2 | |
| *1* | 1 | 0 | | |
| *2* | | | 0 | 1 |
| *3* | 3 | | | 0 |

Отже, можна стверджувати, що такий латинський квадрат має однозначне латинське заповнення, наприклад таблиця 2.12.■

**Наслідок 2.2.7.** *Кількість заповнень часткового латинського квадрату 4-го порядку ізотопного групі Кляйна у якому заповнені 8 комірок, типу 4+2+1+1, то такий латинський квадрат має однозначне заповнення точно 1152 варіантів.*

**Доведення.** Нехай частковий латинський квадрат у якому 8 комірок заповнені маючи появу 4+2+1+1 комірок, отримаємо, що елемент який повторюється 4 рази має 1 можливий варіант розташування, елемент який повторюється 2 рази можуть розташовуватись у 6 можливих варіантах, а решта у 4 можливих варіантах розташування. Для одного з можливих варіантів розташувань отримуємо $1 \cdot 6 \cdot 4 \cdot 4 = 96$ варіантів.

Скомбінувавши значення комірок, отримали наступну кількість квадратів:

4 нулі, 2 одиниці, 1 двійка, 1 трійка – 96 розташувань;

4 нулі, 2 двійки, 1 одиниця, 1 трійка – 96 розташувань;

4 нулі, 2 трійки, 1 двійка, 1 одиниця – 96 розташувань;

4 одиниці, 2 нулі, 1 двійка, 1 трійка – 96 розташувань;

4 одиниці, 2 двійки, 1 нуль, 1 трійка – 96 розташувань;

4 одиниці, 2 трійки, 1 нуль, 1 двійка – 96 розташувань;

4 двійки, 2 нулі, 1 одиниця, 1 трійка – 96 розташувань;

4 двійки, 2 одиниці, 1 нуль, 1 трійка – 96 розташувань;

4 двійки, 2 трійки, 1 нуль, 1 одиниця – 96 розташувань;

4 трійки, 2 нулі, 1 одиниця, 1 двійка – 96 розташувань;

4 трійки, 2 одиниці, 1 двійка, 1 нуль – 96 розташувань;

4 трійки, 2 двійки, 1 нуль, 1 одиниця – 96 розташувань;

Обчисливши кількість можливих розташувань частково заповнених латинських квадратів маємо загальну кількість $96 \cdot 12 = 1152$ . ■

Отже, можна стверджувати, що частково заповненні латинські квадрати 4-го порядку мають однозначне заповнення у 17520 варіантах мінімальної кількості відомих відкритих комірок.

# 3 КРИПТОАНАЛІЗ ТА РОЗРОБКА АЛГОРИТМУ ВІДНОВЛЕННЯ СЕКРЕТНОГО КЛЮЧА

## 3.1 Розробка алгоритму відновлення секретного ключа

Оскільки у розділі 2 було визначено та описано умови за допомогою яких можливо відновлювати секретний ключ у вигляді латинських квадратів 3-го та 4-го порядків постає завдання розробити алгоритм за допомогою якого буде здійснюватися однозначне заповнення отриманих частково заповнених латинських квадратів.

Під час розробки алгоритму, необхідно враховувати декілька аспектів такі як:

1) Інформація про ключ, яка була отримана, а саме кількість, розташування та значення відкритих комірок;

Відповідно перед початком роботи алгоритму, необхідно мати набір відкритих комірок, на базі яких буде проводитись заповнення ключа у вигляді латинського квадрату. Згідно доведених тверджень та наслідків отримано кількість можливих варіантів для заповнення часткових латинських квадратів 3-го та 4-го порядку.

2) Процес вибору комірки, яка буде заповнюватись;

Під час роботи алгоритму, важливий етап, це процес вибору комірки, яка буде заповнюватись, та подальший вибір комірок для заповнень, до повного відновлення ключа.

3) Процес заповнення порожніх клітинок;

Наступний необхідний етап відновлення, це безпосередньо заповнення комірок, відповідно проаналізувавши рядок та стовпець в якому знаходиться комірка, потрібно заповнити елементом, який був відсутній у рядку та стовпці.

4) Перевірка на відсутність конфліктів;

Під час перевірки на відсутність конфліктів необхідно враховувати, чи повторюються значення комірок у рядку та стовпці, адже при повторені

елементів це не є латинський квадрат, а отже виникає конфлікт і необхідно обрати інший варіант заповнення клітинки.

5) Перевірка на заповнення ключа.

Оскільки алгоритм розрахований на покрокове заповнення елементами, необхідно перевіряти чи заповнено квадрат повністю, у випадку наявності вільних комірок, алгоритм приступає до їх заповнення та після повного заповнення квадрату алгоритм закінчує свою роботу.

Врахувавши ці аспекти було сформовано алгоритм у вигляді блок-схеми представлено на рис. 3.1.

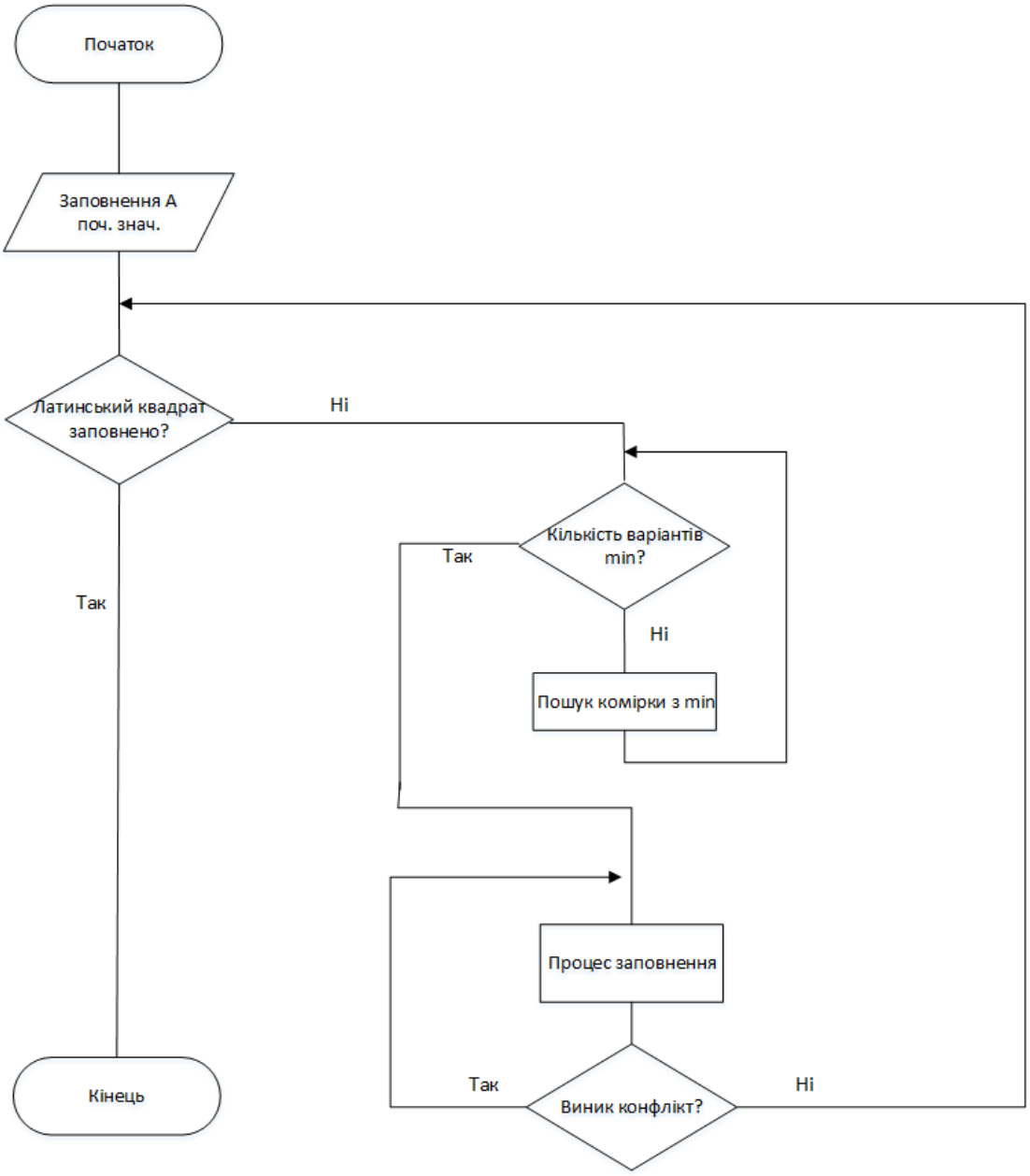



Рисунок 3.1 – Блок схема алгоритму заповнення латинського квадрату

Найпершим етапом роботи алгоритму є заповнення секретного отриманими значеннями комірок та їх розташування. Оскільки це важливий етап подальшого заповнення необхідно зчитати та опрацювати ці значення.

Наступним кроком буде обов’язкова перевірка на заповненість отриманого ключа, оскільки є можливий варіант отримання відразу заповненого такого ключа. У випадку часткового заповнення, алгоритм переходить у наступний етап вибору комірки для заповнення. Цей процес відбувається за принципом найменшої кількості можливих варіантів значень у вибраній комірці.

Під час вибору певної незаповненої комірки, алгоритм визначатиме можливі варіанти для заповнення. Для визначення можливих варіантів заповнення необхідно аналізувати рядок та стовпець на перехресті яких знаходиться обрана комірка. Після визначення можливих варіантів алгоритм підставляє у незаповнену комірку значення з можливої множини цих значень.

В подальшому необхідно провести перевірку на конфлікт. Ця перевірка аналізує рядок та стовпець на перехресті якої знаходиться комірка на предмет повторення деяких елементів. У випадку виникнення конфлікту значення комірки необхідно замінити на інший варіант. Після заповнення деякої комірки без виникнення конфлікту, алгоритм повертається до пункту з перевіркою на заповнення цілого ключа та наявність незаповнених комірок. Цей процес відбувається циклічно до повного заповнення ключа. Після чого алгоритм закінчує свою роботу.

Існує можливість неоднозначного відновлення ключа, в тому випадку, якщо отримані відкриті значення не будуть відповідати бібліотеці сформованих частково заповнених латинських квадратів маючи які однозначно можливо відновити ключ.

### 3.2 Криптоаналіз на основі алгоритму відновлення секретного ключа

Розробивши алгоритм, а також дослідивши за яких умов можливо однозначно заповнити отриманий частковий латинський квадрат. Оскільки

необхідна умова однозначного заповнення, це отримання будь яким методом частковий ключ яким є частковий латинський квадрат, який в подальшому повинен однозначно заповнитись. Розглянемо варіанти таких наборів, та покроково заповнимо їх.

Згідно розділу 2 було встановлено за допомогою ряду тверджень які саме елементи та їх розташування необхідні для однозначного відновлення ключа.

Відповідно твердження 2.1.1, щоб відновити латинський квадрат 3-го порядку необхідно мати 3 заповнені комірки, які утворюють трансверсаль.

Отримавши такий квадрат та обравши порожню комірку $k_{00}$ і проаналізувавши нульовий рядок та стовпець видно, що цій клітинці необхідно присвоїти значення $k_{00} = 1$, оскільки в комірці $k_{01}$ не може бути значення 1 тому, що у першому стовпі вже є таке значення, а комірка $k_{02} = 0$. Відповідно у комірках $k_{20} = 0$ та $k_{01} = 2$, оскільки це останній незаповнений елемент стовпця та рядка відповідно. Аналогічним чином заповнюється решта комірок, тому, що вони будуть останніми незаповненими елементами. Результат відображено на рис. 3.2.

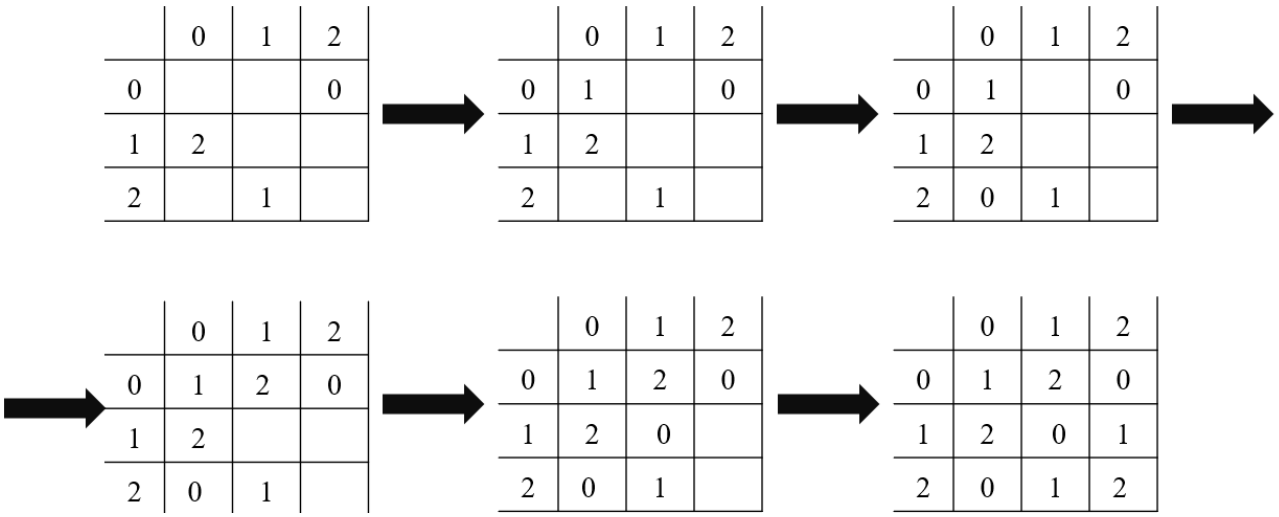



Рисунок 3.2 – Заповнення латинського квадрату за трансверсалями

Довільний частковий латинський квадрат 3-го порядку у якого буде відома будь яка трансверсаль, можна аналогічним чином заповнити.

