СОДЕРЖАНИЕ

1 Задание на практическую работу

Целью работы является приобретение навыков программной реализации и криптоанализа применительно к блочному шифру Хилла.

В рамках практической работы необходимо выполнить следующее:

1) написать программную реализацию следующих шифров:
   - шифр Хилла;
   - рекуррентный шифр Хилла;
2) изучить методы криптоанализа блочных шифров с использованием дополнительных источников;
3) провести криптоанализ данных шифров;
4) подготовить отчет о выполнении работы.

2 Краткая теоретическая часть

2.1 Описание шифров

Шифр Хилла представляет собой пример блочного шифра, основанного на матричных преобразованиях с использованием арифметики остатков. Данный шифр устроен следующим образом.

Открытый текст рассматривается как последовательность символов некоторого алфавита A мощностью m, которые представляются элементами множества $\mathbb{Z}_m$. Перед зашифрованием открытый текст разбивается на блоки длиной n, и каждый блок представляется в виде n-мерного вектора.

Ключом шифра является квадратная матрица размера $n \times n$, составленная из элементов множества $\mathbb{Z}_m$: $K = \left(k_{i,j}\right)_{i=1,j=1}^{n,n}$, $k_{i,j} \in \mathbb{Z}_m$. Эта матрица должна быть обратима в $\mathbb{Z}_m$, чтобы была возможна операция расшифрования. Матрица будет являться обратимой только в том случае, если ее детерминант $|K|$ удовлетворяет следующим двум условиям: $|K| \neq 0$ и $\text{НОД}(|K|, m) = 1$.

Операция зашифрования заключается в том, что ключевая матрица умножается на вектор–столбец $X = (x_1, \ldots, x_n)^T$, соответствующий блоку открытого текста:

$$Y = E_K(X) = K(x_1, \ldots, x_n)^T = (y_1, \ldots, y_n)^T.$$

Для того, чтобы расшифровать шифртекст, необходимо разбить его на блоки длиной n, представить каждый блок в виде вектора $Y = (y_1, \ldots, y_n)^T$ и выполнить обратное умножение:

$$X = D_K(Y) = K^{-1}(y_1, \ldots, y_n)^T = (x_1, \ldots, x_n)^T.$$

В случае рекуррентного шифра Хилла для каждого блока открытого текста формируется своя ключевая матрица. Для этого задаются две обратимые матрицы K_1 и K_2, которые используются для зашифрования первых двух блоков открытого текста. После этого для каждого последующего блока вычисляется новая ключевая матрица на основе двух предыдущих.

$$K_i = K_{i-1}K_{i-2}.$$

Для расшифрования шифртекста, полученного с помощью рекуррентного шифра Хилла, необходимо найти обратные матрицы для матриц K_1 и K_2, после чего все последующие обратные матрицы могут быть вычислены на основании предыдущих:

$$K_i^{-1} = K_{i-2}^{-1}K_{i-1}^{-1}.$$

2.2 Методы криптоанализа шифров

Шифр Хилла – блочный шифр, основывающийся на линейных операциях, поэтому данный шифр уязвим к атаке по открытому тексту [1]. Для совершения данной атаки необходимо знать количество строк квадратного ключа – n и m пар комбинаций закрытый/открытый блок текста длины n. При наличии описанных выше знаний атака совершается по следующему алгоритму [2]:

1) Из открытого текста берется m последовательностей открытых символов длинной n и сопоставленные им последовательности закрытого текста.
2) Запишем последовательности символов открытого текста в виде матрицы P размера nxn и последовательности символов закрытого текста в виде матрицы C размера nxn, выпишем данные матрицы в формуле (2.2.1), так же стоит отметить, что матрица P должна быть обратима по модулю 26. В случае если P необратима необходимо выбрать другую.

$$P = \begin{bmatrix} x_{11} & x_{12} & x_{13} & \cdots & x_{1n} \\ x_{21} & x_{22} & x_{23} & \cdots & x_{2n} \\ x_{31} & x_{32} & x_{33} & \cdots & x_{3n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ x_{n1} & x_{n2} & x_{n3} & \cdots & x_{nn} \end{bmatrix}$$
$$C = \begin{bmatrix} y_{11} & y_{12} & y_{13} & \cdots & y_{1n} \\ y_{21} & y_{22} & y_{23} & \cdots & y_{2n} \\ y_{31} & y_{32} & y_{33} & \cdots & y_{3n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ y_{n1} & y_{n2} & y_{n3} & \cdots & y_{nn} \end{bmatrix} \qquad (2.2.1)$$

3) После чего для вычисления ключа необходимо воспользоваться матричной алгеброй и применить формулу (2.2.2), после чего полученную матрицу необходимо транспонировать.

$$L = P^{-1} * C$$
$$K = L^{T} \qquad (2.2.2)$$

где L – вычисляемая матрица;

P – матрица составленная из символов открытого текста;

C – матрица составленная из символов закрытого текста;

K – ключ.

Отдельно стоит рассмотреть взлом данного шифра перебором. Предположим, что мы знаем количество строк/столбцов матрицы ключа, тогда при его размерности nxn существует соответственно m^{n^2} вариаций ключа, где m – мощность алфавита, но так как при формировании ключа мы накладывает ограничения на матрицу, перебор осуществляется по меньшему количеству ключей. Как можно заметить, перебор возможен только если ключ – матрица небольшой размерности. Существует еще одна вариация взлома перебором при известной размерности ключа. В ходе данного метода нам необходимо подбирать не целые матрицы размера nxn, а строки длинной n. При этом взлом осуществляется по следующему алгоритму [3]:

1) Необходимо разбить текст на блоки размера n;
2) При переборе перемножаем взятую строку ключа и блок текста длинной n;
3) Применяя статистический анализ, находим наиболее подходящие n строк;
4) Перебирая n! матриц каждая из которых, отличается от предыдущей одной транспозицией, находим ключ.

