*УДК* 003.26.09 *http://dx.doi.org/10.30970/vam.2024.34.00000*

# МОДИФІКОВАНИЙ ШИФР ГІЛЛА З ШУМОМ ТА ПЕРЕСТАНОВКОЮ

**О. Гутік, О. Попадюк**

*Львівський національний університет імені Івана Франка,*
*вул. Університетська 1, Львів, 79000, Україна*
*e-mail: oleg.gutik@lnu.edu.ua, olha.popadiuk@lnu.edu.ua*

Класичний шифр Гілла є першою моделлю шифрування, яка базується на алгебричних перетвореннях. Проте було з'ясовано, що цей шифр є вразливий до атак типу "відкритий текст — шифротекст". У зв'язку з цим багато науковців почали працювати над різними модифікаціями шифру Гілла. Деякі модифікації стосуються побудови матриці-ключ, а також часто застосовують поєднання шифру Гілла з іншими алгоритмами. У статті запропоновано новий підхід до модифікації класичного шифру Гілла, спрямований на підвищення його криптостійкості. Запропонований метод базується на використанні циркулянтної матриці як матриці-ключа та додаткових кроках алгоритму, що включають додавання шуму до тексту повідомлення і здійснення перестановки елементів шифротексту. Оскільки порушується лінійність та зменшується кореляція між відкритим текстом і шифротекстом, то запропонований алгоритм підвищує криптостійкість. Використання циркулянтної матриці дозволяє зменшити обчислювальну складність шифрування та дешифрування. Наведено приклад застосування модифікованого шифру Гілла з шумом та перестановкою.

*Ключові слова*: fine-tuning, Python, генеративний ШІ, LLM.

## 1. Вступ

До 1929 року процеси шифрування та дешифрування не мали формалізованої математичної основи, а криптологи не прагнули до побудови чітких моделей із фіксованими ключами [16]. Переломним моментом у розвитку галузі стало дослідження Лестера Гілла, який у 1929 році запропонував алгебричний підхід до кодування, що згодом ліг в основу математичного моделювання криптографічних процесів. Його праця "Cryptography in an Algebraic Alphabet" була опублікована в журналі American Mathematical Monthly [14].

У статті [14] Гілл вперше запропонував модель шифрування, що базувалася на лінійних алгебричних перетвореннях. Цей метод доповідався автором на засіданні Американського математичного товариства, де він також продемонстрував механічний пристрій для реалізації шифрування та дешифрування. Технічні аспекти функціонування пристрою детально описані у праці Гілла "Concerning Certain Linear Transformation Apparatus of Cryptography" [15].

Застосування методів Гілла та Фрідмана сприяло трансформації уявлень про криптографію: вона почала сприйматися не як мистецтво, а як наукова дисципліна. Зокрема, у низці фундаментальних монографій з сучасної криптографії [4, 7, 22] наголошується, що шифрування є не лише прикладною наукою, а й окремим напрямом математичних досліджень.

Шифр Гілла має низку переваг, зокрема ефективне маскування частот символів у відкритому тексті та високу пропускну здатність. Проте, незважаючи на ці переваги, класична реалізація шифру виявилася вразливою до атак типу "відкритий

текст — шифротекст", що обмежило його практичне застосування в 50-ті роки у зв'язку з розвитком комп'ютерної техніки. Наразі сучасні дослідники активно працюють над модифікаціями шифру Гілла з метою підвищення його криптографічної стійкості.

Упродовж останнього десятиліття алгоритм шифру Гілла зазнав численних модифікацій, спрямованих на усунення його криптографічних слабкостей. У праці [26] наведено огляд різних методів, що використовуються для модифікації шифру Гілла з метою покращення його продуктивності в безпеці даних. Серед запропонованих рішень відзначимо використання самоповторюваних матриць [6], рандомізація вихідного шифру для генерації множинних варіантів шифрованого тексту [19], а також застосування модифікованих режимів роботи та S-блоків [24]. Деякі підходи поєднують шифр Гілла з іншими алгоритмами, такими як Rivest Cipher 4 (RC4) [5] та криптографія еліптичних кривих [3], що дозволяє підвищити ефективність, адаптивність і стійкість до атак.