Згідно твердження 2.1.2 однозначно можливо заповнити латинський квадрат 3-го порядку, якщо отримаємо діагональ одного елемента та будь який довільний інший елемент.

Отримавши частковий латинський квадрат з відомими комірками $k_{01} = 0$, $k_{10} = 0, k_{22} = 0, k_{21} = 2$, першою коміркою для заповнення було обрано $k_{20}$, оскільки це єдина незаповнена комірка у другому рядку, тому її було заповнено значенням 2. Наступна комірка заповнена однозначно за аналогією до першої, оскільки $k_{10} = 0, k_{11} = 1$, тому $k_{12} = 2$. В залишку отримуємо$k_{00} = 2, k_{02} = 1$, які так само заповнюються однозначно через, що вони останні незаповнені елементи. Результат заповнення відображено на рис 3.3.

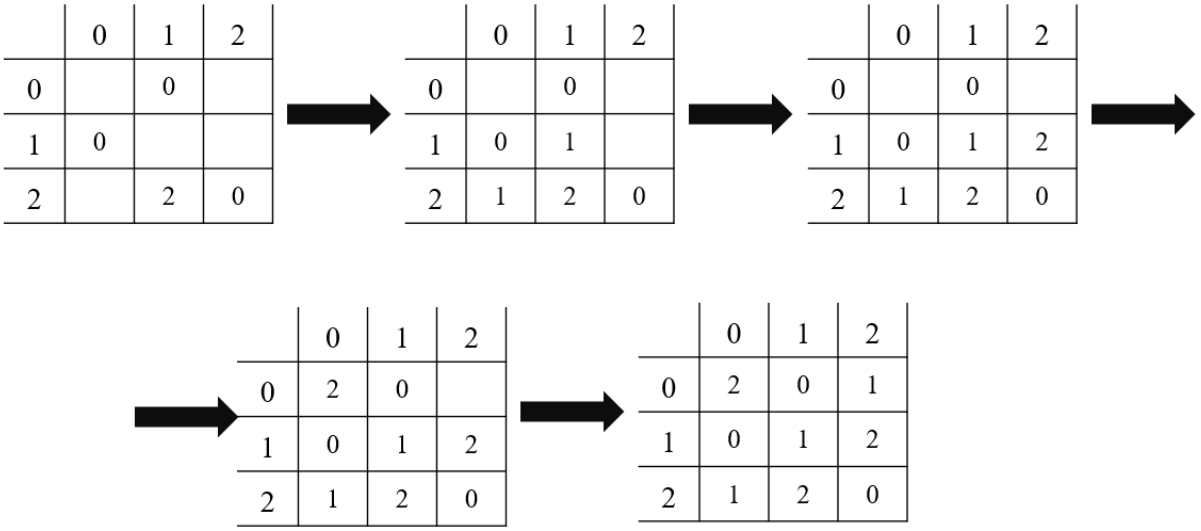



Рисунок 3.3 – Заповнення латинського квадрату за діагоналлю одного елемента

Латинські квадрати 3-го порядку мають лише 3 можливі діагоналі одного елемента, тому маючи принаймні одну довільну таку діагональ та будь яку відкриту 4-ту комірку можливо заповнити однозначно використовуючи алгоритм.

Відповідно до твердження 2.1.3 однозначно можливо заповнити латинський квадрат 3-го порядку отримавши 4 комірки з яких 3 утворять повний рядок або стовпець а 4-та будь який довільний елемент.

Отримавши частково заповнений латинський квадрат 3-го порядку у якому заповнено 3 комірки $k_{20} = 0, k_{21} = 2, k_{22} = 1$ які утворили рядок та один довільний елемент $k_{01} = 1$. Першою для заповнення було обрано комірку $k_{11} =$

1, оскільки вона однозначно заповнюється останнім вільним значенням в стовпці, наступним елементом було заповнено комірку $k_{10} = 2$. Комірка $k_{00}$, була заповнена елементом 1. Аналогічним чином заповнено значеннями комірки $k_{02} = 2$ та $k_{12} = 0$. Перевіривши квадрат на відсутність конфліктів отримали відновлений ключ. Відновлення представлено рис. 3.4.

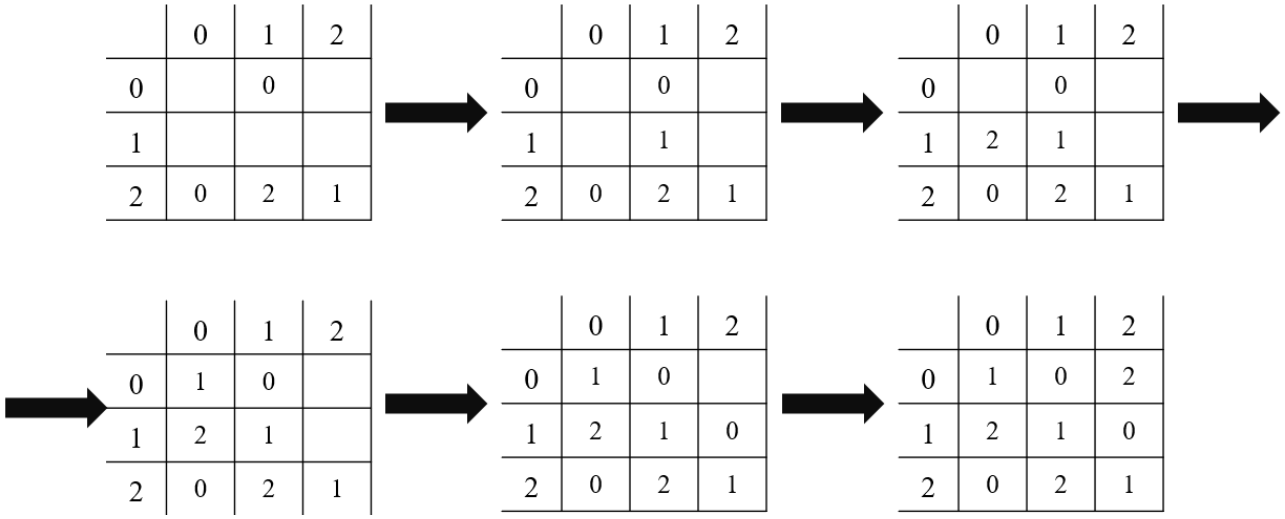



Рисунок 3.4 – Заповнення латинського квадрату отримавши довільний рядок

Маючи будь який довільно відкритий рядок та стовпець та один відкритий елемент однозначно можливо відновити ключ у вигляді латинського квадрату.

Згідно твердження 2.1.4 отримавши частково заповнений ключ у вигляді латинського квадрату 3-го порядку у якому відкрито 2 комірки одного елемента та будь яка комірка з відкритим іншим елементом можна однозначно відновити ключ використовуючи алгоритм.

Отримавши квадрат у якому відкрито комірки $k_{00} = 1, k_{01} = 2, k_{12} = 1$, обираємо першу комірку для заповнення $k_{02} = 0$, оскільки обрана комірка у рядку 0 остання яка не є заповнена. Наступною обрано комірку $k_{22} = 2$ за аналогічним параметром. Далі заповнено 2 комірки у рядку 1 за наступними параметрами $k_{11} = 0$, оскільки у стовпці одним вже присутня комірка $k_{01}$ із значенням 2, а $k_{10} = 2$ заповнено за фактором останньої клітинки у рядку. За аналогією відновлено $k_{20} = 0$ та $k_{21} = 1$, як останні значення у стовпцях. Результат відображено на рис. 3.5.

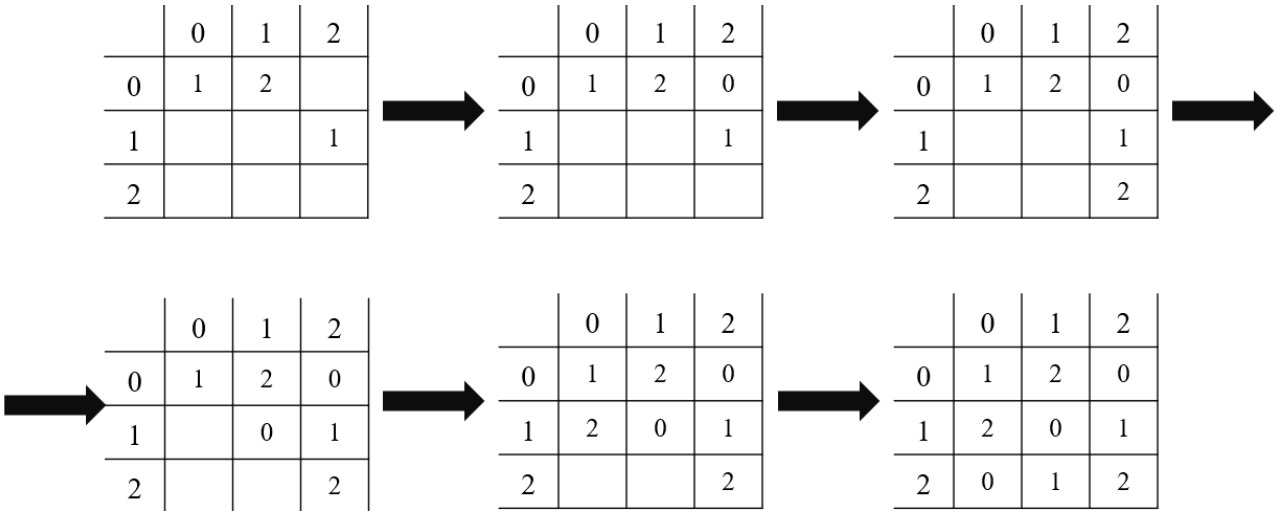



Рисунок 3.5 – Заповнення латинського квадрату отримавши 3 відкриті елементи

Оскільки згідно наслідку 2.1.4, якщо буде отримано будь який варіант такого часткового заповнення можливо однозначно відновити такий ключ.

Представлений алгоритм відновлення секретного ключа також використовується для заповнення латинського квадрату 4-го порядку.

Згідно твердження 2.2.1, якщо отримаємо частковий латинський квадрат 4-го порядку у якому заповнено 5 комірок з яких, 4 утворюють трансверсаль та ще 1 довільний елемент то такий латинський квадрат має однозначне заповнення.

Отримавши частковий ключ у вигляді латинського квадрату, в якому маємо заповнені комірки $k_{02} = 3, k_{10} = 3, k_{13} = 0, k_{21} = 2, k_{30} = 1$, де 4 комірки утворюють трансверсаль, тоді за допомогою алгоритму відновимо ключ. Обравши перший рядок у якому заповнимо комірки $k_{11} = 1$ та $k_{12} = 2$, тому що у першому стовпці маємо комірку із значенням 2. Наступними елементами будуть заповнені комірки $k_{01} = 0$ та $k_{31} = 3$, оскільки у нульовому рядку вже є заповнена комірка із значенням 3, а елемент $k_{31}$ заповнено за фактом останьої вільної комірки. Елемент $k_{22} = 1$, оскільки у третьому рядку присутнє значення комірки 1, тому у $k_{32} = 0$, як останній незаповнений елемент стовпця. Аналогічним чином заповнено нульовий стовпець, $k_{00} = 2, k_{20} = 0$, тому, що у нульовому рядку присутнє значення комірки 1, відповідно у випадку розташування елементів $k_{00} = 0$ та $k_{20} = 2$ виникає конфлікт. Комірки $k_{03} =$

$1, k_{23} = 3, k_{33} = 2$, оскільки елементи є останніми незаповненими у рядках, тому заповнюються однозначно. Результат заповнення відображено на рис. 3.6.