Стоит отметить, что не смотря на возможность атаки простым перебором ключей, данный метод является не эффективным и не используется.

Для рекуррентного шифра Хилла наиболее оптимальным является атака по открытому тексту. Отличие заключается в том, что необходимо установить не один ключ, а два. Злоумышленник, собирая пары значений сопоставленных символов из открытого и закрытого текста и путем решения уравнений получает ключи. Подробнее данный алгоритм описан ниже:

1) Из открытого текста берется m последовательностей открытых символов длинной n и сопоставленные им последовательности закрытого текста. Причем для нахождения первого ключа берутся первые n символов, а для нахождения второго – вторые n символов.
2) Запишем последовательности символов открытого текста в виде матрицы P_i размера nxn и последовательности символов закрытого текста в виде матрицы C_i размера nxn, выпишем данные матрицы в формуле (2.2.3), так же стоит отметить, что матрица P_i должна быть обратима по модулю 26. В случае если P_i необратима необходимо выбрать другую.

$$P_i = \begin{bmatrix} x_{11} & x_{12} & x_{13} & \cdots & x_{1n} \\ x_{21} & x_{22} & x_{23} & \cdots & x_{2n} \\ x_{31} & x_{32} & x_{33} & \cdots & x_{3n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ x_{n1} & x_{n2} & x_{n3} & \cdots & x_{nn} \end{bmatrix}$$
$$C_i = \begin{bmatrix} y_{11} & y_{12} & y_{13} & \cdots & y_{1n} \\ y_{21} & y_{22} & y_{23} & \cdots & y_{2n} \\ y_{31} & y_{32} & y_{33} & \cdots & y_{3n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ y_{n1} & y_{n2} & y_{n3} & \cdots & y_{nn} \end{bmatrix} \tag{2.2.3}$$

3) После чего для вычисления ключа необходимо воспользоваться матричной алгеброй и применить формулу (2.2.4).

$$\begin{gathered} L_i = {P_i}^{-1} * C_i \\ K_i = L_i^T \end{gathered} \tag{2.2.4}$$

где L – вычисляемая матрица;

P_i – матрица, составленная из символов открытого текста;

C_i – матрица, составленная из символов закрытого текста;

K_i – ключ матрица.

Отдельно стоит заметить, что взлом перебором является еще более неэффективным, чем при атаке на обычный шифр Хилла.

3 Примеры шифрования

Шифр Хилла. Для начала условимся во всех обозначениях (3.1), используемых далее, пусть:

$$
\begin{gathered}
A = \{a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z\}; \\
|A| = m = 26; \\
X = \{x = (x_1, x_2, x_3, \dots, x_r), \ \ x_i \in A\}; \\
Y = \{y = (y_1, y_2, y_3, \dots, y_r), \ \ y_i \in A\}; \\
k = \begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \\
n = 3
\end{gathered}
\tag{3.1}
$$

где A – алфавит;

m – мощность алфавита;

X – открытый текст;

x_i – элемент открытого текста;

Y – закрытый текст;

y_i – элемент закрытого текста;

k – ключ;

n – количество строк/столбцов ключа матрицы.

Возьмем для примера $X = \text{abcdefg}$, используя ключ, описанный выше, зашифруем данный открытый текст, для этого:

1) Сопоставим символам открытого текста их численные эквиваленты равные их порядковому номеру в алфавите, при нумерации в нем с нуля (3.2):

$$
\begin{gathered}
a = 0 \\
b = 1 \\
c = 2 \\
d = 3 \\
e = 4 \\
f = 5 \\
g = 6
\end{gathered}
\tag{3.2}
$$

2) Открытый текст представляется в виде (3.3):

$$X = (0, 1, 2, 3, 4, 5, 6) \tag{3.3}$$

3) Разбиваем открытый текст на блоки размера n. Заметим, что при таком разбиении последний блок состоит не из n символов, а из меньшего количества. В таких ситуация необходимо дополнить текст недостающим количеством символов (3.4):

$$\begin{gathered} I = n - L \bmod n \\ I = 3 - 7 \bmod 3 = 2 \end{gathered} \tag{3.4}$$

где I – количество недостающих символов;

n – количество строк/столбцов ключа матрицы;

L – длина открытого текста.

Дополненные символы выбираются по особому правилу, это могут быть случайно добавленные символы, либо выбранные неким алгоритмом. В данном случае: $I = 2$, добавим, к примеру инициалы, то есть «I» и «O», при этом в численных эквивалентах данные символы являются: 8 и 14 соответственно. Разбиение на блоки размером n, в данном случае при $n = 3$ приведены в формуле (3.5):

$$\begin{gathered} X_1 = (x_1, x_2, x_3) = (0, 1, 2) \\ X_2 = (x_4, x_5, x_6) = (3, 4, 5) \\ X_3 = (x_7, x_8, x_9) = (6, 8, 14) \end{gathered} \tag{3.5}$$

4) Для зашифрования необходимо умножить по модулю мощности алфавита ключевую матрицу на вектор столбец, соответствующий блоку открытого текста, данная операция приведена в формуле (3.6).

$$\begin{gathered} Y_i = k * X_i \\ Y_1 = \begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} * (0,1,2)^T = (0, 10, 21) \\ Y_2 = \begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} * (3,4,5)^T = (15, 23, 21) \end{gathered} \tag{3.6}$$

$$Y_3 = \begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} * (6{,}8{,}14)^T \; = \; (8, 8, 24)$$

где Y_i – i-ый блок шифротекста размером n;

k – ключевая матрица;

X_i – i-ый блок открытого текста размером n.

