УДК 003.26

В. А. Вітюк
З. В. Бондаренко

РЕАЛІЗАЦІЯ ТА КРИПТОАНАЛІЗ БЛОКОВОГО ШИФРУ ГІЛЛА ЗАСОБАМИ ЛІНІЙНОЇ АЛГЕБРИ

Вінницький національний технічний університет

Анотація

У роботі досліджено математичні основи блокового шифрування на прикладі шифру Гілла. Визначено алгебраїчні умови існування оберненої матриці ключа в кільці лишків. Розроблено та описано алгоритм генерації придатних для шифрування ключів. Проведено комп'ютерне моделювання процесу та оцінку стійкості методу до злому.

Ключові слова: криптографія, лінійна алгебра, шифр Гілла, матричні операції, модульна арифметика, генерація ключів.

Abstract

The paper investigates the mathematical foundations of block encryption using the Hill cipher. Algebraic conditions for the existence of an inverse key matrix in the residue ring are determined. An algorithm for generating keys suitable for encryption is developed and described. Computer simulation of the process and evaluation of the method's resistance to breaking are performed.

Keywords: cryptography, linear algebra, Hill cipher, matrix operations, modular arithmetic, key generation.

Вступ

Інформаційна безпека є критично важливою у сучасному світі. Більшість алгоритмів захисту даних базуються на складних математичних задачах [1]. Шифр Гілла є класичним прикладом поліграмного шифру, який використовує апарат лінійної алгебри. На відміну від простих шифрів заміни, він кодує блоки символів, що дозволяє приховати частотні закономірності мови [2]. Мета роботи – продемонструвати, як матричні перетворення забезпечують конфіденційність інформації та описати алгоритм створення стійких ключів.

Результати дослідження

Математична модель шифру Гілла базується на операціях з матрицями за модулем. Текст повідомлення розбивається на k блоків довжиною n, які записуються як стовпці матриці P розмірності n×k.

Процес шифрування описується рівнянням:

$$C = (K \times P) \ mod\ m$$

де C – матриця зашифрованого тексту (n×k), P – матриця відкритого тексту, K – квадратна матриця-ключ розмірності n×n, а m – потужність алфавіту (наприклад, 26 для англійської мови).

Для дешифрування необхідно виконати обернене перетворення:

$$P = (K^{-1} \times C) \ mod\ m$$

Найскладнішим етапом є генерація коректного ключа K. З курсу лінійної алгебри відомо, що матриця є оборотною в кільці Z_m тоді і тільки тоді, коли її визначник det(K) взаємно простий з модулем m, тобто НСД(det(K),m)=1 [3].

У роботі запропоновано алгоритм генерації ключів, що гарантує виконання цієї умови:

1) генерація випадкової матриці n×n з числами в діапазоні [0,m−1];
2) обчислення визначника det(K);
3) перевірка умови: якщо НСД(det(K),m)=1, матриця приймається, інакше – генерується нова.

Для перевірки теоретичних розрахунків було розроблено програмний алгоритм генерації ключів та шифрування. Замість ручного підбору параметрів, алгоритм автоматично формує випадкові матриці та

перевіряє їх на оборотність за допомогою розширеного алгоритму Евкліда. Це дозволило провести серію експериментів для оцінки надійності методу (Табл. 1).

Таблиця 1. Залежність характеристик шифру від розмірності матриці

Розмірність матриці (n×n)	Кількість можливих ключів	Складність злому
2×2	$\approx 1.5\times10^{5}$	Низька (можливий швидкий злам)
3×3	$\approx 4.6\times10^{10}$	Середня (вимагає обчислювальних ресурсів)
4×4	$\approx 1.4\times10^{16}$	Висока (надійно для навчальних задач)

Експерименти показали, що при використанні матриці 2×2 кількість комбінацій невелика, що робить шифр вразливим. Однак збільшення розмірності до 4×4 призводить до експоненціального зростання кількості ключів, роблячи прямий перебір неможливим за розумний час на стандартному обладнанні [1].

Висновки

У роботі проаналізовано застосування лінійної алгебри в кібербезпеці. Доведено, що коректне використання матричних операцій дозволяє ефективно захищати текстові дані. Комп'ютерне моделювання підтвердило, що стійкість шифру Гілла прямо залежить від розмірності матриці ключа. Отримані результати демонструють важливість математичного апарату при проектуванні алгоритмів захисту інформації [1, 3].

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Quljanov J. B. Fundamentals of Linear Algebra and Their Practical Applications in Cryptographic Systems. International Multidisciplinary Journal for Research & Development. 2025. Vol. 12, No. 1.

2. Wang X., Zhang Y. A Dynamic Hill Cipher with Arnold Scrambling Technique for Medical Images Encryption. Mathematics. 2024. Vol. 12, No. 24.

3. Chen L., Li S. A Survey on the Unimodular Hill Cipher and Its Applications in Modern Cryptography. Journal of Cybersecurity and Privacy. 2025. Vol. 3, No. 2. P. 112-128.

Вітюк Володимир Артемович – студент групи 1КІ-25МС, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, email: vitiukvolodymyr@gmail.com

Науковий керівник: ***Бондаренко Злата Василівна*** – кандидат педагогічних наук, доцент, кафедра вищої математики, Вінницький національний технічний університет, м. Вінниця, email: bondarenko@vntu.edu.ua

Vitiuk Volodymyr Artemovich – Department of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: vitiukvolodymyr@gmail.com

Supervisor: ***Bondarenko Zlata V.*** – Candidate of Pedagogical Sciences, Associate Professor, Department of Higher Mathematics, Vinnytsia National Technical University, Vinnytsia, email: bondarenko@vntu.edu.ua