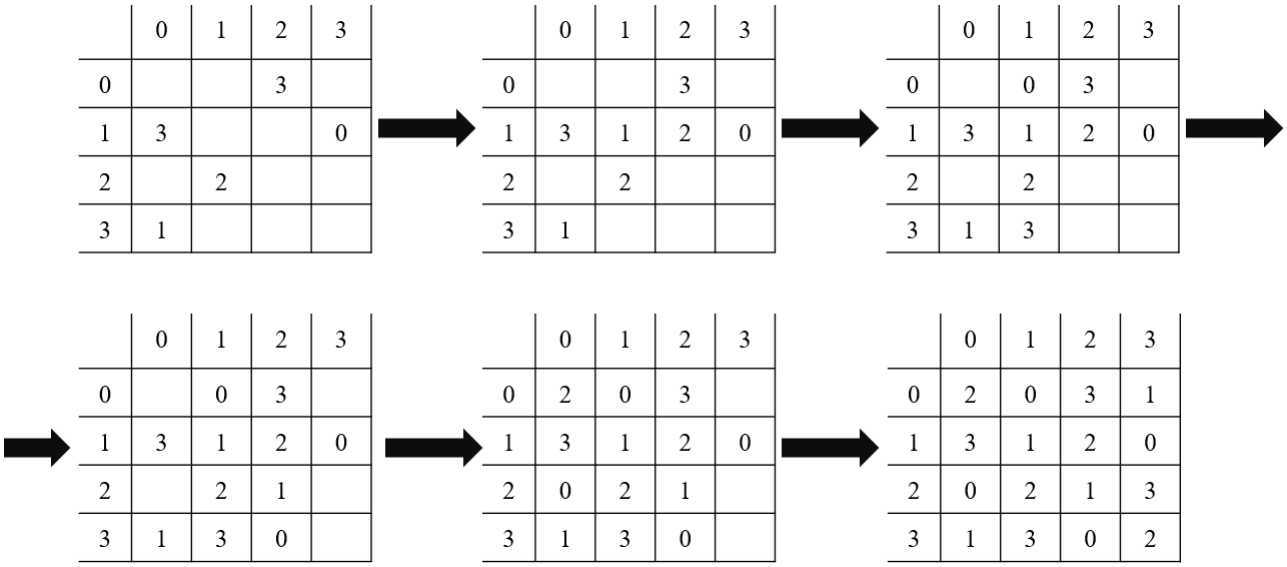



Рисунок 3.6 – Заповнення латинського квадрату маючи трансверсаль та один довільний елемент

Маючи будь який частково заповнений ключ на основі латинського квадрату 4-го порядку, у якому заповнено 5 комірок з яких 4 утворюють трансверсаль, а 5 будь який довільний елемент, можна буде однозначно відновити секретний ключ.

Згідно твердження 2.2.2 отримавши частково заповнений ключ у якому заповнені 6 комірок типу 2+2+1+1, які не утворюють трансверсаль, то можна однозначно відновити секретний ключ у вигляді латинського квадрату.

Отримавши квадрат у якому заповнено 6 комірок $k_{01} = 0, k_{02} = 3, k_{03} = 1, k_{12} = 1, k_{31} = 2, k_{32} = 0$, типу 2+2+1+1, дані заповнені комірки не утворюють трансверсаль. Обравши першу комірку для заповнення $k_{22} = 2$, оскільки у другому стовпці ця комірка є єдиною незаповненою і вона має однозначне заповнення. Наступні комірки для заповнення були обрані з першого стовпця, через те, що вже є заповнено 2 елементи. У першому рядку присутня комірка із значенням $k_{12} = 1$, тому в комірці $k_{11} = 3$, а комірка $k_{21} = 1$, заповнена однозначно як останній незаповнений елемент в першому стовпці. Наступними комірками було обрано $k_{13}$ та $k_{10}$, тому що у першому рядку заповнено 2

елементи. Комірка $k_{13} = 2$, оскільки у нульовому стовпці присутнє значення комірки 2. Тому $k_{10} = 0$, як останній незаповнений елемент першого рядка. У нульовому рядку було обрано та заповнено комірки $k_{20} = 3$ та $k_{30} = 1$, тому, що у другому рядку присутнє значення $k_{21} = 1$, тому у другому рядку не може бути ще однієї комірки із значенням 1, $k_{20}$ заповнено однозначно як останній незаповнений елемент в нульовому стовпці. Аналогічним чином заповнено комірки $k_{23} = 0$ та $k_{33} = 3$, як останні незаповнені елементи.

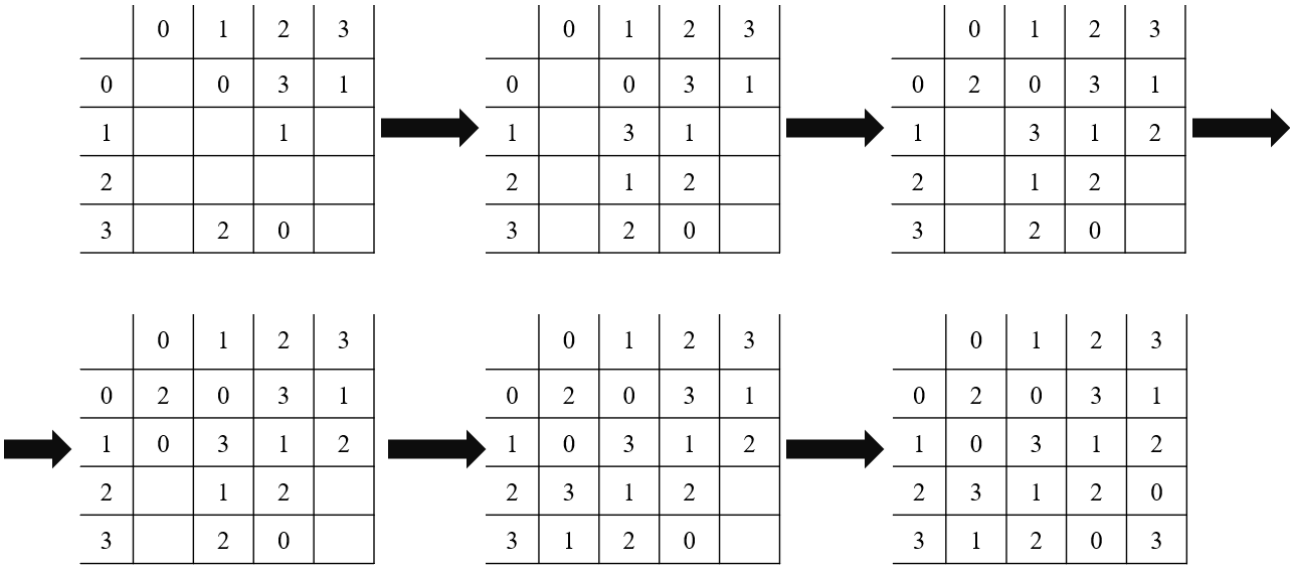



Рисунок 3.7 – Заповнення часткового латинського квадрату 2+2+1+1

Згідно твердження 2.2.3 отримавши частково заповнений латинський квадрат у якому заповнено довільних 7 комірок за типом 3+2+1+1 або 2+2+2+1, то такий латинський квадрат має однозначне заповнення.

Отримавши частково заповнений секретний ключ у вигляді латинського квадрату 4-го порядку. Маючи відомі комірки $k_{00} = 2, k_{10} = 3, k_{11} = 0, k_{13} = 2$, $k_{23} = 0, k_{31} = 1, k_{32} = 2$, користуючись алгоритмом відновимо ключ. Обравши першу комірку для заповнення, та враховуючи наявне заповнення, маємо $k_{21} = 2$, оскільки у нульовому рядку присутня комірка із значенням 2, $k_{01} = 3$, як остання незаповнена комірка у першому стовпці. Наступною коміркою було обрано $k_{12} = 1$, тому, що єдина незаповнена комірка в першому рядку. Наступним кроком було відновлено нульовий стовпець та третій рядок

відповідними значеннями $k_{20} = 1, k_{30} = 0, k_{33} = 3,$ оскільки в інакшому заповнені виникає конфлікт, а саме елементи комірок будуть повторюватись. $k_{22} = 3,$ тому, що, це остання незаповнена комірка у другому рядку. $k_{02} = 0,$ та $k_{03} = 2,$ заповнені однозначно як останні незаповнені комірки в другому та третьому стовпці відповідно. Результат заповнення відображено на рис 3.8.

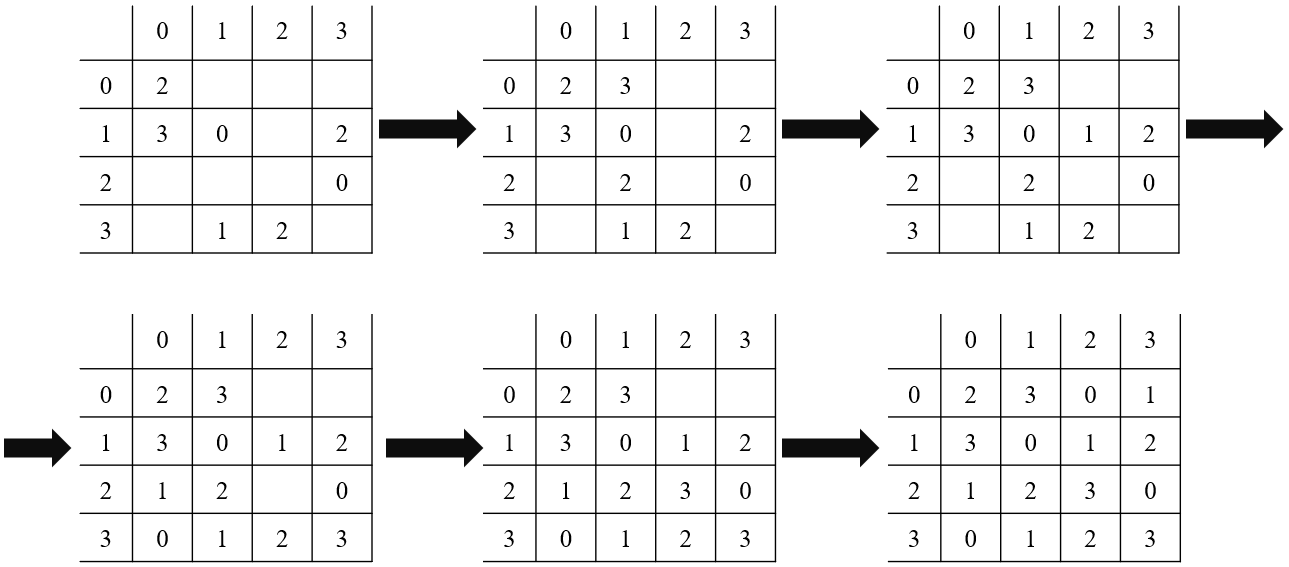



Рисунок 3.8 – Заповнення часткового латинського квадрату 3+2+1+1

Використовуючи алгоритм відновлення, аналогічним чином відновлюється секретний ключ представлений латинським квадратом 4-го порядку для часткового заповнення типу 2+2+2+1.

Отримавши частково заповнений ключ у вигляді латинського квадрату, де $k_{02} = 1, k_{03} = 2, k_{11} = 1, k_{21} = 3, k_{22} = 4, k_{32} = 3, k_{33} = 4.$ Першою коміркою було заповнено $k_{12} = 2$ з другого стовпця, так як останній незаповнений елемент заповнюється однозначно. Наступним кроком було відновлено комірки третього стовпця, $k_{13} = 3$ та $k_{23} = 1,$ так як комірки з елементами 2 та 4 представлені у стовпці, а у другому рядку присутні елемент із значенням 3. Далі було відновлено комірки першого стовпця, таким чином отримали $k_{01} = 4, k_{31} = 2,$ оскільки при інакшому заповнені було б отримано конфлікт. Нульовий стовпець відновлено однозначно оскільки присутні всі

елементи рядків окрім нульових, тоді маємо: $k_{00} = 3, k_{01} = 4, k_{02} = 2, k_{03} = 1$. Відновлення зображено на рис. 3.9.

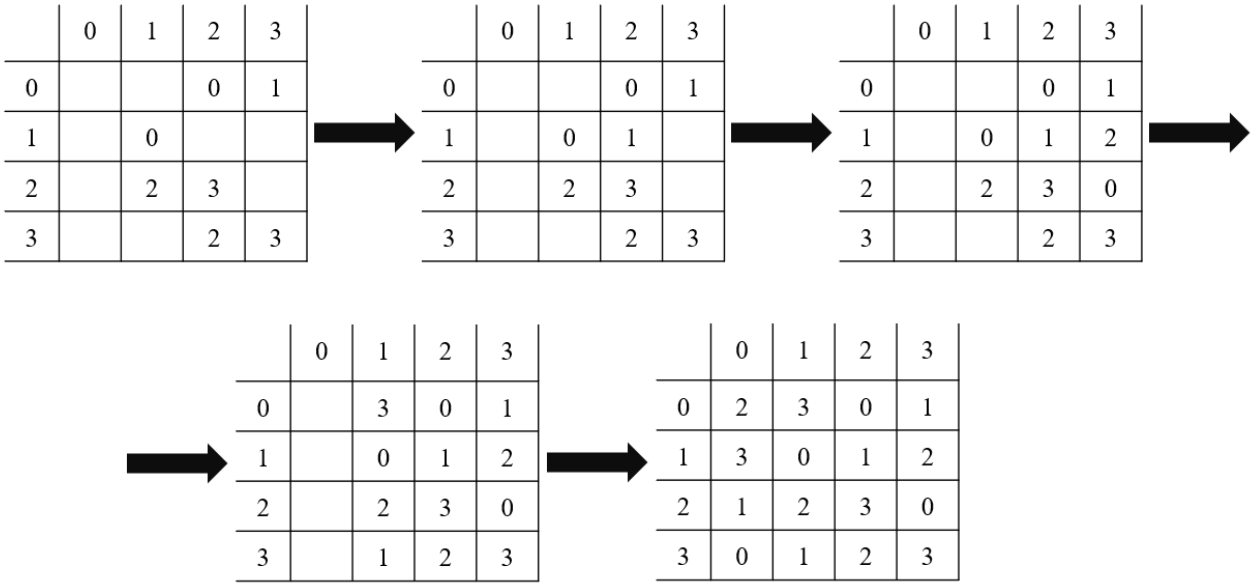



Рисунок 3.9 – Заповнення часткового латинського квадрату 2+2+2+1

Згідно твердження 2.2.4 отримавши частково заповнений латинський квадрат у якому заповнено довільних 7 комірок за типом 3+2+2, то такий латинський квадрат має однозначне заповнення.