Тогда $Y \; = \; akvpxviiy \; = \; (0{,}10{,}21{,}15{,}23{,}21{,}8{,}8{,}24)$

Теперь проведем обратную операцию, то есть расшифруем полученную последовательность. Для этого необходимо найти матрицу обратную ключу матрице по модулю мощности алфавита. Проведем необходимые вычисления для нахождения обратной матрицы (3.7).

$$k \; = \begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$$
$$k^{-1} = \frac{1}{|k|} * k^{*T} \tag{3.7}$$

где k^{-1} – матрица обратная ключу матрице k;

|k| – определитель k;

k^{*T}– транспонированная матрица алгебраических дополнений.

1) Найдем определить и обратное к нему число по модулю 26 (3.8):

$$|k| = \begin{vmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{vmatrix} = ((6 * 16 * 15 + 24 * 10 * 20 + 13 * 17 * 1) \; -$$
$$- (1 * 16 * 20 \; + \; 13 * 24 * 15 \; + \; 10 * 17 * 6)) \bmod 26 \;\; = \; 441 \bmod 26 \; = \; 25$$
$$|k^{-1}| * |k| = 1 \bmod 26$$
$$|k^{-1}| = 25 \tag{3.8}$$

2) Найдем транспонированную матрицу алгебраических дополнений, все элементы взяты по модулю 26 (3.9):

$$k = \begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \tag{3.9}$$

$$M_{11} = \; \begin{vmatrix} 16 & 10 \\ 17 & 15 \end{vmatrix} = 70 \qquad M_{12} = \begin{vmatrix} 13 & 10 \\ 20 & 15 \end{vmatrix} = 5 \qquad M_{13} = \begin{vmatrix} 13 & 16 \\ 20 & 17 \end{vmatrix} = -99$$

$$M_{21} = \begin{vmatrix} 24 & 1 \\ 17 & 15 \end{vmatrix} = 343 \qquad M_{22} = \begin{vmatrix} 6 & 1 \\ 20 & 15 \end{vmatrix} = 70 \qquad M_{23} = \begin{vmatrix} 6 & 24 \\ 20 & 17 \end{vmatrix} = -378$$

$$M_{31} = \begin{vmatrix} 24 & 1 \\ 16 & 10 \end{vmatrix} = 224 \qquad M_{32} = \begin{vmatrix} 6 & 1 \\ 13 & 10 \end{vmatrix} = 47 \qquad M_{33} = \begin{vmatrix} 6 & 24 \\ 13 & 16 \end{vmatrix} = -216$$

$$k^* = \begin{pmatrix} 70 & -5 & -99 \\ 343 & 70 & -378 \\ 224 & 47 & -216 \end{pmatrix} \tag{3.9}$$

$$k^{*T} = \begin{pmatrix} 70 & -343 & 224 \\ 5 & 70 & -47 \\ -99 & 378 & -216 \end{pmatrix} \bmod 26 = \begin{pmatrix} 18 & 21 & 16 \\ 5 & 18 & 5 \\ 5 & 14 & 18 \end{pmatrix}$$

3) Используя формулу (9), найдем обратную матрицу (3.10):

$$k^{*T} = \begin{pmatrix} 18 & 21 & 16 \\ 5 & 18 & 5 \\ 5 & 14 & 18 \end{pmatrix}$$

$$k^{-1} = 25 * \begin{pmatrix} 18 & 21 & 16 \\ 5 & 18 & 5 \\ 5 & 14 & 18 \end{pmatrix} \bmod 26 = \begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} \tag{3.10}$$

4) Для зашифрования необходимо умножить по модулю мощности алфавита ключевую матрицу на вектор столбец, соответствующий блоку открытого текста, данная операция приведена в формуле (3.11):

$$X_i = k^{-1} * Y_i$$

$$X_1 = \begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} * (0,10,21)^T = (0,1,2)$$

$$X_2 = \begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} * (15,23,21)^T = (3,4,5) \tag{3.11}$$

$$X_3 = \begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} * (8,8,24)^T = (6,8,14)$$

Тогда X = abcdefgio.

Рекурентный шифр Хилла. Данный шифр отличается от простого шифра Хилла заданием первых двух матриц и последующим формированием ключевой матрицы на двух предыдущих для каждого блока текста начиная с третьего. Перед началом шифрования условимся в обозначениях, используемых далее (3.12):

$$A = \{a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z\};$$
$$|A| = m = 26;$$
$$X = \{x = (x_1, x_2, x_3, \dots, x_r),\quad x_i \in A\};$$
$$Y = \{y = (y_1, y_2, y_3, \dots, y_r),\quad y_i \in A\};$$
$$k_1 = \begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \qquad (3.12)$$
$$n_1 = 3$$
$$k_2 = \begin{pmatrix} 3 & 1 & 5 \\ 0 & 4 & 3 \\ 2 & 1 & 7 \end{pmatrix}$$
$$n_2 = 3$$
$$n_1 = n_2 = n$$

где A – алфавит;

m – мощность алфавита;

X – открытый текст;

x_i – элемент открытого текста;

Y – закрытый текст;

y_i – элемент закрытого текста;

k_1 – первый ключ;

n_1 – количество строк/столбцов первого ключа матрицы;

k_2 – второй ключ;

n_2 – количество строк/столбцов второго ключа матрицы;

n – количество строк/столбцов ключа матрицы.