В окремих працях також запропоновано нові математичні структури — наприклад, використання циркулятної і несингулярної матриць [2], Lehmer-Pell послідовностей [20], які використовують самооборотні матриці у нових схемах шифрування, а також послідовності, які використовують узагальнені числа Мерсенна, p-числа Фібоначчі та m-балансуючі числа [21]. У свою чергу інші підходи, такі як блокове шифрування з використанням логічних операцій XOR та зсуву, а також Radix64 [25], показали, що безпека шифру покращується до 53% лавинного ефекту на основі фактичного експерименту. Модифікований шифр Гілла, здатний шифрувати не лише алфавітні символи, а й будь-які інші типи повідомлень [17], а також моделі з включенням маскуючих символів [1], демонструють прагнення до створення гнучких і стійких криптографічних систем, здатних відповідати сучасним викликам у сфері кібербезпеки.

У сучасних технологіях передача різних мультимедійних даних, таких як конфіденційні зображення, відео, текст, є дуже важливою, і безпека відіграє ключову роль, зокрема, у медичній та військовій галузях. Для шифрування таких зображень, які містять дані, розроблено багато методів, таких як криптографія та стеганографія. Тому для цього напрямку також використовують різні модифікації шифру Гілла, зокрема, який використовує інволютивну матрицю [12], методи генерації самооборотних матриць [23] та як матрицю-ключ використовують матриці Фібоначчі з тридіагональних симетричних форм Тепліца [18].

У статті [10] показано, що модифікований шифр Гілла на основі циркулярних матриць, який представлено в праці [2], вразливий як до атаки відомого відкритого тексту, так і до атаки вибраного відкритого тексту. Проте також запропоновано новий вдосконалений алгоритм шифрування і надано аналіз безпеки та оцінку ефективності цього нового алгоритму шифрування.

## 2. Шифр Гілла

Шифр Гілла — це тип блокового шифру. Ключем шифрування для шифру Гілла є квадратна матриця $K$ цілих чисел. Ці цілі числа беруться з кільця $\mathbb{Z}_q$, де $q$ — розмір набору символів, що використовується для повідомлення у відкритому тексті. Для довільного фіксованого додатного цілого числа $q \geq 2$ через $\mathbb{Z}_q$ позначимо кільце лишків за модулем $q$. Для звичайного додавання та множення $\mathbb{Z}_q$ — кільце, яке містить $q$ елементів. Далі елементи $\mathbb{Z}_q$ позначимо через $\{0, 1, 2, \ldots, q-1\}$.

Важливо зазначити, що не всі такі квадратні матриці є насправді ключами для

шифру Гілла. Визначник матриці $K$ має задовольняти рівність[1]

$$(\det K, q) = 1.$$

Рядок відкритого тексту над алфавітом порядку $q$ переписується як вектор $P$ над множиною $\mathbb{Z}_q$ з використанням природної відповідності. Розбиваємо відкритий текст $P$ на слова (блоки) $P_i$ однакової довжини, тобто $P = P_1P_2 \dots P_m$.

Для шифрування обчислень використовуємо формулу

$$C_i \equiv P_iK (\mathrm{mod}\, q),$$

і для розшифровки

$$P_i \equiv C_iK^{-1} (\mathrm{mod}\, q),$$

де $i = 1, 2, \dots, m$. Тут $P = P_1P_2 \dots P_m$ — вектор-рядок відкритого тексту, $K$ — матриця-ключ, $C = C_1C_2 \dots C_m$ — зашифрований текст, а $K^{-1}$ — модульна арифметична матриця, обернена до матриці $K$. Якщо довжина відкритого повідомлення $P$ не кратна довжині блоку $P_i$, то текст $P$ доповнюємо до кратності блоку $P_i$. Усі блоки $P_i$ відкритого тексту мають однакову довжину, наприклад $n$, а матриця $K$ є розміру $n \times n$. Очевидно, що величина $n$ може бути достатньо великою, але не може перевищувати довжину відкритого тексту $P$.

## 3. Циркулянтна матриця

**Означення 1** (*[8]*). *Під* ***циркулянтною матрицею порядку*** $n$*, або скорочено* ***циркулянтою***, *розуміється квадратна матриця вигляду*

$$C = \mathrm{circ}(c_1, c_2, \dots, c_n) = \begin{pmatrix} c_1 & c_2 & \dots & c_n \\ c_n & c_1 & \dots & c_1 \\ \vdots & \vdots & \ddots & \vdots \\ c_2 & c_3 & \dots & c_1 \end{pmatrix}$$

Елементи кожного рядка циркулянтної матриці $C$ збігаються з елементами попереднього рядка, які зміщені на одну позицію праворуч по колу. Весь циркулянт, очевидно, визначається першим рядком (або стовпцем).