Отримавши частково заповнений ключ, який представлений у вигляді латинського квадрату 4-го порядку в якому заповнено 7 комірок за типом 3+2+2, де $k_{00} = 3, k_{01} = 0, k_{02} = 2, k_{13} = 3, k_{20} = 2, k_{22} = 3, k_{32} = 0$. Користуючись алгоритмом відновимо секретний ключ. Оскільки один з елементів повторюється 3 рази, то відповідно комірка $k_{31} = 3$, тому, що тільки у третьому рядку та першому стовпці відсутня комірка з елементом 3. Наступними обрано комірки $k_{03} = 1$ та $k_{32} = 1$, як останні незаповнені комірки в нульовому рядку та другому стовпці відповідно. Наступним кроком було заповнено комірку $k_{23} = 0$, оскільки у третьому рядку вже присутня комірка з елементом 0, а комірка $k_{33} = 2$, заповнена автоматично як остання незаповнена клітинка стовпця. Аналогічним чином було однозначно заповнено комірки $k_{30} = 1, k_{10} = 0$ та $k_{11} = 2$, як останні незаповнені клітинки рядів та стовпців. Заповнення відображено на рис. 3.10.

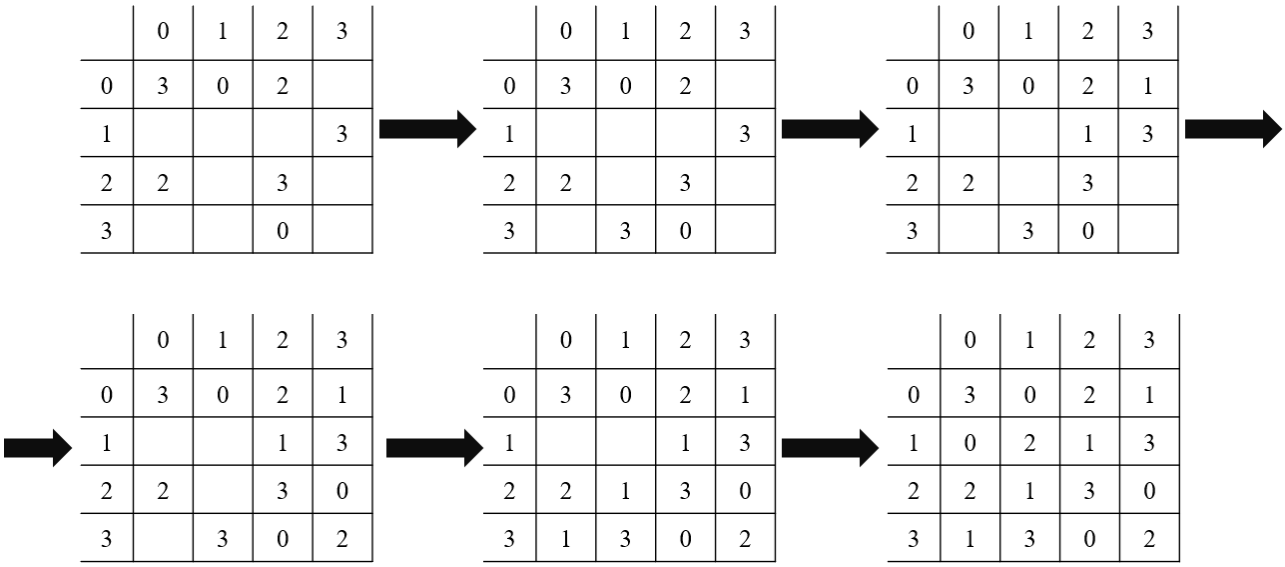



Рисунок 3.10 – Заповнення часткового латинського квадрату 3+2+2

Згідно твердження 2.2.5 отримавши частково заповнений латинський квадрат у якому заповнено довільних 8 комірок за типом 3+3+2 або 4+2+2, то такий латинський квадрат має однозначне заповнення.

Отримавши частково заповнений ключ представлений латинським квадратом 4-го порядку у якому заповнено 8 комірок за типом 3+3+2, використовуючи алгоритм відновимо секретний ключ. Маючи відкриті комірки $k_{01} = 3, k_{03} = 0, k_{10} = 2, k_{20} = 3, k_{21} = 2, k_{22} = 0, k_{30} = 0, k_{33} = 2$. Обравши першу комірку $k_{00} = 1$, ця комірка відновлюється автоматично оскільки вона остання в нульовому стовпці. Наступним кроком обрано та заповнено $k_{23} = 1$, оскільки комірка остання незаповнена комірка в другому рядку. Наступною коміркою $k_{11} = 0$, тому, що у третьому рядку вже присутня комірка з елементом 0, тому заповнено однозначно, також відновлено автоматично комірку $k_{31} = 1$, як останній незаповнений елемент. Комірки $k_{02} = 2, k_{13} = 3$, заповнені однозначно оскільки варіанти їх заповнень однозначні, як останні незаповнені комірки в нульовому рядку та третьому стовпці відповідно. Остання незаповнена комірка заповнюється однозначно $k_{12} = 1$. Результат відновлення відображено на рис. 3.11

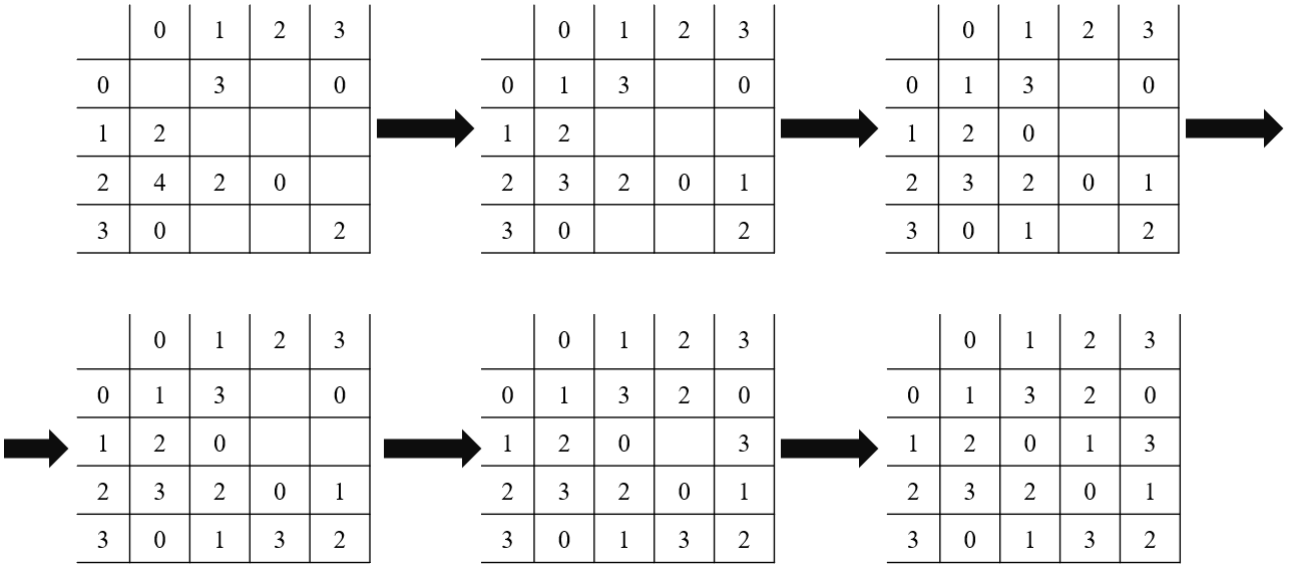



Рисунок 3.11 – Заповнення часткового латинського квадрату 3+3+2

Отримавши частково заповнений ключ представлений латинським квадратом 4-го порядку у якому заповнено 8 комірок за типом 4+2+2, використовуючи алгоритм відновимо секретний ключ. Маючи відкриті комірки $k_{00} = 1, k_{01} = 3, k_{03} = 0, k_{12} = 1, k_{20} = 3, k_{22} = 0, k_{23} = 1, k_{31} = 1.$ Обравши першу комірку $k_{02} = 3$, оскільки у нульовому рядку заповнені, це єдиний незаповнений елемент. Наступним елементом обрано $k_{21} = 2$, оскільки в третьому рядку це єдиний незаповнений елемент. Комірки $k_{11} = 0$ та $k_{32} = 3$, заповнені однозначно оскільки в першому та другому стовпці заповнені 3 комірки. $k_{13} = 3$, тому, що у третьому рядку та першому стовпці присутні комірки зі значенням 3. Наступним етапом було заповнено комірку $k_{10} = 2$, оскільки у першому рядку заповнено всі комірки без виникнення конфліктів заповнення. $k_{33} = 2$ обрано та заповнено через наявність лише одного варіанту заповнення, аналогічно заповнено $k_{30} = 0$. Результат заповнення відображено на рис. 3.12.

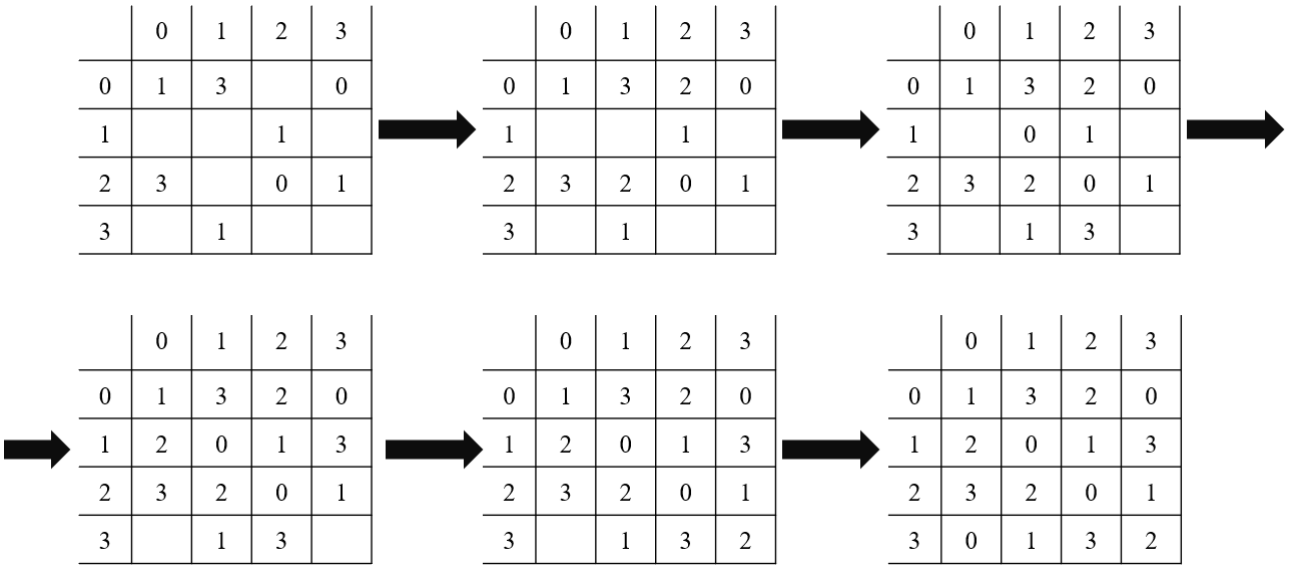



Рисунок 3.12 – Заповнення часткового латинського квадрату 4+2+2

Згідно твердження 2.2.6 отримавши частково заповнений латинський квадрат у якому заповнено довільних 8 комірок за типом 3+3+1+1, то такий латинський квадрат має однозначне заповнення.