Возьмем для примера X = abcdefg, используя ключи, описанные выше, зашифруем данный открытый текст, для этого:

1) Сопоставим символам открытого текста их численные эквиваленты равные их порядковому номеру в алфавите, при нумерации в нем с нуля (3.13):

$$a = 0$$
$$b = 1$$
$$c = 2 \qquad (3.13)$$
$$d = 3$$
$$e = 4$$

$$f = 5$$

$$g = 6$$

2) Открытый текст представляется в виде (3.14):

$$X = (0, 1, 2, 3, 4, 5, 6) \tag{3.14}$$

3) Разбиваем открытый текст на блоки размера n. Заметим, что при таком разбиении последний блок состоит не из n символов, а из меньшего количества. В таких ситуация необходимо дополнить текст недостающим количеством символов (3.15):

$$\begin{gathered} I = n - L \bmod n \\ I = 3 - 7 \bmod 3 = 2 \end{gathered} \tag{3.15}$$

где I – количество недостающих символов;

n – количество строк/столбцов ключа матрицы;

L – длина открытого текста.

Дополненные символы выбираются по особому правила, это могут быть случайно добавленные символы, либо выбранные неким алгоритмом. В данном случае: $I = 2$, добавим, к примеру инициалы, то есть «I» и «O», при этом в численных эквивалентах данные символы являются: 8 и 14 соответственно. Разбиение на блоки размером n, в данном случае при $n = 3$ приведены в формуле (3.16):

$$\begin{gathered} X_1 = (x_1, x_2, x_3) = (0, 1, 2) \\ X_2 = (x_4, x_5, x_6) = (3, 4, 5) \\ X_3 = (x_7, x_8, x_9) = (6, 8, 14) \end{gathered} \tag{3.16}$$

4) В случае с рекуррентным шифром Хилла первые два блока открытого текста шифруются первым и вторым ключом матрицей соответственно. Выполним эту операцию (3.17):

$$Y_i = k_i * X_i$$

$$Y_1 = \begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} * (0,1,2)^T = (0,10,21)$$

$$Y_2 = \begin{pmatrix} 3 & 1 & 5 \\ 0 & 4 & 3 \\ 2 & 1 & 7 \end{pmatrix} * (3,4,5)^T = (12,5,19) \quad (3.17)$$

5) Начиная с третьего блока и для каждого последующего ключ матрица формируется на основе двух предыдущих по формуле (3.18):

$$k_i = k_{i-1} * k_{i-2} \quad (3.18)$$

где k_i – матрица ключ для i-го блока текста.

Рассчитаем ключ для третьего блока текста (3.19):

$$k_3 = k_1 * k_2 = \begin{pmatrix} 3 & 1 & 5 \\ 0 & 4 & 3 \\ 2 & 1 & 7 \end{pmatrix} * \begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} =$$

$$= \begin{pmatrix} 131 & 173 & 88 \\ 112 & 115 & 85 \\ 165 & 183 & 117 \end{pmatrix} \bmod 26 = \begin{pmatrix} 1 & 17 & 10 \\ 8 & 11 & 7 \\ 9 & 1 & 13 \end{pmatrix} \quad (3.19)$$

6) Зашифруем третий блок открытого текста (3.20):

$$Y_3 = \begin{pmatrix} 1 & 17 & 10 \\ 8 & 11 & 7 \\ 9 & 1 & 13 \end{pmatrix} * (6,8,14)^T = (22,0,10) \quad (3.20)$$

Тогда $Y = akvmftwak = (0,10,21,12,5,19,22,0,10)$

Теперь проведем обратную операцию, то есть расшифруем полученную последовательность. Для этого необходимо найти матрицы обратные ключам, использованным при шифровании каждого конкретного блока. Для этого воспользуемся формулой нахождения обратны матриц (3.21)

$$k_i^{-1} = \frac{1}{|k_i|} * k_i^{*T} \quad (3.21)$$

где k_i^{-1} – матрица обратная ключу матрице k_i;

$|k_i|$ – определитель k_i;

k_i^{*T} – транспонированная матрица алгебраических дополнений.

5) Найдем обратные матрицы для первых двух ключей

6) Найдем определить первого ключа и обратное к нему число по модулю 26 (3.22):

$$|k_1| = \begin{vmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{vmatrix} = ((6*16*15+24*10*20+13*17*1) -$$
$$-(1*16*20 + 13*24*15 + 10*17*6)) \bmod 26 = 441 \bmod 26 = 25 \qquad (3.22)$$
$$|k^{-1}| * |k| = 1 \bmod 26$$
$$|k^{-1}| = 25$$

7) Найдем транспонированную матрицу алгебраических дополнений, все элементы взяты по модулю 26 (3.23):

$$k_1 = \begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$$
$$M_{11} = \begin{vmatrix} 16 & 10 \\ 17 & 15 \end{vmatrix} = 70 \qquad M_{12} = \begin{vmatrix} 13 & 10 \\ 20 & 15 \end{vmatrix} = 5 \qquad M_{13} = \begin{vmatrix} 13 & 16 \\ 20 & 17 \end{vmatrix} = -99$$
$$M_{21} = \begin{vmatrix} 24 & 1 \\ 17 & 15 \end{vmatrix} = 343 \qquad M_{22} = \begin{vmatrix} 6 & 1 \\ 20 & 15 \end{vmatrix} = 70 \qquad M_{23} = \begin{vmatrix} 6 & 24 \\ 20 & 17 \end{vmatrix} = -378 \qquad (3.23)$$
$$M_{31} = \begin{vmatrix} 24 & 1 \\ 16 & 10 \end{vmatrix} = 224 \qquad M_{32} = \begin{vmatrix} 6 & 1 \\ 13 & 10 \end{vmatrix} = 47 \qquad M_{33} = \begin{vmatrix} 6 & 24 \\ 13 & 16 \end{vmatrix} = -216$$
$$k^* = \begin{pmatrix} 70 & -5 & -99 \\ 343 & 70 & -378 \\ 224 & 47 & -216 \end{pmatrix}$$
$$k^{*T} = \begin{pmatrix} 70 & -343 & 224 \\ 5 & 70 & -47 \\ -99 & 378 & -216 \end{pmatrix} \bmod 26 = \begin{pmatrix} 18 & 21 & 16 \\ 5 & 18 & 5 \\ 5 & 14 & 18 \end{pmatrix}$$