*Визначник* матриці $\mathrm{circ}(c_1, c_2, \dots, c_n)$ є однорідним поліномом степеня $n$ від змінних $c_1, c_2, \dots, c_n$. Немає "простих" формул для обчислення цього визначника.

Добуток циркулянтної матриці та вектора розміром $n$ можна обчислити за допомогою $O(n \log n)$ операцій з використанням швидкого перетворення Фур'є [11].

*Дискретне перетворення Фур'є (ДПФ)* вектора $x \in \mathbb{C}^n$ – це добуток матриці на вектор $y = F_nx$, де матриця ДПФ $F_n = (f_{kj}) \in \mathbb{C}^{n \times n}$ визначається формулою

$$f_{kj} = \omega_n^{(k-1)(j-1)}$$

з

$$\omega_n = \exp(-2\pi i/n) = \cos(2\pi/n) - i \cdot \sin(2\pi/n).$$

ДПФ повсюдно поширене в комп'ютерній науці та інженерії, і одна з причин пов'язана з такою властивістю: якщо число $n$ є надскладеним,[2] то ДПФ можна виконати за набагато меншу кількість циклів, ніж $O(n^2)$ необхідних для звичайного множення матриць на вектор.

[1] Визначник матриці $K$ взаємно простий з числом $q$.

[2] Натуральне число з більшою кількістю дільників, ніж у будь-якого меншого натурального числа.

## 4. Запропонована схема шифрування

У 1984 році [9] Т. Ель-Ґамаль запропонував схему з відкритим ключем, засновану на дискретних логарифмах, тісно пов'язану з методом Діффі-Геллмана. У методі Ельгамаля важливими елементами є вибране просте число $q$ та вибраний примітивний корінь числа $q$.

Надалі через $\varphi(n)$ будемо позначати функцію Ойлера, тобто кількість натуральних чисел, менших або рівних заданому натуральному числу $n$ і взаємно простих з $n$. Нехай $q$ — просте ціле число. Виберемо таємний ключ $D$ такий, що $1 < D < \varphi(q)$, потім додатково виберемо примітивний корінь числа $q$, скажімо $\alpha$. Далі приймемо $E_1 = \alpha$ і $E_2 = E_1^D (\mathrm{mod}\, q)$, потім зробимо трійку $(q, E_1, E_2)$ відкритим ключем, а $D$ збережемо як таємний ключ. Припустимо, що Аліса та Боб хочуть обмінятися ключами.

Нехай $\sigma : \mathbb{Z}_q \to \mathbb{Z}_q$ – перестановка. Для спрощення обчислення образ вектора $P$ під дією перестановки $\sigma : \mathbb{Z}_q \to \mathbb{Z}_q$ позначимо через $(P)\sigma$. Також в алгоритмі ми будемо використовувати перестановку $\xi : \{1, \ldots, r\} \to \{1, \ldots, r\}$ та перестановку $\iota : \{1, \ldots, n^2\} \to \{1, \ldots, n^2\}$, де $r$ – кількість символів тексту повідомлення разом з шумом, $n$ – таємний ключ.

**Алгоритм шифрування.**

Аліса виконує такі дії:

1. Вибирає таємне число $e$, таке що $1 < e < \varphi(q)$.
2. Обчислює значення: $k \leftarrow E_1^e (\mathrm{mod}\, q)$.
3. Знаходить таємний ключ: $n \leftarrow E_2^e (\mathrm{mod}\, q)$
4. Будує матрицю-ключ:

$$K \leftarrow C_n^q(\alpha) = \begin{pmatrix} \alpha & \alpha^n & \alpha^{n^2} & \ldots & \alpha^{n^{n-1}} \\ \alpha^{n^{n-1}} & \alpha & \alpha^n & \ldots & \alpha^{n^{n-2}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha^n & \alpha^{n^2} & \alpha^{n^3} & \ldots & \alpha \end{pmatrix}$$

5. До тексту $P$ вкінці дописує, враховуючи частоту вживання літер у мові, $s$ випадкових додаткових символів, які будемо називати *шумом*.
6. На індекси символів тексту повідомлення застосуємо перестановку $\xi$, так відбудеться переставлення символів повідомлення.
7. Текст повідомлення $P$ розбиваємо на $m$ частин по $n$ символів у кожній, утворивши вектор $P = P_1 P_2 \ldots P_m$.
8. Здійснює шифрування за формулою:

$$\mathrm{Enc}(P) : C_i \leftarrow ((P_i K)(\mathrm{mod}\, q))\sigma^{(i)\iota},$$

   де $i = 1, 2, \ldots, m$.
9. Передає Бобу значення $(k, C)$.