Отримавши частково заповнений ключ, який представлений у вигляді латинського квадрату 4-го порядку в якому заповнено 8 комірок за типом 3+3+1+1, де $k_{01} = 1, k_{02} = 0, k_{10} = 0, k_{12} = 3, k_{21} = 3, k_{22} = 2, k_{23} = 0, k_{33} = 3$. Використовуючи алгоритм відновимо секретний ключ представлений латинським квадратом 4-го порядку. Обравши першу комірку $k_{20}$, цей елемент буде однозначно відновлений, оскільки у другом рядку всі елементи заповнено, тому $k_{20} = 1$. Комірка $k_{32} = 1$, аналогічно відновлюється через мінімальну кількість можливих варіантів заповнень. Оберемо наступну комірку $k_{00}$, оскільки у нульовому рядку заповнено дві комірки $k_{01} = 1$ та $k_{02} = 0$, а у третьому стовпці наявна комірка з елементом $k_{33} = 3$, відповідно у комірці $k_{03}$ не може бути значення елементу 3. Тому $k_{00} = 3$, а $k_{03} = 2$. У третьому стопці залишилась одна незаповнена комірка $k_{13} = 1$, яка заповнилась автоматично. Наступний комірка обрана у першому рядку, $k_{11} = 2$, вона заповнена автоматично через мінімальну кількість варіантів заповнень. Аналогічним чином

доповнено комірки $k_{30} = 2, k_{31} = 0$. Відновлення латинського квадрату відображено на рис. 3.13.

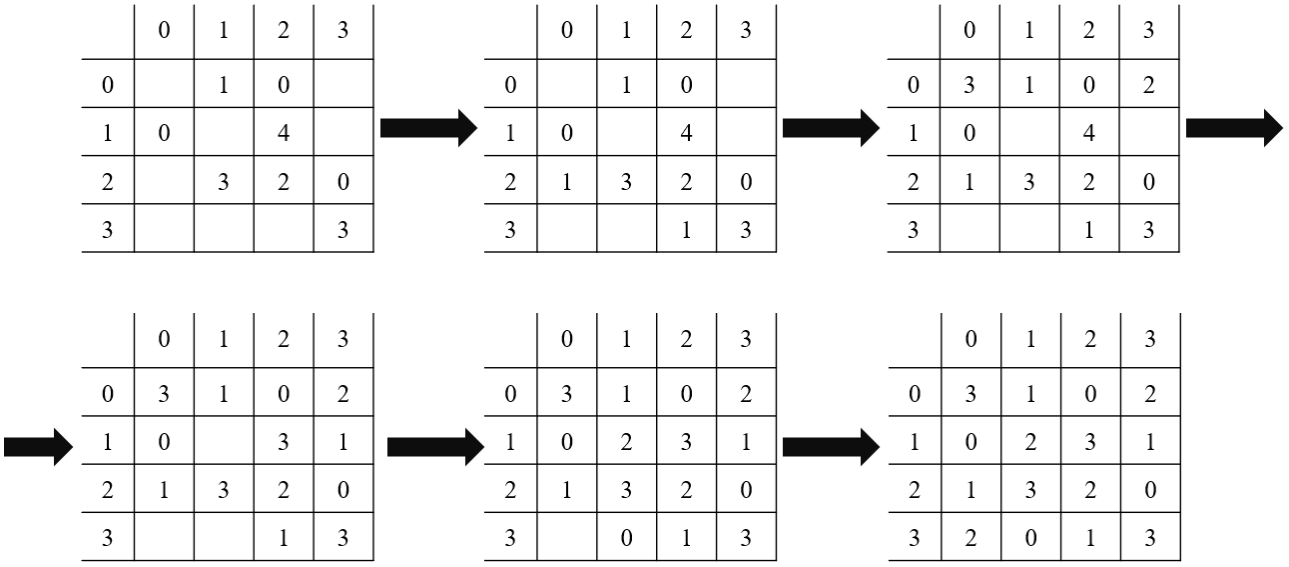



Рисунок 3.13 – Заповнення часткового латинського квадрату 3+3+1+1

Згідно твердження 2.2.7 отримавши частково заповнений латинський квадрат у якому заповнено довільних 8 комірок за типом 4+2+1+1, то такий латинський квадрат має однозначне заповнення.

Отримавши частково заповнений ключ, який представлений у вигляді латинського квадрату 4-го порядку в якому заповнено 8 комірок за типом 4+2+1+1, де $k_{00} = 2, k_{02} = 1, k_{03} = 0, k_{13} = 2, k_{21} = 2, k_{30} = 0, k_{31} = 1, k_{32} = 2$ Використовуючи алгоритм відновимо секретний ключ. Обравши першу комірку у нульовому ряду, та проаналізувавши її заповненість, маємо $k_{01} = 3$, як комірка з найменшою кількістю можливих варіантів заповнення. Наступною коміркою було обрано $k_{33} = 3$, як комірка з найменшою кількістю можливих варіантів заповнення. Подальшим кроком було обрано комірки у першому та третьому стовпці, які є останніми незаповненими комірками у цих стовпцях, а саме $k_{11} = 0$ та $k_{23} = 1$. У першому ряду було обрано комірку $k_{11}$, яка мала два можливих варіанти заповнення, але оскільки у другому стовпці присутня комірка із значенням 1, то відповідно заповнення є однозначне оскільки в інакшому заповнені виникає конфлікт, тому $k_{11} = 1$ та $k_{12} = 3$, оскільки це остання

незаповнена комірка у першому рядку. Комірки $k_{20} = 3, k_{22} = 0$, тому ще це останні незаповнені елементи у нульовому та другому стовпці. Результат відновлення відображено на рис. 3.14.

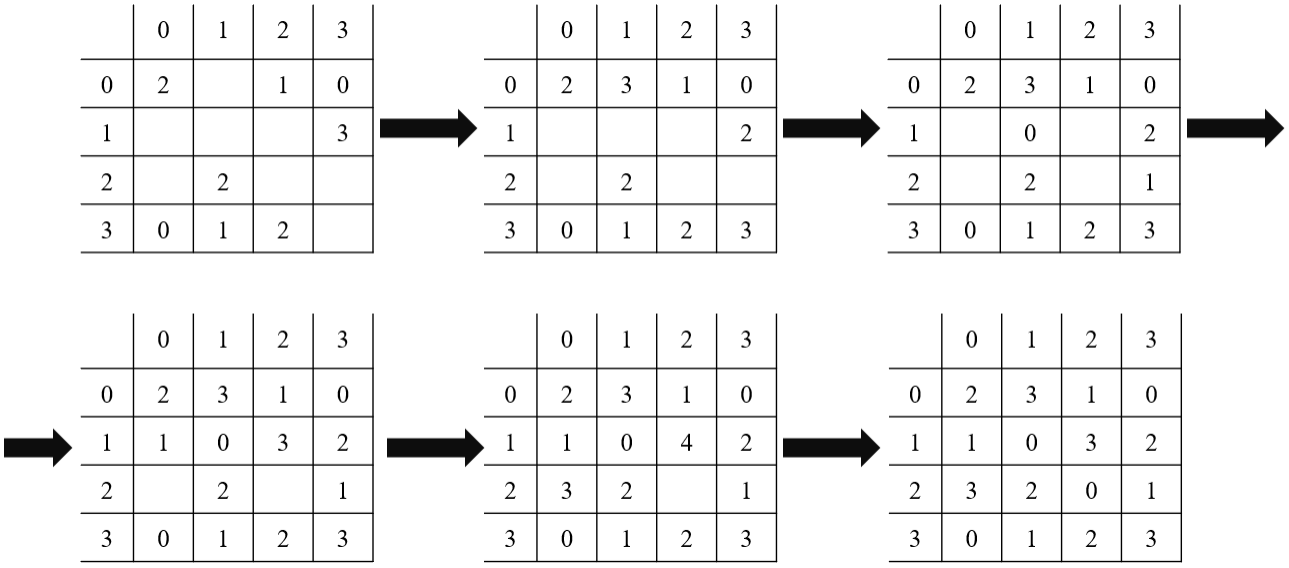



Рисунок 3.14 – Заповнення часткового латинського квадрату 4+2+1+1

Провівши аналіз заповнення часткового латинського квадрата, можна зробити висновок, що у отримавши певний набір відкритих комірок, можливо однозначно його відтворити, що дозволяє нам зберігати у пам’яті лише деяку кількість комірок і їх розташування замість повного квадрату.

# 4 ЕКОНОМІЧНА ЧАСТИНА

Метою економічної частини магістерської кваліфікаційної роботи є обґрунтування економічної доцільності розробленого методу криптоаналізу на основі часткових латинських квадратів.

Дослідження на тему «Методи криптоаналізу на основі часткових латинських квадратів» може бути віднесена до наукових досліджень і спрямоване на вирішення наукових проблем, пов’язаних із практичним застосуванням. Основою дослідження є отримання наукового результату, який в подальшому дозволить розробити програмний продукт в сфері кібербезпеки, а саме в розділі криптології.

Для виконання поставленої мети необхідно:

- провести науковий аудит досліджень, тобто встановити її науковий рівень та значимість;
- провести планування витрат на проведення наукових досліджень;
- здійснити розрахунок рівня важливості наукового дослідження та перспективності, визначити ефективність наукових досліджень.

## 1.1 Оцінювання наукового ефекту

Основними ознаками наукового ефекту науково-дослідної роботи є новизна роботи, рівень її теоретичного опрацювання, перспективність, рівень розповсюдження результатів, можливість реалізації. Науковий ефект НДР на тему «Метод криптоаналізу на основі часткових латинських квадратів», можна охарактеризувати двома показниками: ступенем наукової новизни та рівнем теоретичного опрацювання.

Значення показників ступеня новизни і рівня теоретичного опрацювання науково-дослідної роботи в балах наведено в табл. 4.1 та 4.2.

Таблиця 4.1 – Показники ступеня новизни науково-дослідної роботи виставлені експертами

| Ступінь новизни | Характеристика ступеня новизни | Значення ступеня новизни, бали | | |
|---|---|---|---|---|
| | | Експерти | | |
| 1 | 2 | 3 | | |
| Принципово нова | Робота якісно нова за постановкою задачі і ґрунтується на застосуванні оригінальних методів дослідження. Результати дослідження відкривають новий напрям в даній галузі науки і техніки. Отримані принципово нові факти, закономірності; розроблена нова теорія. Створено принципово новий пристрій, спосіб, метод | 0 | 0 | 0 |
| Нова | Отримана нова інформація, яка суттєво зменшує невизначеність наявних значень (поновому або вперше пояснені відомі факти, закономірності, впроваджені нові поняття, розкрита структура змісту). Проведено суттєве вдосконалення, доповнення і уточнення раніше досягнутих результатів | 45 | 0 | 0 |
| Відносно нова | Робота має елементи новизни в постановці задачі і методах дослідження. Результати дослідження систематизують і узагальнюють наявну інформацію, визначають шляхи подальших досліджень; вперше знайдено зв’язок (або знайдено новий зв’язок) між явищами. В принципі відомі положення розповсюджені на велику кількість об’єктів, в результаті чого знайдено ефективне рішення. Розроблені більш прості способи для досягнення відомих результатів. Проведена часткова раціональна модифікація (з ознаками новизни) | 0 | 38 | 37 |
| Традиційна | Робота виконана за традиційною методикою. Результати дослідження мають інформаційний характер. Підтверджені або поставлені під сумнів відомі факти та твердження, які потребують перевірки. Знайдено новий варіант рішення, який не дає суттєвих переваг в порівнянні з існуючим | 0 | 0 | 0 |
| Не нова | Отримано результат, який раніше зафіксований в інформаційному полі, та не був відомий авторам | 0 | 0 | 0 |
| **Середнє значення балів експертів** | | **40** | | |

Згідно отриманого середнього значення балів виставлених експертами ступінь новизни характеризується, як відносно нова, тобто результати досліджень систематизують та узагальнюють інформацію, розроблено більш прості способи досягнення відомих результатів.

Таблиця 4.2 – Показники рівня теоретичного опрацювання науково-дослідної роботи виставлені експертами

| Характеристика рівня теоретичного опрацювання | Значення показника рівня теоретичного опрацювання, бали | | |
|---|---|---|---|
| | Експерти | | |
| | 1 | 2 | 3 |
| Відкриття закону, розробка теорії | 0 | 0 | 0 |
| Глибоке опрацювання проблеми: багатоаспектний аналіз зв'язків, взаємозалежності між фактами з наявністю пояснень, наукової систематизації з побудовою евристичної моделі або комплексного прогнозу | 65 | 0 | 0 |
| Розробка способу (алгоритму, програми), пристрою, отримання нової речовини | 0 | 58 | 50 |
| Елементарний аналіз зв'язків між фактами та наявною гіпотезою, класифікація, практичні рекомендації для окремого випадку тощо | 0 | 0 | 0 |
| Опис окремих елементарних фактів, викладення досвіду, результатів спостережень, вимірювань тощо | 0 | 0 | 0 |
| **Середнє значення балів експертів** | **57,6** | | |

Згідно отриманого значення балів експертів рівень теоретичного опрцювання науково-дослідницької роботи характеризується, як розробка способу (алгоритму, програми), пристрою, отримання нової речовини.