8) Используя формулу (24), найдем обратную матрицу (3.24):

$$k^{*T} = \begin{pmatrix} 18 & 21 & 16 \\ 5 & 18 & 5 \\ 5 & 14 & 18 \end{pmatrix}$$
$$k^{-1} = 25 * \begin{pmatrix} 18 & 21 & 16 \\ 5 & 18 & 5 \\ 5 & 14 & 18 \end{pmatrix} \bmod 26 = \begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} \qquad (3.24)$$

9) Проведем аналогичные операции для нахождения обратной матрицы для второго ключа.
10) Найдем определить второго ключа и обратное к нему число по модулю 26 (3.25):

$$|k_2| = \begin{vmatrix} 3 & 1 & 5 \\ 0 & 4 & 3 \\ 2 & 1 & 7 \end{vmatrix} = (41) \bmod 26 = 15$$
$$|{k_2}^{-1}| * |k_2| = 1 \bmod 26 \tag{3.25}$$
$$|{k_2}^{-1}| = 7$$

11) Найдем транспонированную матрицу алгебраических дополнений, все элементы взяты по модулю 26 (3.26):

$$ {k_2}^{*T} = \begin{pmatrix} 25 & -2 & -17 \\ 6 & 11 & -9 \\ -8 & -1 & 12 \end{pmatrix} \bmod 26 = \begin{pmatrix} 25 & 24 & 9 \\ 6 & 11 & 17 \\ 18 & 25 & 12 \end{pmatrix} \tag{3.26}$$

12) Используя формулу (24), найдем обратную матрицу (3.27):

$$ {k_2}^{-1} = \begin{pmatrix} 19 & 12 & 11 \\ 16 & 25 & 15 \\ 22 & 19 & 6 \end{pmatrix} \tag{3.27}$$

13) Теперь необходимо найти обратную матрицу для третьего ключа шифрования, ее можно найти, основываясь на обратных матрицах для двух предыдущих матриц по формуле (3.28):

$$ {k^{-1}}_i = {k^{-1}}_{i-2} * {k^{-1}}_{i-1} \tag{3.28}$$

Применим данную формулу (3.29):

$$ {k^{-1}}_3 = {k^{-1}}_1 * {k^{-1}}_2 = \begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} * \begin{pmatrix} 19 & 12 & 11 \\ 16 & 25 & 15 \\ 22 & 19 & 6 \end{pmatrix} = $$
$$ = \begin{pmatrix} 10 & 21 & 15 \\ 1 & 19 & 9 \\ 13 & 2 & 17 \end{pmatrix} \tag{3.29}$$

14) После чего необходимо расшифровать все блоки шифртекста (3.30):

$$\mathrm{X_i} = {k_i}^{-1} * \mathrm{Y_i}$$

$$\mathrm{X_1} = \begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} * (0{,}10{,}21)^{\mathrm{T}} = (0, 1, 2)$$

$$\mathrm{X_2} = \begin{pmatrix} 19 & 12 & 11 \\ 16 & 25 & 15 \\ 22 & 19 & 6 \end{pmatrix} * (12{,}5{,}19)^{\mathrm{T}} = (3, 4, 5) \tag{3.30}$$

$$\mathrm{X_3} = \begin{pmatrix} 10 & 21 & 15 \\ 1 & 19 & 9 \\ 13 & 2 & 17 \end{pmatrix} * (22{,}0{,}10)^{\mathrm{T}} = (6, 8, 14)$$

Тогда $\mathrm{X} = \mathrm{abcdefgio} = (0{,}1{,}2{,}3{,}4{,}5{,}6{,}8{,}14)$.

4 Программная реализация шифров

Программная реализация была выполнена на языке python, с полным кодом можно ознакомиться по ссылке: https://github.com/il3241/crypto_pr2_github.

Примеры выполнения программного кода для последовательностей, показанных в разделе ручного зашифрования и расшифрования:

Шифр Хилла.

Зашифрование.

Пример входных данных

- Текст для зашифрования: abcdefgio
- Размер блока: 3
- Ключевая матрица: $\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$

Пример выходных данных представлен на рисунке 1.

```
abcdefgio
3
6 24 1
13 16 10
20 17 15
en
close text:
 akvpxviiy
```

Рисунок 1.

Расшифрование.

Пример входных данных

- Текст для зашифрования: akvpxviiy
- Размер блока: 3
- Ключевая матрица: $\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$

Пример выходных данных представлен на рисунке 2.

```
akvpxviiy
3
6 24 1
13 16 10
20 17 15
de
open text:
 abcdefgio
```

Рисунок 2.

Рекуррентный шифр Хилла.

Зашифрование.

Пример входных данных

- Текст для зашифрования: abcdefgio
- Размер блока: 3
- Первая ключевая матрица: $\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$
- Вторая ключевая матрица: $\begin{pmatrix} 3 & 1 & 5 \\ 0 & 4 & 3 \\ 2 & 1 & 7 \end{pmatrix}$

Пример выходных данных представлен на рисунке 3.

```
abcdefgio
3
6 24 1
13 16 10
20 17 15
3 1 5
0 4 3
2 1 7
en
close text:
 akvmftwak
```

Рисунок 3.