**Алгоритм дешифрування.**

Боб після отримання значення $(k, C)$ виконує такі кроки для дешифрування повідомлення:

1. Обчислює таємний ключ: $n \leftarrow k^D (\mathrm{mod}\, q)$, де $D$ – таємний ключ Боба.

2. Знаходить матрицю-ключ: $K \leftarrow C_n^q(\alpha)$.
3. Здійснює дешифрування за формулою:

$$\mathrm{Dec}(C) : P_i' \leftarrow ((C_i)(\sigma^{(i)\iota})^{-1})K^{-1}(\mathrm{mod}\, q),$$

де $i = 1, 2, \ldots, m$.

4. На кожен індекс символу тексту $P'$ діє оберненою перестановкою $\xi^{-1}$.
5. Видаливши зайві символи, отримує оригінальний текст.

**Зауваження 1.** *Зрозуміло, що процедуру додавання шуму до відкритого тексту можна звести до додавання шуму розміру $s, s \geq 1$, до кожного блоку, довівши довжину кожного блоку $P_i$ до значення $n + s$. Тоді матриця-ключ повинна мати розмір $(n + s) \times (n + s)$.*

## 5. Приклад

Припустимо, що Аліса хоче надіслати повідомлення Бобу. Тоді вона спочатку обчислює матрицю-ключ $K$, використовуючи запропонований вище метод, а потім шифрує відкритий текст $P$ за допомогою матриці-ключа $K$.

Припустимо, що $q = 29$, а таємний ключ Боба $D = 13$. Далі Боб вибирає примітивний корінь $q$, скажімо, $\alpha = 3$.

Боб приймає $E_1 = \alpha = 3$ та обчислює $E_2 = E_1^D = 3^{13}(\mathrm{mod}\, 29) = 19$.

Отже, відкритий ключ Боба $\mathrm{pk}(q, E_1, E_2)$ дорівнює $\mathrm{pk}(29, 3, 19)$, а таємний ключ $D = 13$.

Припустимо, що ми використовуємо алфавіт

| 0 | 1 | 2 | 3 | 4 | 5 | ... | 24 | 25 | 26 | 27 | 28 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| A | B | C | D | E | F | ... | Y | Z | . | , | ! |

Тут відкритий текст

$$P = \textbf{HELLO,WORLD!}$$

Нехай перестановка $\sigma$ визначена так

$$\begin{aligned}
(0)\,\sigma &= 7, & (1)\,\sigma &= 26,\\
(2)\,\sigma &= 1, & (3)\,\sigma &= 24,\\
(4)\,\sigma &= 0, & (5)\,\sigma &= 21,\\
(6)\,\sigma &= 27, & (7)\,\sigma &= 4,\\
(8)\,\sigma &= 9, & (9)\,\sigma &= 12,\\
(10)\,\sigma &= 19, & (11)\,\sigma &= 23,\\
(12)\,\sigma &= 8, & (13)\,\sigma &= 25,\\
(14)\,\sigma &= 28, & (15)\,\sigma &= 17,\\
(16)\,\sigma &= 14, & (17)\,\sigma &= 20,\\
(18)\,\sigma &= 6, & (19)\,\sigma &= 10,\\
(20)\,\sigma &= 2, & (21)\,\sigma &= 5,\\
(22)\,\sigma &= 3, & (23)\,\sigma &= 11,
\end{aligned}$$

$$(24)\,\sigma = 18, \qquad (25)\,\sigma = 15,$$
$$(26)\,\sigma = 22, \qquad (27)\,\sigma = 16,$$
$$(28)\,\sigma = 13.$$

Нехай перестановка $\xi$ визначена так

$$(1)\,\xi = 7, \qquad (2)\,\xi = 2,$$
$$(3)\,\xi = 14, \qquad (4)\,\xi = 11,$$
$$(5)\,\xi = 4, \qquad (6)\,\xi = 1,$$
$$(7)\,\xi = 13, \qquad (8)\,\xi = 16,$$
$$(9)\,\xi = 5, \qquad (10)\,\xi = 9,$$
$$(11)\,\xi = 3, \qquad (12)\,\xi = 15,$$
$$(13)\,\xi = 6, \qquad (14)\,\xi = 12,$$
$$(15)\,\xi = 8, \qquad (16)\,\xi = 10.$$

