

УДК 004.04; 512.62

Пожуєва І.С.¹, Шабля Д.О.²

¹ канд. техн. наук, доц. НУ «Запорізька політехніка»

² студ. гр. КНТ-514 НУ «Запорізька політехніка»

ВИКОРИСТАННЯ МАТРИЦЬ У ШИФРІ ХІЛЛА

На сьогоднішній день є дуже багато онлайн-сервісів, яким ми довіряємо свої персональні дані. Але доступ до цих даних мають мати тільки авторизовані особи. Саме для цього і використовується шифрування. Шифрування - це процес кодування інформації з метою запобігання несанкціонованого доступу. Є дуже багато способів за допомогою яких можна зашифрувати дані, але у цій доповіді ми розглянемо саме шифр Хілла. Проаналізуємо як він працює: як закодувати та декодувати інформацію та як у ньому використовуються матриці.

Почнемо з того, що дамо визначення шифру Хілла. Це симетричний алгоритм шифрування, який використовує лінійну алгебру та матричні перетворення. Він ґрунтується на множенні вектора відкритого тексту на ключову матрицю. Щоб наглядно показати як працює шифр Хілла, ми будемо використовувати українську абетку та спробуємо зашифрувати слово "МОРОЗИ-ВО". Пронумеруємо кожну літеру українського алфавіту, це буде потрібно у процесі шифрування та дешифрування повідомлення у шифрі Хілла: А:=0, Б:=1, В:=2, Г:=3, Ґ:=4, Д:=5, Е:=6, Є:=7, Ж:=8, З:=9, И:=10, І:=11, Ї:=12, Й:=13, К:=14, Л:=15, М:=16, Н:=17, О:=18, П:=19, Р:=20, С:=21, Т:=22, У:=23, Ф:=24, Х:=25, Ц:=26, Ч:=27, Ш:=28, Щ:=29, Ъ:=30, Ю:=31, Я:=32.

Оберемо ключову матрицю, яка буде відповідати такій умові: НСД ($|K|$; n) = 1; де K – визначник матриці-ключа, який не дорівнює 0. Як приклад, створимо ключову матрицю розміром 3×3 :

$$K = \begin{bmatrix} 2 & 5 & 7 \\ 3 & 7 & 8 \\ 5 & 8 & 9 \end{bmatrix} \quad (1)$$

Візьмемо слово "МОРОЗИВО", яке має 8 літер, тому доповнимо його символом "А" до 9 літер і отримаємо "МОРОЗИВОА". Тепер перетворимо літери у відповідні числа: М:=16, О:=18, Р:=20, О:=18, З:=9, И:=10, В:=2, О:=18, А:=0. Розіб'ємо на вектори по 3 елементи:

$$\begin{bmatrix} 16 \\ 18 \\ 20 \end{bmatrix}, \begin{bmatrix} 18 \\ 9 \\ 10 \end{bmatrix}, \begin{bmatrix} 2 \\ 18 \\ 0 \end{bmatrix} \quad (2)$$

Виконаємо шифрування кожного елемента за формулою: $E(\bar{x}) = k * \bar{x}$, де $\bar{x}$ – вектор стовбець відкритого тексту, k – ключ-матриця. Множимо кожен вектор на матрицю K , використовуючи модуль 33.

Перший вектор (16,18,20):

$$\begin{bmatrix} 2 & 5 & 7 \\ 3 & 7 & 8 \\ 5 & 8 & 9 \end{bmatrix} * \begin{bmatrix} 16 \\ 18 \\ 20 \end{bmatrix} = \begin{bmatrix} 31 \\ 4 \\ 8 \end{bmatrix} \quad (3)$$

1. $(2*16+5*18+7*20) \bmod 33=31$
2. $(3*16+7*18+8*20) \bmod 33=4$
3. $(5*16+8*18+9*20) \bmod 33=8$

Використовуючи те, що ми пронумерували літери української абетки, перетворюємо отримані числа у літери: 31, 4, 8 - Ю, Ї, Ж.

Другий вектор (18,9,10):

$$\begin{bmatrix} 2 & 5 & 7 \\ 3 & 7 & 8 \\ 5 & 8 & 9 \end{bmatrix} * \begin{bmatrix} 18 \\ 9 \\ 10 \end{bmatrix} = \begin{bmatrix} 19 \\ 32 \\ 21 \end{bmatrix} \quad (4)$$

$$1. (2*18+5*9+7*10) \bmod 33=19$$

$$2. (3*18+7*9+8*10) \bmod 33=32$$

$$3. (5*18+8*9+9*10) \bmod 33=21$$

Перетворюємо отримані числа у букви: 19, 32, 21 - П, Я, С.

Третій вектор (2,18,0):

$$\begin{bmatrix} 2 & 5 & 7 \\ 3 & 7 & 8 \\ 5 & 8 & 9 \end{bmatrix} * \begin{bmatrix} 2 \\ 18 \\ 0 \end{bmatrix} = \begin{bmatrix} 28 \\ 0 \\ 22 \end{bmatrix} \quad (5)$$

$$1. (2*2+5*18+7*0) \bmod 33=28$$

$$2. (3*2+7*18+8*0) \bmod 33=0$$

$$3. (5*2+8*18+9*0) \bmod 33=22$$

Перетворюємо отримані числа у букви: 28, 0, 22 - Ш, А, Т.

У результаті шифрування отримуємо: "ЮЇЖПЯСПАТ".

Тепер дешифруємо отримане повідомлення. Для цього скористаємося формулою: $D(\bar{y})=(K^{-1})*\bar{y}$; де $\bar{y}$ - вектор стовбець зашифрованого повідомлення, K^{-1} – обернена ключ-матриця за модулем 33. Наша обернена матриця матиме вигляд:

$$K^{-1} = \begin{bmatrix} 26 & 11 & 3 \\ 25 & 13 & 2 \\ 22 & 30 & 26 \end{bmatrix} \quad (6)$$

Наступним кроком помножимо обернену матрицю за модулем 33 на вектори-стовпці зашифрованого повідомлення:

$$\begin{bmatrix} 26 & 11 & 3 \\ 25 & 13 & 2 \\ 22 & 30 & 26 \end{bmatrix} * \begin{bmatrix} 31 \\ 4 \\ 8 \end{bmatrix} = \begin{bmatrix} 16 \\ 18 \\ 20 \end{bmatrix} \quad (7)$$

$$\begin{bmatrix} 26 & 11 & 3 \\ 25 & 13 & 2 \\ 22 & 30 & 26 \end{bmatrix} * \begin{bmatrix} 19 \\ 32 \\ 21 \end{bmatrix} = \begin{bmatrix} 18 \\ 9 \\ 10 \end{bmatrix} \quad (8)$$

$$\begin{bmatrix} 26 & 11 & 3 \\ 25 & 13 & 2 \\ 22 & 30 & 26 \end{bmatrix} * \begin{bmatrix} 28 \\ 0 \\ 22 \end{bmatrix} = \begin{bmatrix} 2 \\ 18 \\ 0 \end{bmatrix} \quad (9)$$

У результаті отримуємо ті самі вектори, які у нас були спочатку, це означає, що ми успішно дешифрували повідомлення "ЮГЖПЯСШАТ".

Тобто, в цій роботі нами були розглянуті поняття та алгоритм шифрування Хілла, а також на конкретному прикладі продемонстровано схема шифрування та дешифрування повідомлення за допомогою дій над матрицями.