Расшифрование.

Пример входных данных

- Текст для зашифрования: akvmftwak
- Размер блока: 3
- Первая ключевая матрица: $\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$
- Вторая ключевая матрица: $\begin{pmatrix} 3 & 1 & 5 \\ 0 & 4 & 3 \\ 2 & 1 & 7 \end{pmatrix}$

Пример выходных данных представлен на рисунке 4.

```
akvmftwak
3
6 24 1
13 16 10
20 17 15
3 1 5
0 4 3
2 1 7
de
open text:
 abcdefgio
```

Рисунок 4.

5 Примеры криптоанализа

Оптимальный криптоанализ шифра Хилла заключается, как было уже написано ранее, в использовании атаки по открытому тексту. Для этого необходимо перехватить m пар блоков открытого и сопоставленных им блоков закрытого текста, после чего составив матрицы из них матрицы размера nxn применить формулу (2.2.2) и получить ключ, для применения формулы (2.2.2) необходимо, чтобы матрица составленная из элементов открытого текста была обратима по модулю 26, в случае если она этим свойством не обладает, необходимо использовать другие пары блоков. Пример такого криптоанализа написан ниже. Условимся в обозначениях, используемых далее (5.1):

$$X = \mathrm{cryptogrbphy} = (2,17,24,15,19,14,6,17,1,15,7,24)$$
$$K = \begin{pmatrix} 3 & 1 & 5 \\ 0 & 4 & 3 \\ 2 & 1 & 7 \end{pmatrix} \tag{5.1}$$
$$n = 3$$
$$Y = \mathrm{nkheorotkqwx} = (13,10,7,4,14,17,14,19,10,16,22,23)$$

где X – открытый текст;

K – ключ матрица;

n – количество строк/столбцов ключа матрицы;

Y – закрытый текст.

В рассматриваемом примере размер блока равен 3. Пусть были перехвачены первые три блока открытого и закрытого текста (5.2):

$$\begin{aligned} o_1 &= (2,17,24) & c_1 &= (13,10,7) \\ o_2 &= (15,19,14) & c_2 &= (4,14,17) \\ o_3 &= (6,17,1) & c_3 &= (14,19,10) \end{aligned} \tag{5.2}$$

где o_i – i-ый блок открытого текста;

c_i – i-ый блок закрытого текста.

Теперь необходимо составить матрицы из перехваченных блоков (5.3):

$$P = \begin{pmatrix} 2 & 17 & 24 \\ 15 & 19 & 14 \\ 6 & 17 & 1 \end{pmatrix} \qquad C = \begin{pmatrix} 13 & 10 & 7 \\ 4 & 14 & 17 \\ 14 & 19 & 10 \end{pmatrix} \tag{5.3}$$

где P – матрица из элементов открытого текста;

C – матриц из элементов закрытого текста.

Необходимо проверить обратимость матрицы P. В данном случае эта матрица обратима (5.4)

$$|\mathrm{P}| = \begin{vmatrix} 2 & 17 & 24 \\ 15 & 19 & 14 \\ 6 & 17 & 1 \end{vmatrix} = 4119 \bmod 26 = 11$$
$$|\mathrm{P}|^{-1} * |\mathrm{P}| = 1 \bmod 26 \tag{5.4}$$
$$|\mathrm{P}|^{-1} = 19$$

Теперь необходимо найти матрицу обратную P. Для ее нахождения необходимо воспользоваться формулой (5.5):

$$\mathrm{P}^{-1} = \frac{1}{|\mathrm{P}|} * \mathrm{P}^{*\mathrm{T}} \tag{5.5}$$

Число обратное определителю матрицы P уже было найдено в (5.4) поэтому необходимо найти транспонированную матрицу алгебраических дополнений. Для этого выполним (5.6):

$$\mathrm{P} = \begin{pmatrix} 2 & 17 & 24 \\ 15 & 19 & 14 \\ 6 & 17 & 1 \end{pmatrix}$$
$$\mathrm{M}_{11} = \begin{vmatrix} 19 & 14 \\ 17 & 1 \end{vmatrix} = -219 \quad \mathrm{M}_{12} = \begin{vmatrix} 15 & 14 \\ 6 & 1 \end{vmatrix} = -69 \quad \mathrm{M}_{13} = \begin{vmatrix} 15 & 19 \\ 6 & 1 \end{vmatrix} = 141$$
$$\mathrm{M}_{21} = \begin{vmatrix} 17 & 24 \\ 17 & 1 \end{vmatrix} = -391 \quad \mathrm{M}_{22} = \begin{vmatrix} 2 & 24 \\ 6 & 1 \end{vmatrix} = -142 \quad \mathrm{M}_{23} = \begin{vmatrix} 2 & 17 \\ 6 & 17 \end{vmatrix} = -68$$
$$\mathrm{M}_{31} = \begin{vmatrix} 17 & 24 \\ 19 & 14 \end{vmatrix} = -218 \quad \mathrm{M}_{32} = \begin{vmatrix} 2 & 24 \\ 16 & 14 \end{vmatrix} = -332 \quad \mathrm{M}_{33} = \begin{vmatrix} 2 & 17 \\ 15 & 19 \end{vmatrix} = -217 \tag{5.6}$$
$$\mathrm{P}^{*} = \begin{pmatrix} -219 & -69 & 141 \\ -391 & -142 & -68 \\ -218 & -332 & -217 \end{pmatrix}$$
$$\mathrm{P}^{*\mathrm{T}} = \begin{pmatrix} -219 & -391 & 218 \\ -69 & -142 & -332 \\ 141 & -68 & -217 \end{pmatrix} \bmod 26 = \begin{pmatrix} 15 & 25 & 10 \\ 10 & 14 & 6 \\ 11 & 10 & 17 \end{pmatrix}$$