Нехай перестановка $\iota$ визначена так

$$(1)\,\iota = 7, \qquad (2)\,\iota = 4,$$
$$(3)\,\iota = 10, \qquad (4)\,\iota = 5,$$
$$(5)\,\iota = 1, \qquad (6)\,\iota = 2,$$
$$(7)\,\iota = 3, \qquad (8)\,\iota = 13,$$
$$(9)\,\iota = 16, \qquad (10)\,\iota = 6,$$
$$(11)\,\iota = 9, \qquad (12)\,\iota = 14,$$
$$(13)\,\iota = 8, \qquad (14)\,\iota = 15,$$
$$(15)\,\iota = 12, \qquad (16)\,\iota = 11.$$

Спочатку виберемо число $e$ таке, що $1 < e < \varphi(q)$. Нехай $e = 22$. Обчислюємо значення,

$$k = E_1^e(\mathrm{mod}\, q) = 3^{22}(\mathrm{mod}\, 29) \equiv 22$$

і таємний ключ

$$n = E_2^e(\mathrm{mod}\, q) = 19^{22}(\mathrm{mod}\, 29) \equiv 4.$$

Побудуємо матрицю-ключ,

$$K = C_n^q(\alpha) = C_4^{29}(3) = \begin{pmatrix} \alpha & \alpha^n & \alpha^{n^2} & \alpha^{n^3} \\ \alpha^{n^3} & \alpha & \alpha^n & \alpha^{n^2} \\ \alpha^{n^2} & \alpha^{n^3} & \alpha & \alpha^n \\ \alpha^n & \alpha^{n^2} & \alpha^{n^3} & \alpha \end{pmatrix} = \begin{pmatrix} 3 & 3^4 & 3^{4^2} & 3^{4^3} \\ 3^{4^3} & 3 & 3^4 & 3^{4^2} \\ 3^{4^2} & 3^{4^3} & 3 & 3^4 \\ 3^4 & 3^{4^2} & 3^{4^3} & 3 \end{pmatrix}$$

та

$$K(\mathrm{mod}\, 29) = \begin{pmatrix} 3 & 23 & 20 & 7 \\ 7 & 3 & 23 & 20 \\ 20 & 7 & 3 & 23 \\ 23 & 20 & 7 & 3 \end{pmatrix}.$$

**Шифрування:**

До відкритого тексту повідомлення $P$ додаємо шум і запишемо у вигляді масиву

$$P' = \begin{pmatrix} H & E & L & L & O & , & W & O & R & L & D & ! & A & K & M & E \end{pmatrix} \sim$$
$$\sim \begin{pmatrix} 7 & 4 & 11 & 11 & 14 & 27 & 22 & 14 & 17 & 11 & 3 & 28 & 0 & 10 & 12 & 4 \end{pmatrix}.$$

Застосувавши перестановку $\xi$ на індекси символів тексту $P'$, отримаємо повідомлення

$$P'_\xi = \begin{pmatrix} 27 & 4 & 3 & 14 & 17 & 0 & 7 & 12 & 11 & 4 & 11 & 10 & 22 & 11 & 28 & 14 \end{pmatrix}.$$

Далі текст $P'_\xi$ розбиваємо на 4 рівні частини $p_i$ і за формулою

$$\mathrm{Enc}(P) : C_i \leftarrow ((p_i K)(\mathrm{mod}\, 29))\sigma^{(i)\iota},$$

де $i = 1, 2, 3, 4$, виконуємо шифрування.