Показник, який характеризує науковий ефект, визначається за формулою:

$$E_{\text{нау}} = 0{,}6 \cdot k_{\text{нов}} + 0{,}4 \cdot k_{\text{теор}}, \qquad (4.1)$$

де $k_{\text{нов}}, k_{\text{теор}}$- показники ступеня новизни та рівня теоретичного опрацювання науково-дослідної роботи, $k_{\text{нов}} = 40,, k_{\text{теор}} = 57{,}6$ балів;

*0,6 та 0,4* – питома вага (значимість) показників ступеня новизни та рівня теоретичного опрацювання науково-дослідної роботи.

$$E_{\text{нау}} = 0{,}6 \cdot k_{\text{нов}} + 0{,}4 \cdot k_{\text{теор}} = 0{,}6 \cdot 40 + 0{,}4 \cdot 57{,}6 = 47{,}04 \text{ балів}.$$

Визначення характеристики показника $E_{\text{нау}}$ проводиться на основі висновків експертів виходячи з граничних значень, які наведені в табл. 5.3.

Таблиця 4.3 – Граничні значення показника наукового ефекту

| Досягнутий рівень показника | Кількість балів |
|---|---|
| Високий | 70…100 |
| Середній | 50…69 |
| Достатній | 15…49 |
| Низький (помилкові дослідження) | 1…14 |

Відповідно до визначеного рівня наукового ефекту проведеної науково-дослідної роботи на тему «Метод криптоаналізу на основі часткових латинських квадратів», даний рівень становить 47,04 балів і відповідає статусу - достатній рівень. Тобто у даному випадку можна вести мову про потенційну фактичну ефективність науково-дослідної роботи.

### 1.2 Розрахунок витрат на здійснення науково-дослідної роботи

4.2.1 Розрахунок витрат, що стосуються виконавців розробки методу криптоаналізу на основі часткових латинських квадратів.

Основна заробітна плата дослідників

Витрати на основну заробітну плату дослідників ($З_о$) розраховуємо у відповідності до посадових окладів працівників, за формулою:[21]

$$З_о = \sum_{i=1}^{k} \frac{M_{ni} \cdot t_i}{T_p}, \quad (4.2)$$

де $k$ - кількість посад дослідників залучених до процесу досліджень;

$M_{ni}$ – місячний посадовий оклад конкретного дослідника, грн;

$t_i$ - число днів роботи конкретного дослідника, дн;

$T_p$- середнє число робочих днів у місяці, $T_p = 22$ дні.

$$З_о = 17169{,}00 \cdot 20 \,/\, 22 = 15608{,}18 \; \textit{грн.}$$

Проведені розрахунки зведемо до таблиці.

Таблиця 4.4 – Витрати на заробітну плату дослідників

| Найменування посади | Місячний посадовий оклад, грн | Оплата за робочий день, грн | Число днів роботи | Витрати на заробітну плату, грн |
|---|---|---|---|---|
| Науковий керівник дослідної роботи | 17169,00 | 780,04 | 20 | 15608,18 |
| Науковий співробітник | 9149,00 | 415,86 | 20 | 8317,27 |
| Всього | | | | 23925,45 |

Додаткова заробітна плата дослідників

Додаткову заробітну плату розраховуємо як 10 … 12% від суми основної заробітної плати дослідників та робітників за формулою: [21]

$$З_{дод} = \left(З_о + З_р\right)\frac{Н_{дод}}{100\%}, \quad (4.5)$$

де $Н_{дод}$ – норма нарахування додаткової заробітної плати. Приймемо 12%.

$$З_{дод} = 23925{,}45 \cdot 12/100\% = 2871{,}05 \text{ грн.}$$

4.2.2 Відрахування на соціальні заходи

Нарахування на заробітну плату дослідників та робітників розраховуємо як 22% від основної суми основної та додаткової заробітної плати дослідників та робітників за формулою:[21]

$$З_н = \left(З_о + З_р + З_{дод}\right)\frac{Н_{зп}}{100\%}, \quad (4.6)$$

де $Н_{зп}$ – норма нарахування на заробітну плату. Станом на грудень 2024 року це 22%.

$$З_н = (23925{,}45 + 2871{,}05) \cdot \frac{22}{100\%} = 5895{,}23 \text{ грн.}$$

4.2.3 Сировина та матеріали

Витрати на матеріали (М), у вартісному виражені розраховуються окремо по кожному виду матеріалів за формулою:[21]

$$M = \sum_{j=1}^{n} H_j \cdot Ц_j \cdot K_j - \sum_{j=1}^{n} B_j \cdot Ц_{вj}\,, \quad (4.7)$$

де $H_j$ – норма витрат матеріалу j-го найменування, кг;

$n$– кількість видів матеріалів;

Ц$_j$ – вартість матеріалу j-го найменування, грн/кг;

К$_j$ – коефіцієнт транспортних витрат, (Кj = 1,1 … 1,15);

В$_j$ – маса відходів j-го найменування, кг;

Ц$_{вj}$ – вартість відходів j-го найменування, грн/кг.

$M_1 = 4{,}0 \cdot 211{,}00 \cdot 1{,}1 = 928{,}40$ *грн.*

Проведені розрахунки зведемо до таблиці.

Таблиця 4.5 – Витрати на матеріали

| Найменування матеріалу, марка, тип, сорт | Ціна за 1 кг, грн | Норма витрат, кг | Вартість витраченого матеріалу, грн |
|---|---|---|---|
| Папір Офісний А4 500 | 211,00 | 4,0 | 928,40 |
| Канцелярське приладдя | 327,00 | 3,0 | 1079,10 |
| Картридж для принтера | 2820,00 | 2,0 | 6204,00 |
| Flesh-пам'ять 128 GB | 319,00 | 1,0 | 350,90 |
| Всього | | | 8562,4 |

4.2.4 Амортизація обладнання, програмних засобів та приміщень

Амортизаційна відрахування по кожному виду обладнання, приміщень та програмному забезпеченню тощо, розраховуємо з використанням прямолінійного методу амортизації за формулою:[21]

$$A_{\text{обл}} = \frac{\text{Ц}_\text{б}}{\text{Т}_\text{в}} \cdot \frac{t_{\text{вик}}}{12}, \qquad (4.8)$$

де Ц$_б$ – балансова вартість обладнання, програмних засобів, приміщень тощо, які використовувались для проведення досліджень, грн;

$t_{вик}$ – термін використання обладнання, програмних засобів, приміщень під час досліджень, місяців;

$Т_в$ – строк корисного використання обладнання, програмних засобів, приміщень тощо, років.

$А_{обл} = (6799{,}00 \cdot 1) / (5 \cdot 12) = 113{,}31$ *грн.*

Проведені розрахунки зведемо до таблиці.

Таблиця 4.6 – Амортизаційні відрахування по кожному виду обладнання

| Найменування обладнання | Балансова вартість, грн | Строк корисного використання, років | Термін використання обладнання, місяців | Амортизаційні відрахування, грн |
|---|---|---|---|---|
| Принтер HP LazerJet M111w | 6799,00 | 5 | 1 | 113,31 |
| Комп'ютер HUAWEI MateBook d15 | 24990,00 | 3 | 1 | 694,16 |
| Всього | | | | 807,47 |

4.2.5 Паливо та енергія для науково-виробничих цілей

Витрати на силову електроенергію $B_e$ розраховуємо за формулою:[21]

$$B_e = \sum_{i=1}^{n} \frac{W_{yi} \cdot t_i \cdot Ц_e \cdot K_{впі}}{\eta_i}, \quad (4.9)$$

де $W_{yi}$ – встановлена потужність обладнання на визначеному етапі розробки, кВт;

$t_i$ – тривалість роботи обладнання на етапі дослідження, год;

$Ц_e$ – вартість 1 кВт-години електроенергії, грн (вартість електроенергії визначається за даними енергопостачальної компанії), приймемо $Ц_e = 8{,}48$ грн;

$K_{впі}$ – коефіцієнт, що враховує використання потужності, $K_{впі} < 1$;

$\eta_i$ – коефіцієнт корисної дії обладнання $\eta_i < 1$.

$B_e = 0{,}42 \cdot 5{,}0 \cdot 8{,}48 \cdot 0{,}95/0{,}97 = 17{,}44$ *грн.*

Проведені розрахунки зведемо до таблиці.

Таблиця 4.7 – Витрати на електроенергію

| Найменування обладнання | Встановлена потужність, кВт | Тривалість роботи, год | Сума, грн |
|---|---|---|---|
| Принтер HP LazerJet M111w | 0,42 | 5,0 | 17,44 |
| Комп'ютер HUAWEI MateBook d15 | 0,25 | 160,0 | 332,20 |
| Всього | | | 349,64 |

Після проведення розрахунків, вартість науково-дослідної роботи становить:

$$B = 23925{,}45 + 2871{,}05 + 5895{,}23 + 8562{,}4 + 807{,}47 + 349{,}64 =$$
$$= 42411{,}24 \text{ грн.}$$

### 1.3 Розрахунок витрат на здійснення науково-дослідної роботи

Оцінювання та доведення ефективності виконання науково-дослідної роботи фундаментального чи пошукового характеру є достатньо складним процесом і часто базується на експертних оцінках, тому має вірогідний характер.

Для обґрунтування доцільності виконання науково-дослідної роботи на тему «Метод криптоаналізу на основі часткових латинських квадратів» використовується спеціальний комплексний показник, що враховує важливість, результативність роботи, можливість впровадження її результатів у виробництво, величину витрат на роботу.

Комплексний показник $K_p$ рівня науково-дослідної роботи може бути розрахований за формулою:

$$K_p = \frac{I^n \cdot T_C \cdot R}{B \cdot t}, \qquad (4.10)$$

де $I$ – коефіцієнт важливості роботи. Приймемо $I = 3$;

$n$ – коефіцієнт використання результатів роботи; $n = 0$, коли результати роботи не будуть використовуватись; $n = 1$, коли результати роботи будуть використовуватись частково; $n = 2$, коли результати роботи будуть використовуватись в дослідно-конструкторських розробках; $n = 3$, коли результати можуть використовуватись навіть без проведення дослідно-конструкторських розробок. Приймемо n=2;

$T_C$ – коефіцієнт складності роботи. Приймемо $T_C = 2$;

$R$ – коефіцієнт результативності роботи; якщо результати роботи плануються вище відомих, то $R = 4$; якщо результати роботи відповідають відомому рівню, то $R = 3$; якщо нижче відомих результатів, то $R = 1$. Приймемо $R = 3$;

В – вартість науково-дослідної роботи, тис. грн. Приймемо В =42411,24 грн;

t – час проведення дослідження. Приймемо t = 0,08 років, (1 міс.).

Визначення показників $I, n, T_C, R, B, t$ здійснюється експертним шляхом або на основі нормативів.

$$K_p = \frac{3^2 \cdot 2 \cdot 3}{42{,}4 \cdot 0{,}08} = 15{,}9.$$

Якщо $K_p > 1$, то науково-дослідну роботу на тему «Метод криптоаналізу на основі часткових латинських квадратів» можна вважати ефективною з високим науковим, технічним і економічним рівнем.

### 4.4. Висновок до розділу

Витрати на проведення науково-дослідної роботи на тему «Метод криптоаналізу на основі часткових латинських квадратів» складають 42411,24 грн. Відповідно до проведеного аналізу та розрахунків рівень наукового ефекту проведеної науково-дослідної роботи на тему «Метод криптоаналізу на основі часткових латинських квадратів» є середній, а дослідження актуальними, рівень

доцільності виконання науково-дослідної роботи $K_p > 1$, що свідчить про потенційну ефективність з високим науковим, технічним і економічним рівнем.

# ВИСНОВКИ

У магістерській кваліфікайній роботі досліджено задачу відновлення частково заповнених латинських квадратів і визначення мінімальної кількості відомих комірок, необхідних для їх однозначного доповнення. Проведений аналіз дозволив встановити точні математичні умови для такого доповнення та запропонувати ефективні алгоритми, що забезпечують коректність і швидкість виконання.

Результати дослідження показали, що для латинських квадратів 3-го порядку мінімальне заповнення залежить від розташування відомих комірок. Зокрема, було доведено, що достатньо знати три комірки, якщо вони формують трансверсаль, або чотири комірки, якщо одна з них є довільною. Ці умови гарантують однозначне доповнення до повного латинського квадрата. Для квадратів 4-го порядку встановлено необхідність визначення мінімум восьми трансверсалей, що формують критичний набір, і запропоновано методику їх перевірки у частково заповнених квадратах.

Алгоритм, розроблений у рамках роботи, демонструє ефективність у задачах криптоаналізу та забезпечують високий рівень точності в ідентифікації умов однозначного заповнення. Дослідження також дозволило оцінити складність заповнення латинських квадратів залежно від їх порядку та специфіки початкового стану.

Отримані результати показують, що для латинських квадратів 3-го порядку достатньо зберігати лише 3 комірки, щоб однозначно відновити частково заповнений латинський квадрат, а отже апаратні витрати зменшуються у 3 рази. Аналогічно для латинських квадратів 4-го порядку достатньо зберігати 5 комірок для однозначного відновлення, а тому апаратні витрати зменшуються у 3,2 рази.

## ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. D`enes J., Keedwell A.D. Anew Authentication Scheme based in Latin Squares. Discrete Math. 1992. 162p.

2. Menezes, A.J., van Oorschot, P.C., Vanstone, S.A. "Handbook of Applied Cryptography." CRC Press, 1996.

3. Stallings, W. "Cryptography and Network Security: Principles and Practice." Prentice Hall, 2017.

4. Katz, J., Lindell, Y. "Introduction to Modern Cryptography." CRC Press, 2014.

5. Paar, C., Pelzl, J. "Understanding Cryptography: A Textbook for Students and Practitioners." Springer, 2010.

6. National Institute of Standards and Technology (NIST). "Advanced Encryption Standard (AES)." FIPS PUB 197, 2001.

7. Peter Adams, Elizabeth J. Billington, Darryn E. Bryant, and E.S. Mahmoodian The three-way intersection problem for latin squares, Discrete. Math. (to appear).

8. E.J. Billington, The intersection problem for combinatorial designs, Congr. Numer., 92 (1993), 33–54.

9. E.J. Billington and D.G. Hoffman, Trades and graphs, Graphs and Combinatorics (to appear).

10. C.J. Colbourn, M.J. Colbourn and D.R. Stinson, The computational complexity of recognizing critical sets, In Proc. First SE Asian Graph theory Colloq. Lecture Notes in Math. No. 1073, 248–253, Springer–Verlag, 1984.

11. D. Donovan, A. Howse, and P. Adams, A discussion of latin in terchanges, J. Combin. Math. Combin. Comput., 23 (1997), 161–182.

12. Крайнічук Г.В., Пилявець І.Ю., Радченко Є.В. CIP-квазігрупи 4-го порядку з оборотним елементом $x^2$ серед ізотопів групи Клейна // Збірник наук. праць Міжн. наук. конф. «Сучасні проблеми мех. та мат. – 2023», ІПММ ім. Я.С.Підстригача. Львів. 2023. – С. 285-286.

13. Семенюк О.А., Крайнічук Г.В. Умови відновлення секретоного ключа на відкритих комірках латинського квадрата //Матеріали Всеукраїнської науково-практичної інтернет-конференції "Молодь в науці: дослідження, проблеми, перспективи (МН-2025)", Вінниця, 2024 р. – Електрон. текст. дані. – 2024.

15. UMCL18G212T3. Virtual Silicon standard cell library based on the UMC L180 0.18 μm 1P6M Logic process. Вид. офіц. 2004. 1 с.

16. V.A. SHCHERBACOV, On generalisation of Markovski cryptoalgorithm. In Workshop on General Algebra, February 26-March 1, 2015

17. V.A. SHCHERBACOV, On the structure of left and right F-, SM- and E-quasigroups. J. Gen. Lie Theory Appl., 3(3): p. 197-259, 2009

18. T. A ELGAMAL, public key cryptosystem and a signature scheme based on discrete logarithms. - IEEE Transactions on Information Theory, 31(4): p.469-472, 1985.

19. В.А. Лужецький і Г.А. Крайнійчук Потоковий шифр на основі CIP-квазігруп 4-го порядку Збірник наук. праць Міжн. наук. конф. «Сучасні проблеми мех. та мат. – 2023», ІПММ ім. Я.С.Підстригача. Львів. 2023. – С. 285-286.

20. Методичні вказівки до виконання магістерських кваліфікаційних робіт зі спеціальності «Кібербезпека та захист інформації» освітньо-професійна програма «Безпека інформаційних і комунікаційних систем» / Уклад. В. А. Каплун, Л. М. Куперштейн, Ю. В. Баришев, О. П. Войтович – Вінниця : ВНТУ, 2024. 96 с.

21. В. А. Лужецький і А. В. Остапенко, «аналіз алгоритмів симетричного блокового шифрування», вип. 25, вип. 3, Трав 2013.

22. Gligoroski D., Markovski S., Kocarev L., Gusev M. Edon80: веб-сайт. URL: http://www.ecrypt.eu. org/stream/edon80p3.html (дата звернення: 07.11.2024)

23. Методичні вказівки до виконання економічної частини магістерських кваліфікаційних робіт / Уклад. : В. О. Козловський, О. Й. Лесько, В. В. Кавецький. – Вінниця : ВНТУ, 2021. – 42 с.

# ДОДАТКИ

**Додаток А**

# ПРОТОКОЛ ПЕРЕВІРКИ НАВЧАЛЬНОЇ (КВАЛІФІКАЦІЙНОЇ) РОБОТИ

Назва роботи: Метод криптоаналізу на основі часткових латинських квадратів

Автор роботи: Семенюк Олег Андрійович

Тип роботи: магістерська кваліфікаційна робота

Підрозділ кафедра захисту інформації ФІТКІ

Керівник Шелепало Галина Василівна, к.ф.-м.н., доцент

**Показники звіту подібності**

| Turnitin | |
|---|---|
| Оригінальність | 90 % |
| Загальна схожість | 10 % |

Аналіз звіту подібності (відмітити потрібне):

√ 1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.

☐ 2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її автора. Роботу направити на доопрацювання.

☐ 3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Заявляю, що ознайомлений з повним звітом подібності, який був згенерований Системою щодо роботи.

Автор роботи _____ (підпис) Олег СЕМЕНЮК (прізвище, ініціали)

Особа, відповідальна за перевірку _____ (підпис) Валентина КАПЛУН (прізвище, ініціали)

Керівник роботи _____ (підпис) Галина ШЕЛЕПАЛО (прізвище, ініціали)

**Додаток Б**

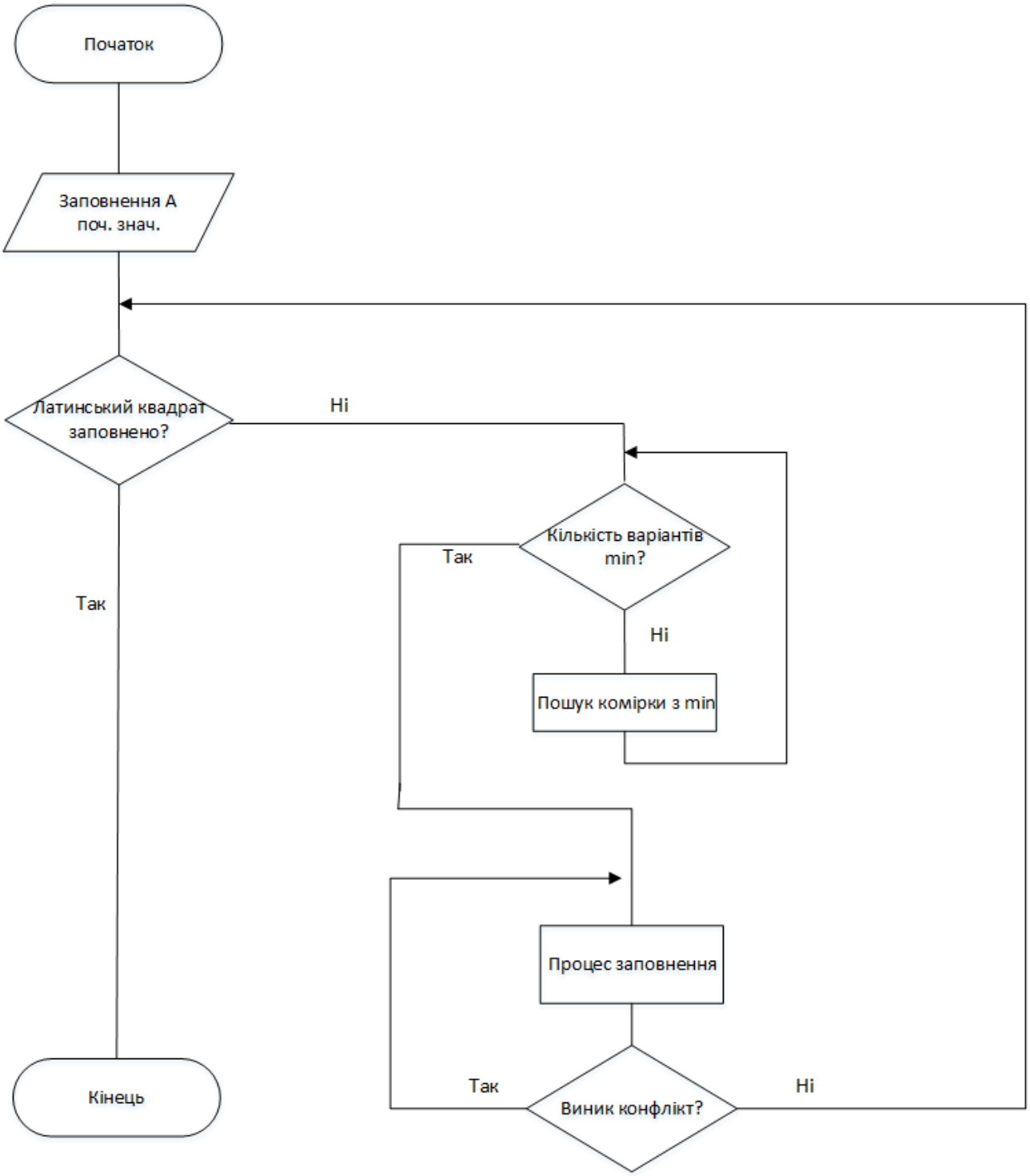
# ІЛЮСТРАТИВНА ЧАСТИНА

«Метод криптоаналізу на основі часткових латинських квадратів»

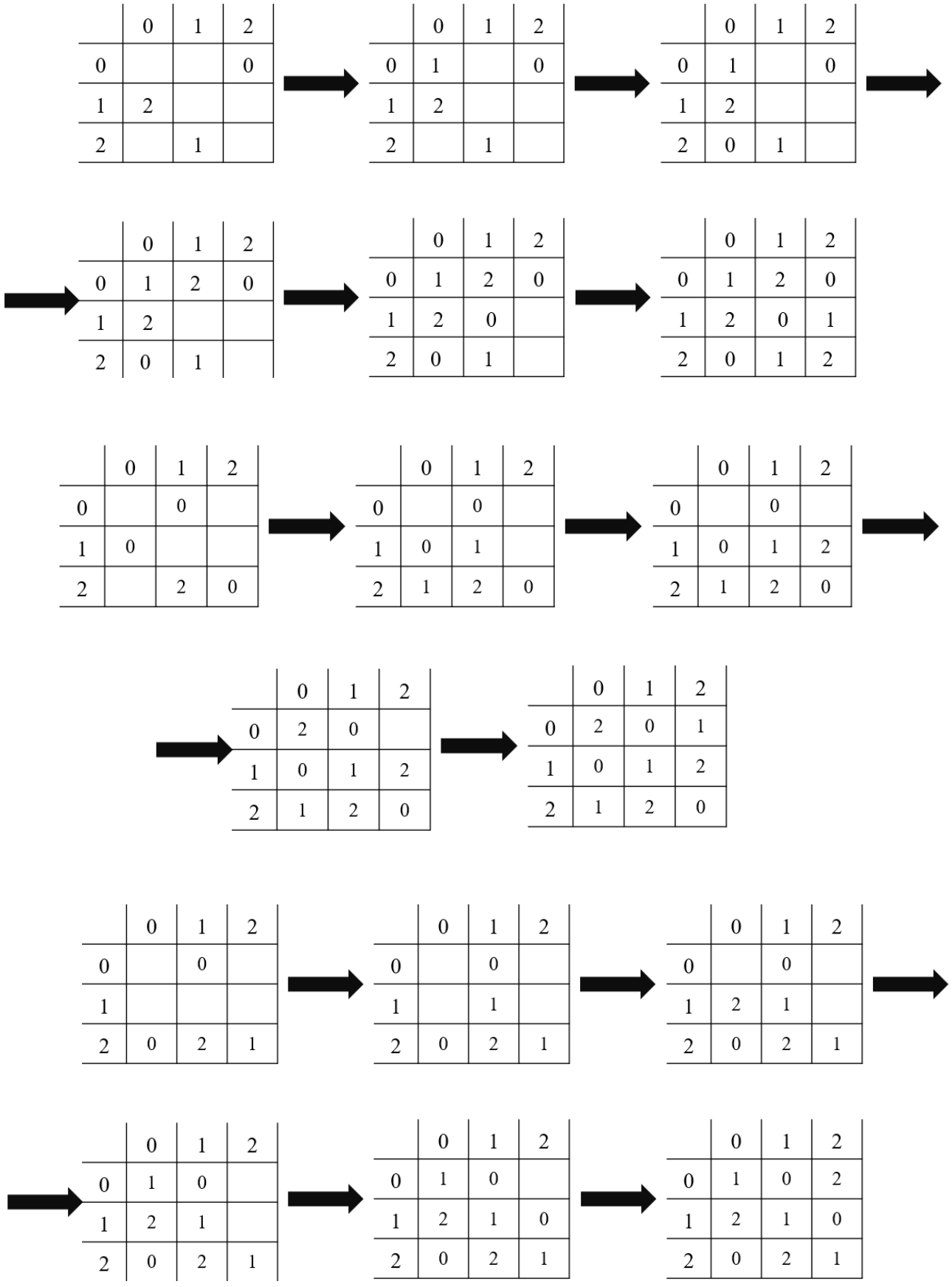
Виконав студент 2-го курсу, групи
1БС-23м
спеціальності 125 – Кібербезпека
та захист інформації
_____ Олег СЕМЕНЮК
16. 12 2024 р.