Теперь необходимо найти матрицу обратную P по формуле (5.7):

$$P^{-1} = 19 * \begin{pmatrix} 15 & 25 & 10 \\ 10 & 14 & 6 \\ 11 & 10 & 17 \end{pmatrix} \bmod 26 = \begin{pmatrix} 25 & 19 & 18 \\ 11 & 6 & 16 \\ 1 & 18 & 11 \end{pmatrix} \quad (5.7)$$

После нахождения обратной матрицы необходимо применить формулу матрицы ключа (5.8):

$$L = P^{-1} * C$$
$$K = L^T$$
$$L = \begin{pmatrix} 25 & 19 & 18 \\ 11 & 6 & 16 \\ 1 & 18 & 11 \end{pmatrix} * \begin{pmatrix} 13 & 10 & 7 \\ 4 & 14 & 17 \\ 14 & 19 & 10 \end{pmatrix} = \begin{pmatrix} 3 & 0 & 2 \\ 1 & 4 & 1 \\ 5 & 3 & 7 \end{pmatrix} \quad (5.8)$$
$$K = \begin{pmatrix} 3 & 1 & 5 \\ 0 & 4 & 3 \\ 2 & 1 & 7 \end{pmatrix}$$

Что и является ключом, использованным при шифровании.

Криптоанализ рекуррентного шифра Хилла состоит из тех же шагов, что и анализ обычного шифра Хилла, с исключением в том, что необходимо установить не одну ключ матрицу, а две. Введем используемые далее обозначения и проведем криптоанализ (5.9):

$$X_1 = \text{crfjtogrbphy} = (2,17,5,9,19,14,6,17,1,15,7,24)$$
$$X_2 = \text{ptehrbgrbphy} = (15,19,4,7,17,1,6,17,1,15,7,24)$$
$$K_1 = \begin{pmatrix} 3 & 1 \\ 0 & 3 \end{pmatrix}$$
$$K_2 = \begin{pmatrix} 3 & 25 \\ 13 & 18 \end{pmatrix} \quad (5.9)$$
$$n = 2$$
$$Y_1 = \text{xzgtppsdjtvi} = (23,25,6,19,15,15,18,3,9,19,21,8)$$
$$Y_2 = \text{mffwxcsdjtvi} = (12,5,5,22,23,2,18,3,9,19,21,8)$$

где X_i – открытый текст;

K_1 – первый ключ матрица;

K_2 – первый ключ матрица;

n – количество строк/столбцов ключа матрицы;

Y_i – закрытый текст.

В рассматриваемом примере размер блока равен 2. Пусть были перехвачены первые блоки двух открытых и соответствующих им закрытых текстов (5.10):

$$o_1 = (2{,}17) \qquad c_1 = (23{,}25)$$
$$o_2 = (15{,}19) \qquad c_2 = (12{,}5) \tag{5.10}$$

где o_i – i-ый блок открытого текста;

c_i – i-ый блок закрытого текста.

Теперь необходимо составить матрицы из перехваченных блоков (5.11):

$$P = \begin{pmatrix} 2 & 17 \\ 15 & 19 \end{pmatrix} \qquad C = \begin{pmatrix} 23 & 25 \\ 12 & 5 \end{pmatrix} \tag{5.11}$$

где P – матрица из элементов открытого текста;

C – матриц из элементов закрытого текста.

Теперь необходимо провести проверку обратимости матрицы P. В данном случае матрица P обратима (5.12).

$$|P| = \begin{vmatrix} 2 & 17 \\ 15 & 19 \end{vmatrix} = -217 \bmod 26 = 17$$
$$|P|^{-1} * |P| = 1 \bmod 26 \tag{5.12}$$
$$|P|^{-1} = 23$$

Теперь необходимо найти матрицу обратную P. Для ее нахождения необходимо воспользоваться формулой (5.13):

$$P^{-1} = \frac{1}{|P|} * P^{*T} \tag{5.13}$$

Число обратное определителю матрицы P уже было найдено в (5.12) поэтому необходимо найти транспонированную матрицу алгебраических дополнений. Для этого выполним (5.14):

$$P = \begin{pmatrix} 2 & 17 \\ 15 & 19 \end{pmatrix} \tag{5.14}$$
$$M_{11} = |19| = 19 \qquad M_{12} = |15| = 15$$
$$M_{21} = |17| = 17 \qquad M_{22} = |2| = 2$$
$$P^* = \begin{pmatrix} 19 & -15 \\ -17 & 2 \end{pmatrix}$$

$$P^{*T} = \begin{pmatrix} 19 & -17 \\ -15 & 2 \end{pmatrix} \bmod 26 = \begin{pmatrix} 19 & 9 \\ 11 & 2 \end{pmatrix} \quad (5.14)$$

Теперь необходимо найти матрицу обратную P по формуле (5.15):

$$P^{-1} = 23 * \begin{pmatrix} 19 & 9 \\ 11 & 2 \end{pmatrix} \bmod 26 = \begin{pmatrix} 21 & 25 \\ 19 & 20 \end{pmatrix} \quad (5.15)$$

После нахождения обратной матрицы необходимо применить формулу матрицы ключа (5.16):

$$\begin{gathered} L = P^{-1} * C \\ K = L^{T} \\ L = \begin{pmatrix} 21 & 25 \\ 19 & 20 \end{pmatrix} * \begin{pmatrix} 23 & 25 \\ 12 & 5 \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 1 & 3 \end{pmatrix} \\ K = \begin{pmatrix} 3 & 1 \\ 0 & 3 \end{pmatrix} \end{gathered} \quad (5.16)$$

Что и является первым ключом, использованным при шифровании. Теперь необходимо проделать аналогичные действия для нахождения второго ключа шифрования. При нахождении второго ключа были так же взяты вторые блоки из открытых и закрытых текстов (5.17):

$$\begin{matrix} o_1 = (5,9) & \qquad c_1 = (6,1) \\ o_2 = (4,7) & \qquad c_2 = (5,8) \end{matrix} \quad (5.17)$$

где o_i – i-ый блок открытого текста;

c_i – i-ый блок закрытого текста.