$$C_1 = ((p_1 K)(\mathrm{mod}\, 29))\sigma^{(1)\iota} =$$
$$= \left( \begin{pmatrix} 27 & 4 & 3 & 14 \end{pmatrix} \begin{pmatrix} 3 & 23 & 20 & 7 \\ 7 & 3 & 23 & 20 \\ 20 & 7 & 3 & 23 \\ 23 & 20 & 7 & 3 \end{pmatrix} (\mathrm{mod}\, 29) \right) \sigma^7 \equiv$$
$$\equiv \begin{pmatrix} 27 & 6 & 14 & 3 \end{pmatrix} \sigma^7 = \begin{pmatrix} 16 & 27 & 20 & 11 \end{pmatrix}.$$

$$C_2 = ((p_2 K)(\mathrm{mod}\, 29))\sigma^{(2)\iota} =$$
$$= \left( \begin{pmatrix} 17 & 0 & 7 & 12 \end{pmatrix} \begin{pmatrix} 3 & 23 & 20 & 7 \\ 7 & 3 & 23 & 20 \\ 20 & 7 & 3 & 23 \\ 23 & 20 & 7 & 3 \end{pmatrix} (\mathrm{mod}\, 29) \right) \sigma^4 \equiv$$
$$\equiv \begin{pmatrix} 3 & 13 & 10 & 26 \end{pmatrix} \sigma^4 = \begin{pmatrix} 6 & 17 & 10 & 18 \end{pmatrix}.$$

$$C_3 = ((p_3 K)(\mathrm{mod}\, 29))\sigma^{(3)\iota} =$$
$$= \left( \begin{pmatrix} 11 & 4 & 11 & 10 \end{pmatrix} \begin{pmatrix} 3 & 23 & 20 & 7 \\ 7 & 3 & 23 & 20 \\ 20 & 7 & 3 & 23 \\ 23 & 20 & 7 & 3 \end{pmatrix} (\mathrm{mod}\, 29) \right) \sigma^{10} \equiv$$
$$\equiv \begin{pmatrix} 18 & 20 & 9 & 5 \end{pmatrix} \sigma^{10} = \begin{pmatrix} 6 & 2 & 12 & 21 \end{pmatrix}.$$

$$C_4 = ((p_4 K)(\mathrm{mod}\, 29))\sigma^{(4)\iota} =$$
$$= \left( \begin{pmatrix} 22 & 11 & 28 & 14 \end{pmatrix} \begin{pmatrix} 3 & 23 & 20 & 7 \\ 7 & 3 & 23 & 20 \\ 20 & 7 & 3 & 23 \\ 23 & 20 & 7 & 3 \end{pmatrix} (\mathrm{mod}\, 29) \right) \sigma^5 \equiv$$
$$\equiv \begin{pmatrix} 10 & 0 & 5 & 16 \end{pmatrix} \sigma^5 = \begin{pmatrix} 19 & 4 & 21 & 14 \end{pmatrix}.$$

Тепер Аліса надсилає цей зашифрований текст Бобу разом зі значенням $k$. Отримавши шифротекст $C$ разом із значенням $(k, C)$, Боб обчислить ключ розшифрування $K^{-1}$ за допомогою свого таємного ключа $D$, який задано як $n = k^D (\mathrm{mod}\, 29) = 22^{13} (\mathrm{mod}\, 29) \equiv 4$.

Таким чином,

$$K^{-1} (\mathrm{mod}\, 29) = \begin{pmatrix} 13 & 23 & 15 & 1 \\ 1 & 13 & 23 & 15 \\ 15 & 1 & 13 & 23 \\ 23 & 15 & 1 & 13 \end{pmatrix}.$$

Зрозуміло $KK^{-1} = I (\mathrm{mod}\, 29)$.

Для відновлення відкритого тексту **HELLO,WORLD!**, успішно надісланого Алісою, Боб повинен виконати відповідні кроки алгоритму дешифрування.

## 6. Аналіз безпеки

Нехай ми зламаємо запропоновану нами модифікацію шифру Гілла за допомогою атаки методом перебору для генерації всіх можливих матриць.

Оборотні матриці розміру $n \times n$ над кільцем $\mathbb{Z}_q$ ($q > 26$ — просте число) утворюють загальну лінійну групу. Її зазвичай позначають як $GL(n, q)$ або $GL_n(q)$.

Загальновідомо [13], що

$$|GL(n, q)| = q^{n(n-1)/2}(q^n - 1)(q^{n-1} - 1) \dots (q - 1).$$

**Приклад 1.** *Розглянемо матрицю-ключ $K = C_4^{29}(3)$ над полем $Z_{29}$. Тут маємо $n = 4$ та $q = 29$.*

*Отже, загальна кількість оборотних матриць дорівнює*

$$|GL(4, 29)| = 29^6(29^4 - 1)(29^3 - 1)(29^2 - 1) \cdot 28 = 2,4131975110057697 \times 10^{23}.$$

*Отже, щоб зловмисник відновив цю матрицю-ключ, потрібно перевірити $10^{23}$ можливих матриць, що не так просто.*

Якщо збільшити розмір матриці-ключ для фіксованого занадто великого $q$, то

$$|GL(n, q)| \to \infty.$$

Отже, зламати цей шифр методом грубої сили складно, оскільки потребує багато ресурсу.

