УДК 517.9

Б. М. Свитка
Н. Б. Дубова

ЛІНІЙНА АЛГЕБРА ЯК ОСНОВА ДЛЯ ПОБУДОВИ ТА ВЗЛОМУ ЛІНІЙНИХ ШИФРІВ

Вінницький національний технічний університет

Анотація

Метою є демонстрація важливості лінійної алгебри як фундаментальної математичної основи для побудови та аналізу лінійних шифрів. У цій роботі будуть розглянуті основні математичні поняття, що використовуються в криптографії, такі як вектори, матриці, обернені матриці та системи лінійних рівнянь. Буде показано, як ці інструменти дозволяють не тільки ефективно шифрувати інформацію, але й виконувати криптоаналіз, знаходячи ключі шляхом розв'язання лінійних систем.

Ключові слова: матриця, вектор, лінійний шифр, обернена матриця, шифрування.

Abstract

The purpose of this thesis is to demonstrate the importance of linear algebra as a fundamental mathematical foundation for the construction and analysis of linear ciphers. Basic mathematical concepts used in cryptography, such as vector spaces, matrices, inverse matrices and systems of linear equations will be considered in this work. It will be shown, how these tools allow not only to effectively encrypt information but also to perform cryptanalysis, finding keys by solving linear systems.

Keywords: matrix, vector, linear cipher, inverse matrix, encryption.

Вступ

Лінійна алгебра відіграє значну роль у вищій математиці та дуже поширена в науці криптографії. Лінійні шифри базуються на лінійних перетвореннях над векторними просторами та деяким скінченним полем або кільцем. Використання математичного моделювання допомагає зрозуміти функціонування процесів шифрування та дешифрування, а також їхні вразливості.

Результати дослідження

Представимо, що у нас є векторний простір тобто множина всіх векторів довжини n, де кожен елемент береться за модулем m.

$$V = \mathbb{Z}_m^n$$

Повідомлення представляється у вигляді вектора:

$$x = \begin{pmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{pmatrix}, x_i \in \mathbb{Z}_m$$

Кожен елемент x_i відповідає числовому коду символу (наприклад, букви). Шифрування відбувається за допомогою матриці-ключа A розміром $n \times n$, де y - це вектор шифротексту:

$$y = Ax (\mathrm{mod}\, m)$$

Щоб потім можна було відновити початковий текст, матриця A повинна бути оберненою за модулем m. Це означає, що її визначник має обернене число за модулем m:

$$\gcd(\det A, m) = 1$$

Матриця називається оборотною, якщо вона здійснює взаємно однозначне перетворення. Нехай A оборотна матриця. Матрицею, оберненою до A, називається матриця A^{-1}, для якої виконуються

умови $A^{-1}A = AA^{-1} = E$ [1]

Якщо матриця оборотна, то дешифрування виглядає так, де A^{-1} - обернена матриця до A за модулем m:

$$x = A^{-1}y(\mathrm{mod}\, m)$$

Приклад (шифр Гілла)

У лінійних шифрах повідомлення подається у вигляді вектора та шифрується за допомогою матриці-ключа. При цьому важливу роль відіграє розбиття повідомлення на блоки фіксованої довжини.

Лінійний шифр k - го порядку (Хілла). Відкрите повідомлення при такому шифруванні розбивається на k - грами. Кожній k - грамі ставимо у відповідність вектор X (тобто матриця розміру $k \cdot 1$)[2].

Розглянемо простий приклад з блоком з двох символів $n = 2$ і модулем $m = 26$:

$$A = \begin{pmatrix} 3 & 5 \\ 2 & 7 \end{pmatrix}, x = \begin{pmatrix} 7 \\ 4 \end{pmatrix}$$

$$y = Ax = \begin{pmatrix} 3 \cdot 7 + 5 \cdot 4 \\ 2 \cdot 7 + 7 \cdot 4 \end{pmatrix} = \begin{pmatrix} 41 \\ 42 \end{pmatrix} = \begin{pmatrix} 15 \\ 16 \end{pmatrix} (\mathrm{mod}\, 26)$$

Щоб розшифрувати, використовується обернена матриця A^{-1} і отримується початковий вектор x.

Взлом лінійного шифру

Якщо зловмисник знає $k \geq n$ пар “відкритий текст - шифротекст” x_i, y_i , можна скласти систему де X матриця з векторів відкритого тексту, а Y матриця з векторів шифротексту:

$$AX = Y(\mathrm{mod}\, m)$$

Якщо матриця X обернена за модулем $m(\det X)$ то ключ знаходиться так:

$$A = YX^{-1}(\mathrm{mod}\, m)$$

Це показує, що простий лінійний шифр не дуже стійкий, бо знання кількох пар «відкритий текст - шифротекст» дозволяє знайти ключ. Структура матриці і розмірність простору визначають, наскільки шифр стійкий.

Висновки

Лінійна алгебра дозволяє описати шифрування і дешифрування як чіткі математичні операції. Вона дає змогу аналізувати стійкість шифрів та прогнозувати можливість їхнього взлому. Навички роботи з матрицями, оберненими матрицями і системами лінійних рівнянь є критично важливими для розуміння криптографії, навіть на прикладі простих лінійних шифрів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Математичні методи криптології: Навчальний посібник [Електронний ресурс] (Для студентів техн. спец. вищ. навч. закл.) / [А.Д. Кожухівський, І.Д. Горбенко, Г.І. Гайдур, О.А. Кожухівська, В.В. Марченко]; М-во освіти і науки України, Державний університет телекомунікацій.- К.: ДУТ, 2021 – 244 с. – Режим доступу: https://files.znu.edu.ua/files/Bibliobooks/Inshi83/0062482.pdf

2. Елементи математичних основ криптографії : навчальний посібник / Марта СТАСЮК – Львів : ЛДУ БЖД, 2021. – 216 с. – Режим доступу: https://books.ldubgd.edu.ua/index.php/ed/catalog/view/125/88/388-1

Свитка Богдана Миколаївна — студентка групи 1ЕХКБ-25б, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: bogdanasvutka@gmail.com

Науковий керівник: ***Дубова Надія Борисівна*** — старший викладач, Вінницький національний технічний університет, м. Вінниця, e-mail: dubova_n_b@vntu.edu.ua

***Svitka Bohdana Mykolaivna* —** student of group 1EHKB-25b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: bogdanasvutka@gmail.com

Scientific advisor: ***Dubova Nadiya Borysivna*** — senior lecturer, Vinnytsia National Technical University, Vinnytsia, e-mail: dubova_n_b@vntu.edu.ua