Теперь необходимо составить матрицы из перехваченных блоков (5.18):

$$P = \begin{pmatrix} 5 & 9 \\ 4 & 7 \end{pmatrix} \qquad C = \begin{pmatrix} 6 & 19 \\ 5 & 22 \end{pmatrix} \quad (5.18)$$

где P – матрица из элементов открытого текста;

C – матриц из элементов закрытого текста.

Теперь необходимо провести проверку обратимости матрицы P. В данном случае матрица P обратима (5.19).

$$
\begin{gathered}
|\mathrm{P}| = \begin{vmatrix} 5 & 9 \\ 4 & 7 \end{vmatrix} = -1 \bmod 26 = 25 \\
|\mathrm{P}|^{-1} \, * \, |\mathrm{P}| \; = \; 25 \bmod 26 \\
|\mathrm{P}|^{-1} \; = \; 25
\end{gathered} \tag{5.19}
$$

Теперь необходимо найти матрицу обратную P. Для ее нахождения необходимо воспользоваться формулой (5.20):

$$
\mathrm{P}^{-1} = \frac{1}{|\mathrm{P}|} * \mathrm{P}^{*\mathrm{T}} \tag{5.20}
$$

Число обратное определителю матрицы P уже было найдено в (5.19) поэтому необходимо найти транспонированную матрицу алгебраических дополнений. Для этого выполним (5.21):

$$
\begin{gathered}
\mathrm{P} = \begin{pmatrix} 5 & 9 \\ 4 & 7 \end{pmatrix} \\
\mathrm{M}_{11} = \; |7| = 7 \qquad\qquad \mathrm{M}_{12} = |4| = 4 \\
\mathrm{M}_{21} = |9| = 9 \qquad\qquad \mathrm{M}_{22} = |5| = 5 \\
\mathrm{P}^{*} = \begin{pmatrix} 7 & -4 \\ -9 & 5 \end{pmatrix} \\
\mathrm{P}^{*\mathrm{T}} = \begin{pmatrix} 7 & -9 \\ -4 & 5 \end{pmatrix} \bmod 26 \; = \begin{pmatrix} 7 & 17 \\ 22 & 5 \end{pmatrix}
\end{gathered} \tag{5.21}
$$

Теперь необходимо найти матрицу обратную P по формуле (5.22):

$$
\mathrm{P}^{-1} = 25 \; * \; \begin{pmatrix} 7 & 17 \\ 22 & 5 \end{pmatrix} \bmod 26 \; = \begin{pmatrix} 19 & 9 \\ 4 & 21 \end{pmatrix} \tag{5.22}
$$

После нахождения обратной матрицы необходимо применить формулу матрицы ключа (5.23):

$$
\begin{gathered}
\mathrm{L} = \mathrm{P}^{-1} * \mathrm{C} \\
\mathrm{K} = \mathrm{L}^{\mathrm{T}} \\
\mathrm{L} \; = \; \begin{pmatrix} 19 & 9 \\ 4 & 21 \end{pmatrix} * \begin{pmatrix} 6 & 19 \\ 5 & 22 \end{pmatrix} = \begin{pmatrix} 3 & 25 \\ 13 & 18 \end{pmatrix}
\end{gathered} \tag{5.23}
$$

$$K = \begin{pmatrix} 3 & 13 \\ 25 & 18 \end{pmatrix}$$

Что и является вторым ключом, использованным при шифровании.

6 Выводы о проделанной работе

В данной практической работе были рассмотрены два шифра: шифр Хилла и рекуррентный шифр Хилла. Данные шифры обладают следующими плюсами и минусами.

Шифр Хилла.

Плюсы:

1) Защищен от взлома частотным анализом;
2) Защищен от взлома подбором ключа.

Минусы:

1) Сложность генерации ключей, особенно больших размеров;
2) Уязвим к атаке по открытому тексту (оптимальный способ).

Рекуррентный шифр Хилла.

Плюсы:

3) Защищен от взлома частотным анализом;
4) Защищен от взлома подбором ключа;
5) По сравнению с простым шифром Хилла более защищен от атаки по открытому тексту.

Минусы:

3) Сложность генерации ключей, особенно больших размеров, которая возрастает по сравнению с обычным рекуррентным, так как используются два ключа;
4) Уязвим к атаке по открытому тексту (оптимальные способ).

7 Список использованных источников

1. A. V. N. Krishna, Dr. A. Vinaya Babu. A Modified Hill Cipher Algorithm for Encryption of Data In Data Transmission // Computer Science and Telecommunications: Georgian Electronic Scientific Journal. — 2007. — № 3(14). — С. 78—83.

2. Небольшой обзор на Шифр Хилла (Краткое пособие) – URL: https://habr.com/ru/post/595281/

3. Взломать шифр Хилла? Легко – URL: https://habr.com/ru/post/345876/