Світлана Заріцька, Олена Романюк
Науковий керівник: викл. Рудницький С. О.

ШИФР ХІЛЛА

Шифр Хілла – поліграмний шифр підстановки, заснований на лінійній алгебрі. Лестер С. Хілл винайшов цей шифр в 1929, і це був перший шифр, який дозволяв на практиці (хоча і з труднощами) оперувати більш ніж з трьома символами за раз. Подальше обговорення шифру передбачає початкові знання матриць [2].

Шифрування: кожній букві спершу зіставляється число. Для латинського алфавіту часто використовується найпростіша схема: $A = 0$, $B = 1$, …, $Z = 25$, але це не є істотною властивістю шифру.

Блок з n букв розглядається як n-мірний вектор і множиться на $n \times n$ матрицюпо модулю 26. (Якщо як основа модуля використовується число більше 26, то можна використовувати іншу числову схему для зіставлення буквах чисел і додати прогалини і знаки пунктуації.) Матриця повністю є ключем шифру. Матриця повинна бути оборотною в Z_{26}^{n} щоб була можлива операція розшифрування [1].

У наступних прикладах використовуються латинські літери від A до Z, відповідні їм чисельні значення наведені в таблиці:

										0	1	2	3	4	5	6	7	8

T	U	V	W	X	Y	Z
19	20	21	22	23	24	25

Розглянемо повідомлення ‘DOG’ і представлений нижче ключ (GYBNQKURP в буквеному вигляді):

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}.$$

Так як букві ‘D’ відповідає число 3, ‘O’ – 14, ‘G’ – 6, то повідомлення – це вектор $\begin{pmatrix} 3 \\ 14 \\ 6 \end{pmatrix}$.

Тоді зашифрований вектор буде:

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}\begin{pmatrix} 3 \\ 14 \\ 6 \end{pmatrix}=\begin{pmatrix} 360 \\ 323 \\ 388 \end{pmatrix}=\begin{pmatrix} 22 \\ 11 \\ 24 \end{pmatrix},$$

що відповідає шифротексту ‘WLY’. Тепер припустимо, що наше повідомлення було ‘GOD’ або $\begin{pmatrix} 6 \\ 14 \\ 3 \end{pmatrix}$.

Тепер зашифрований вектор буде:

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}\begin{pmatrix} 6 \\ 14 \\ 3 \end{pmatrix}=\begin{pmatrix} 375 \\ 332 \\ 403 \end{pmatrix}=\begin{pmatrix} 11 \\ 20 \\ 13 \end{pmatrix},$$

що відповідає шифротексту ‘LUN’. Видно, що кожна буква шифротекста змінилася. Шифр Хілла досяг дифузії по Шеннону, і *n*-розмірний шифр Хілла може досягати дифузії *n* символів за раз.

У міру збільшення розмірності ключа шифр швидко стає недоступним для розрахунків на папері людиною. Шифр Хілла розмірності 6 був реалізований механічно.

Хілл з партнером отримали патент на цей пристрій (U.S. Patent 1845947), який виконував множення матриці 6×6 по модулю 26 за допомогою системи шестерень і ланцюгів. Розташування шестерень (а значить і ключ) не можна було змінювати для конкретного пристрою, тому з метою безпеки рекомендувалося потрійне шифрування. Така комбінація була дуже сильною для 1929 року, і вона показує, що Хілл безсумнівно розумів концепції конфузії і дифузії.

Список використаних джерел:

1. Murray Eisenberg, Hill ciphers and modular linear algebra, mimeographed notes, University of Massachusetts, 1998, 19 pages.
2. Криптографія. Введення [Електронний ресурс] / В. С. Пилиди // Ростов-на-Дону – 2009. – Режим доступу: http://www.ict.edu.ru/ft/005568/rsu596.pdf.

Олександра Іванова
Науковий керівник: к. п. н Шкуренко О. В.

ВИКОРИСТАННЯ ПРЕЗЕНТАЦІЙ НА УРОКАХ В ПОЧАТКОВІЙ ШКОЛІ

Сьогодні процес інформатизації охопив всі сторони життя сучасного суспільства. Цей процес має кілька напрямків, до яких, безумовно, слід віднести інформатизацію освіти. Вона є першоосновою глобальної