## 7. Висновок

У статті ми запропонували блоковий шифр, який є модифікацією шифру Гілла з додаванням шуму та перестановки. Цей метод ускладнює злам шифру, оскільки лінійні та диференціальні методи злому не працюють. Також ми наводимо приклад шифрування та дешифрування повідомлення за допомогою цього методу, щоб продемонструвати, як він працює.

## Список використаної літератури

1. Ігнатович А.О. Моделі підвищення ефективності та надійності блокових шифрів / А.О. Ігнатович, Н.Я. Павич // Вісник ЛДУ БЖД. – 2015. – № 11. – С. 101–109.

2. Adinarayana Reddy K. A Modified Hill Cipher Based on Circulant Matrices / K. Adinarayana Reddy, B. Vishnuvardhan, Madhuviswanatham, A.V.N. Krishna // Procedia Technology. – 2012. – Vol. 4. – P. 114–118. – DOI: 10.1016/j.protcy.2012.05.016.
3. Agrawal K. Elliptic Curve Cryptography with Hill Cipher Generation for Secure Text Cryptosystem / K. Agrawal, A. Gera // International Journal of Computer Applications. – 2014. – Vol. 106, №1. – P. 18–24.
4. Akleylek S. Handbook of Formal Analysis and Verification in Cryptography / S. Akleylek, B. Dundua. – CRC Press, 2024. – (Prospects in Pure and Applied Mathematics).
5. Azanuddin Kartadie R. A combination of Hill cipher and RC4 methods for text security / R. Azanuddin Kartadie, F. Erwis, A.F. Boy, A.H. Nasyuha // TELKOMNIKA Telecommunication Computing Electronics and Control. – 2024. – Vol. 22, № 2. – P. 351–361. – DOI: 10.12928/TELKOMNIKA.v22i2.25628.
6. Bedasa M.F. Data Encryption and Decryption by Using Hill Cipher Algorithm / M.F. Bedasa, A.S. Bedada, W.B. Mulatu // Control Theory and Informatics. – 2020. – Vol. 10.
7. Bruen A.A. Cryptography, Information Theory, and Error-Correction: A Handbook for the 21st Century. 2nd ed. / A.A. Bruen, M.A. Forcinito, J.M. McQuillan. – Wiley, 2021.
8. Davis P.J. Circulant Matrices. 2nd ed. / P.J. Davis. – New-York: Wiley, 1979.
9. Elgamal T. A public key cryptosystem and a signature scheme based on discrete logarithms / T. Elgamal // IEEE Transactions on Information Theory. – 1985. – Vol. 31, № 4. – P. 469–472. – DOI: https://doi.org/10.1109/TIT.1985.1057074.
10. ElHabshy A.A. Augmented Hill Cipher / A.A. ElHabshy // International Journal of Network Security. – 2019. – Vol. 21. – P. 812–818.
11. Golub G.H. Matrix Computations. 3rd ed. / G.H. Golub, C.F. Van Loan. – Baltimore: John Hopkins University Press, 1996.
12. Goutham L. Modified Hill Cipher Based Image Encryption Technique / L. Goutham, M.S. Mahendra, A.P. Manasa, S.N. Prajwalasimha // International Journal for Research in Applied Science & Engineering Technology. – 2017. – Vol. 5, № 4. – P. 342–345.
13. Hachenberger D. Topics in Galois Fields / D. Hachenberger, D. Jungnickel. – Springer, 2020. – DOI: https://doi.org/10.1007/978-3-030-60806-4.
14. Hill L. Cryptography in an algebraic alphabet / L. Hill // American Mathematical Monthly. – 1929. – Vol. 36. – P. 306–312.
15. Hill L. Concerning certain linear transformation apparatus of cryptography / L. Hill // American Mathematical Monthly. – 1931. – Vol. 38. – P. 135–154.
16. Khan F. H. Hill Cipher Key Generation Algorithm by using Orthogonal Matrix / F.H. Khan, R. Shams, F. Qazi, D. Agha // International Journal of Innovative Science and Modern Engineering (IJISME). – 2015. – Vol. 3, № 3. – [Електрон. ресурс]. – Режим доступу: https://www.ijisme.org/wp-content/uploads/papers/v3i3/C0799023315.pdf.
17. Kalaichelvi V. A New Variant of Hill Cipher Algorithm for Data Security / V. Kalaichelvi, K. Manimozhi, P. Meenakshi, B. Rajakumar, P. Vimaladevi // International Journal of Pure and Applied Mathematics. – 2017. – Vol. 117, № 15. – P. 581–588.
18. Kokena F. Fibonacci matrices from tridiagonal symmetric Toeplitz forms and their application in cryptographic Hill cipher schemess / F.Kokena, M. Aksoy // Filomat. – 2025. – Vol. 39, № 14. – P. 4821–4842. – DOI: 10.2298/FIL2514821K.
19. Krishna A.V.N. A Modified Hill Cipher using Randomized Approach / A.V.N. Krishna, K. Madhuravani // International Journal of Computer Network and Information Security (IJCNIS). – 2012. – Vol. 4, № 5. – P. 56–62. – DOI: 10.5815/ijcnis.2012.05.07.
20. Mehraban E. Affine-Hill cipher key generation using self-invertible matrices from $k$-division $L$-Lehmer-Pell sequences / E. Mehraban, T.A. Gulliver, Deveci $\ddot{O}$., E. Hincal // J. Combin. Math. Combin. Comput. – 2025. – Vol. 124. – P. 47–58.
21. Mehraban E. Affine–Hill cipher from Hadamard-type Fibonacci–Mersenne and Fibonacci-balancing $p$-sequences / E. Mehraban, T.A. Gulliver, E. Hincal // Notes on Number Theory and Discrete Mathematics. – 2025. – Vol. 31, № 3. – P. 588–606. – DOI: 10.7546/nntdm.2025.31.3.588-606.