Керівник: доц. кафедри ЗІ, к.фіз-мат.н., доцент
_____ Галина ШЕЛЕПАЛО
16. 12 2024 р.

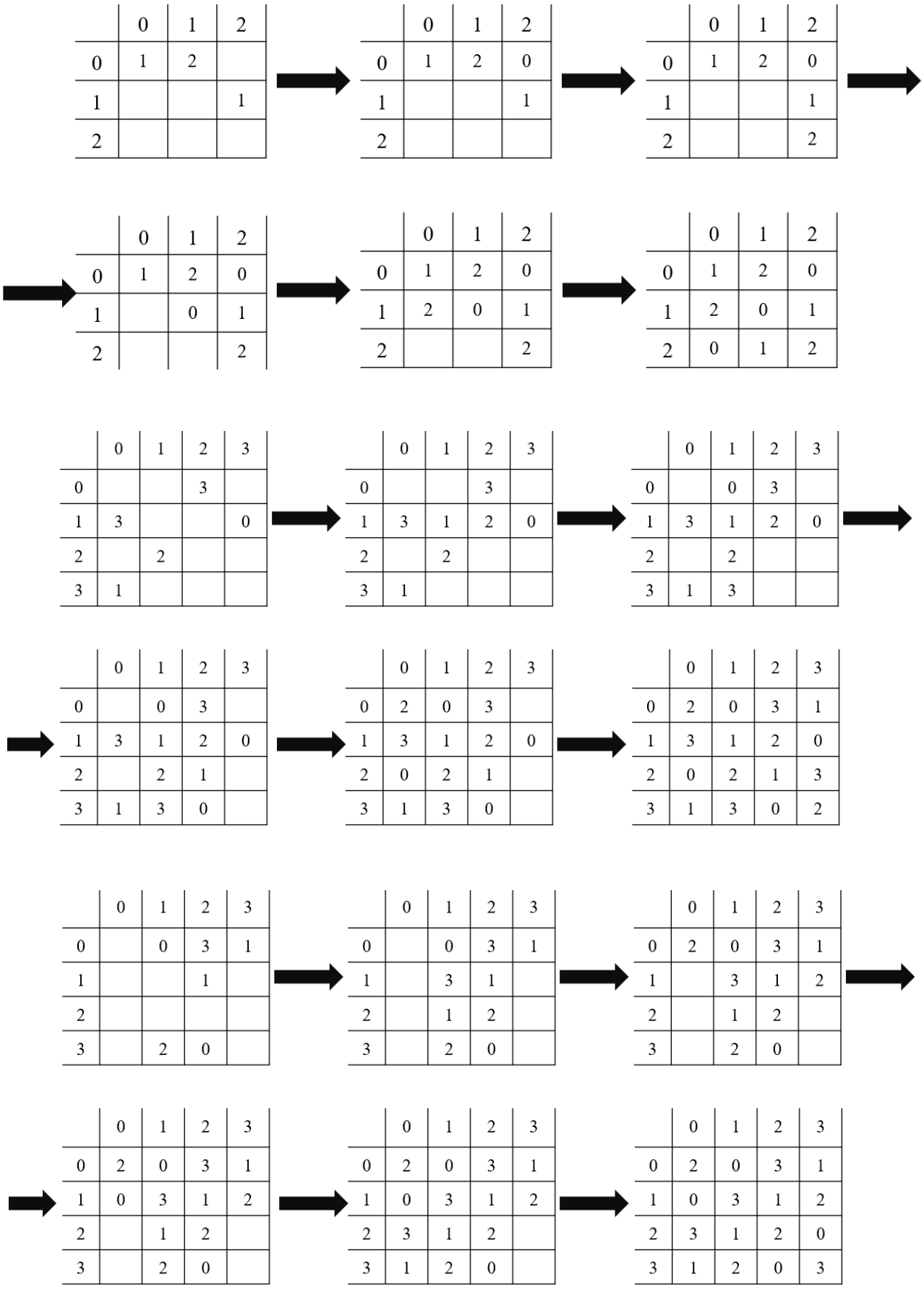
# БЛОК СХЕМА АЛГОРИТМУ ЗАПОВНЕННЯ ЛАТИНСЬКОГО КВАДРАТА



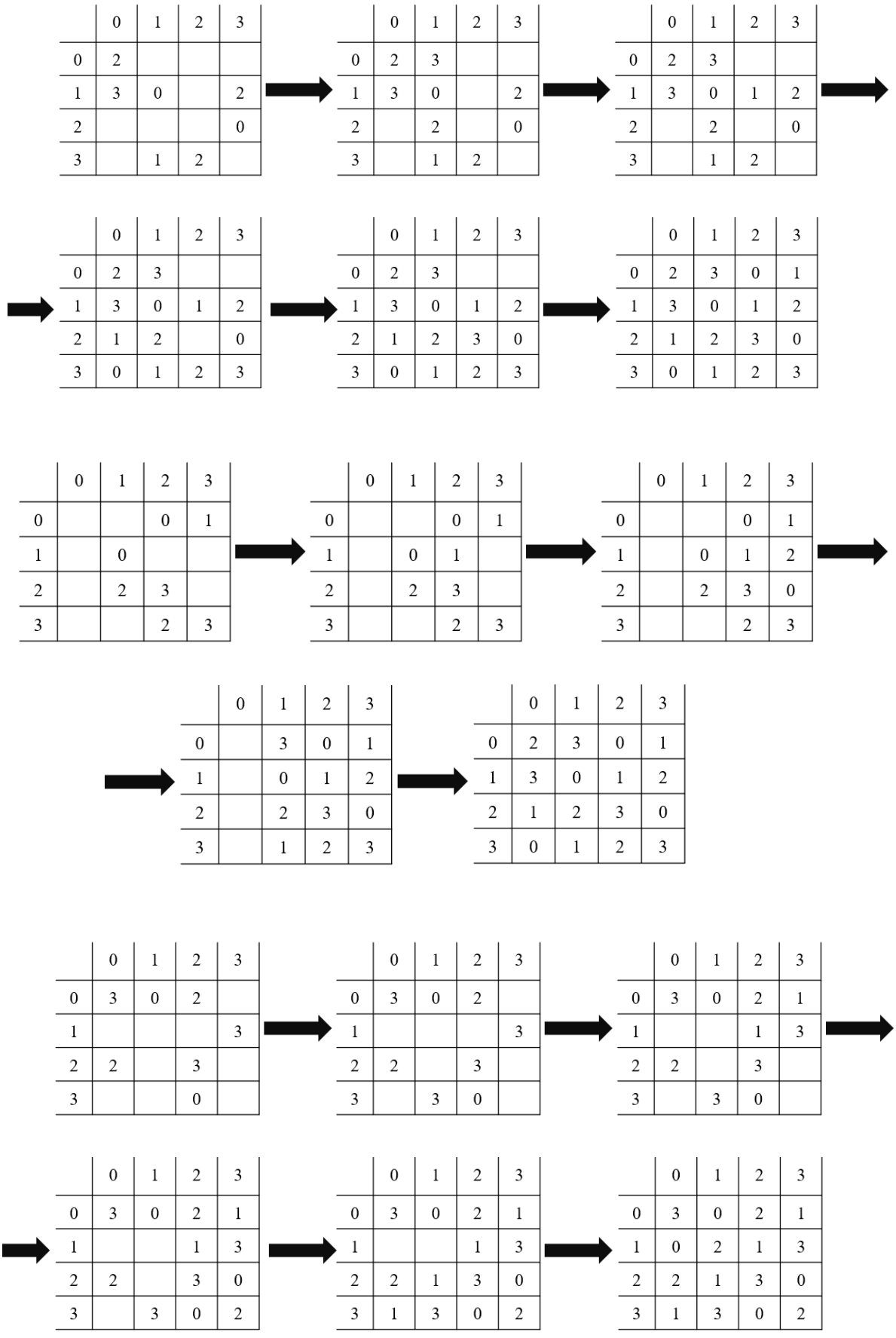
# ВІДНОВЛЕННЯ ЛАТИНСЬКИХ КВАДРАТІВ ЧАСТИНА 1



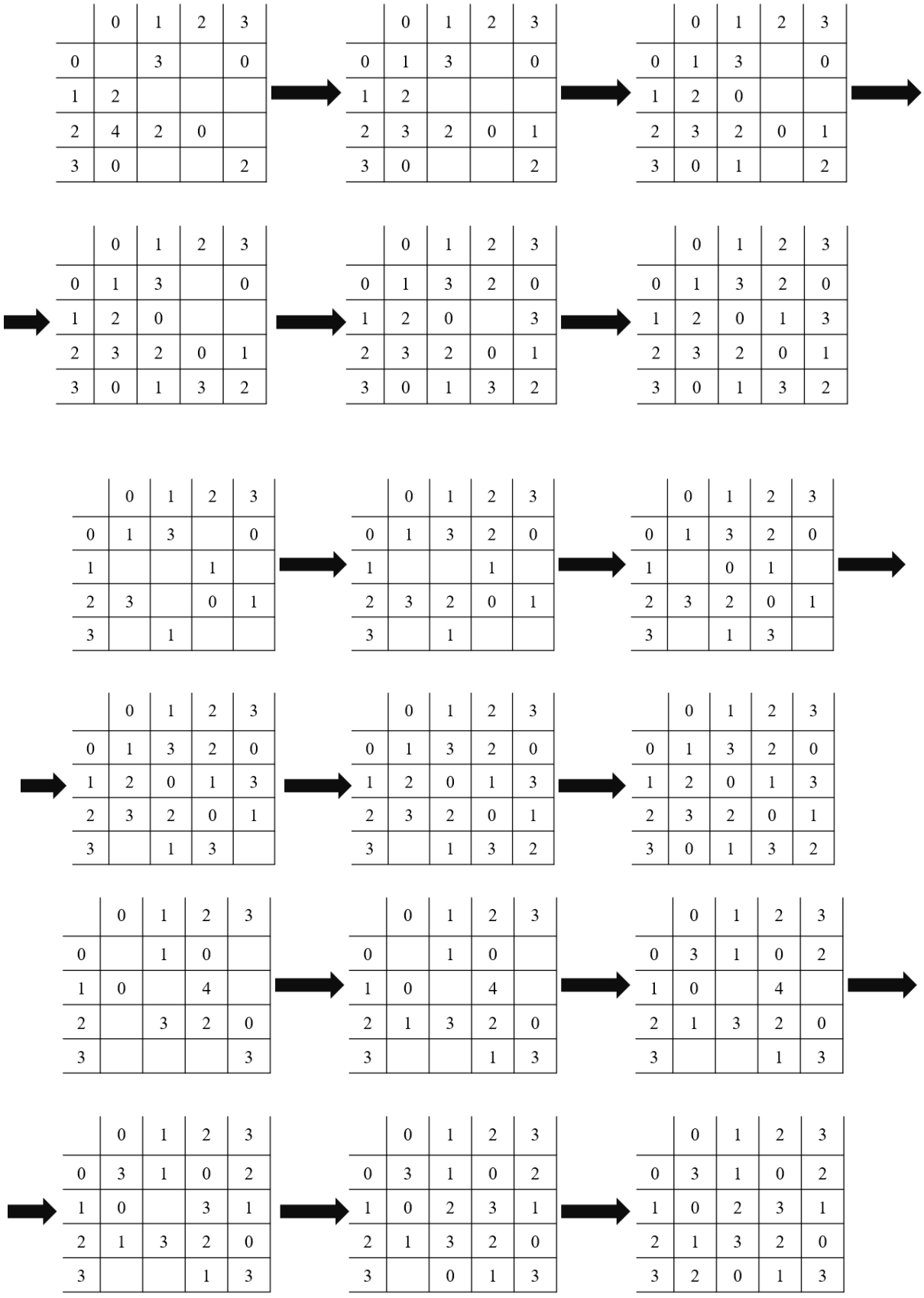
# ВІДНОВЛЕННЯ ЛАТИНСЬКИХ КВАДРАТІВ ЧАСТИНА 2



# ВІДНОВЛЕННЯ ЛАТИНСЬКИХ КВАДРАТІВ ЧАСТИНА 3



# ВІДНОВЛЕННЯ ЛАТИНСЬКИХ КВАДРАТІВ ЧАСТИНА 4



**ТАБЛИЦЯ КЕЛІ ГРУПИ КЛЯЙНА**

| $\oplus$ | *0* | *1* | *2* | *3* |
|---|---|---|---|---|
| *0* | 0 | 1 | 2 | 3 |
| *1* | 1 | 0 | 3 | 2 |
| *2* | 2 | 3 | 0 | 1 |
| *3* | 3 | 2 | 1 | 0 |