22. Meneze A.J. Handbook of Applied Cryptography / A.J. Menezes, S.A. Vanstone, P.C. Van Oorschot. – CRC Press, 2001.
23. Panigrahy S.K. Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm / S.K. Panigrahy, B. Acharya, D. Jena // Proc. 1st International Conference on Advances in Computing. – Chikhli, India, 21–22 February 2008.
24. Paragas J.R. A new variant of Hill cipher algorithm using modified $S$-box / J.R. Paragas, A.M. Sison, R.P. Medina // International Journal of Science and Technology Research. – 2019. – Vol. 8, № 10. – P. 615–619.
25. Paragas J.R. Hill Cipher Modification: A Simplified Approach / J.R. Paragas, A.M. Sison, R.P. Medina // Proc. IEEE 11th Int. Conf. on Communication Software and Networks (ICCSN). – Chongqing, China, 2019. – P. 821–825. – DOI: 10.1109/ICCSN.2019.8905360.
26. Parmar N.B. Hill Cipher Modifications: A Detailed Review / N.B. Parmar, K.R. Bhatt // International Journal of Innovative Research in Computer and Communication Engineering. – 2015. – Vol. 3. – P. 1467–1474.

*Стаття: надійшла до редколегії* 24.09.2024
*доопрацьована* 10.10.2024
*прийнята до друку* 15.10.2024

## MODIFIED HILL CIPHER WITH NOISE AND PERMUTATION

**O. Gutik, O. Popadiuk**

*Ivan Franko National University of Lviv,*
*1, Universytetska str., 79000, Lviv, Ukraine,*
*e-mail:* oleg.gutik@lnu.edu.ua, olha.popadiuk@lnu.edu.ua

The classical Hill cipher is the first encryption model based on algebraic transformations. However, it was found that this cipher is vulnerable to "plaintext - ciphertext" attacks. In this regard, many scientists have begun to work on various modifications of the Hill cipher. Some modifications concern the construction of the key matrix, and also often use a combination of the Hill cipher with other algorithms. The paper proposes a new approach to the modification of the classic Hill cipher aimed at increasing its cryptoresistance. The proposed method is based on the use of a circulant matrix as a key-matrix and additional algorithm steps, which include adding noise to the message and permuting the ciphertext elements. Since the linearity is broken and the correlation between plaintext and ciphertext is reduced, the proposed algorithm increases the cryptoresistance. The use of a circulant matrix reduces the computational complexity of encryption and decryption. An example of the application of a modified Hill cipher with noise and permutation is given.

*Key words*: Hill cipher, cryptography, circulant matrix.