Правительство Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»
(НИУ ВШЭ)

Московский институт электроники и математики им. А.Н. Тихонова

ОТЧЕТ
О ПРАКТИЧЕСКОЙ РАБОТЕ № 2
по дисциплине «Математические основы защиты информации»

МАТРИЧНЫЙ ШИФР ХИЛЛА

Студент гр. БИБ 201
К.Ш.Ёркулов
«_» ____ 2022 г.

Руководитель
Заведующий кафедрой информационной безопасности кибер физических систем
канд. техн. наук, доцент
_____ О.О. Евсютин
«___» _____ 2022 г.

Москва 2022

СОДЕРЖАНИЕ

1 Задание на практическую работу

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

В рамках практической работы необходимо выполнить следующее:

– написать программную реализацию следующих шифров:

а) шифр Хилла:

б) рекуррентный шифр Хилла;

–изучить методы криптоанализа матричных шифров с использованием дополнительных источников;

– провести криптоанализ данных шифров.

2 Краткая теоретическая часть

2.1 Описание шифров

Шифр Хилла — полиграммный шифр подстановки, основанный на линейной алгебре и модульной арифметике. Полиграммный подстановочный шифр - это шифр, который блоки символов шифрует по группам.

Каждой букве алфавита сопоставляется число. Для русского алфавита можно использовать простейшую схему: А = 0, Б = 1, ..., Я = 32. Для зашифрования блок исходного сообщения из **n** букв рассматривается как n-мерный вектор чисел и умножается на матрицу размером **n** x **n** по модулю 33. Данная матрица, совместно с кодовой таблицей сопоставления букв алфавита с числами, является ключом зашифрования. Для расшифрования применяется обратная матрица ^{2} по модулю. Далее подробно описано как устроен данный шифр

Открытый текст разбивается на блоки длиной n, и каждый блок представляется в виде n-мерного вектора.

Ключом является квадратная матрица размера n × n.

$$K = GL_n(\mathbb{Z}_m) .$$

$$K = (k_{i,j}),\ i,j = \overline{1,n}\ k_{i,j} \in \mathbb{Z}_m.$$

Эта матрица должна быть обратима в Z" , чтобы была возможна операция расшифрования. Матрица будет являться обратимой только в том случае, если ее детерминант входит в группу обратимых элементов кольца .

$$|K| = \mathbb{Z}_m^*$$

Операция зашифрования заключается в том, что вектор, соответствующий блоку открытого текста, умножается на ключевую матрицу.

$$X = (x_1, \dots, x_n)^T.$$

$$Y = (y_1, \dots, y_n)^T = E_K(X) = K$$

Для того, чтобы расшифровать шифртекст, необходимо, разбив его на блоки, представить каждый блок в виде вектора и умножить на обратную матрицу ключа.

В случае **рекуррентного шифра Хилла** для каждого блока открытого текста вычисляется новое ключевое значение на основе двух предыдущих.

$$K_{i+1} = K_i * K_{i-1}$$

$$K_{i+1}^{-1} = K_i^{-1} K_{i-1}^{-1}$$

3 Пример шифрования

3.1 Шифр Хилла

Далее рассмотрим пример “ручного” шифрования шифра Хилла.

В данном случае будем использовать матрицу 2 x 2, так как она удобна для ручного вычисления.

В качестве ключа возьмем матрицу K = (1 2; 2 3)

Открытый текст x = crypto (c, r, y, p, t, o) разбиваем на блоки длинной два (ранг матрицы) символа:

$$x_1 = (c, r)^T$$

$x_2 = (y, p)^T$

$x_3 = (t, o)^T$

Перемножаем каждый блок (числовые значения букв) на ключ-матрицу, получаем:

$y_1 = (1\,2;\ 2\,3) * (2; 17) = (36;\ 55)\ mod\ 26 = (10;\ 3)$

$y_2 = (1\,2;\ 2\,3) * (24; 15) = (54;\ 93)\ mod\ 26 = (2;\ 15)$

$y_3 = (1\,2;\ 2\,3) * (19;\ 14) = (47;\ 80)\ mod\ 26 = (21;\ 2)$

$y = (10\ 3\ 2\ 15\ 21\ 2) = (k\ d\ c\ p\ v\ c)$

Для расшифрования умножаем блоки шифртекста на обратную матрицу:

$K^{-1} = (-\ 3\,2;\ 2\ -\ 1)$

$x_1 = (-\ 3\,2;\ 2\ -\ 1) * (10;\ 3) = (-\ 24;\ 17)\ mod\ 26 = (2;\ 17)$

$x_2 = (-\ 3\,2;\ 2\ -\ 1) * (2;\ 15) = (24;\ -\ 11)\ mod\ 26 = (24;\ 15)$

$x_3 = (-\ 3\,2;\ 2\ -\ 1) * (21;\ 2) = (-\ 59;\ 40)\ mod\ 26 = (19;\ 14)$

$x = (2\ 17\ 24\ 15\ 19\ 14) = (c\ r\ y\ p\ t\ o)$ – полученный открытый текст.

3.2 Рекуррентный шифр Хилла

Приведем пример “ручного” шифрования рекуррентным шифром Хилла.

В качестве матрицы ключей взяты: $K_1 = (1\,2;\ 2\,3)$, $K_2 = (2\,3;\ 3\,4)$

Открытый текст x = crypto (c, r, y, p, t, o) разбиваем на блоки длинной два (ранг матрицы) символа:

$x_1 = (c, r)^T$

$x_2 = (y, p)^T$

$x_3 = (t, o)^T$

Перемножаем каждый блок (числовые значения букв) на соответствующую ключ матрицу, получаем:

$y_1 = (1\,2;\ 2\,3) * (2; 17) = (36;\ 55)\ mod\ 26 = (10;\ 3)$

$y_2 = (2\,3;\ 3\,4) * (24; 15) = (93;\ 132)\ mod\ 26 = (15;\ 2)$

$y_3 = (8\,11; 13\,18) * (19;\ 14) = (306; 499)\ mod\ 26 = (20;\ 5)$

$K_3 = K_2 * K_1 \Rightarrow K_3 = (1\,2;\ 2\,3) * (2\,3;\ 3\,4) = (8\,11;\ 13\,18)$

$y = (10\ 3\ 2\ 2\ 20\ 5) = (k\ d\ c\ c\ u\ f)$

Для расшифрования умножаем блоки шифртекста на обратную матрицу:

$K_1^{-1} = (-\ 3\,2;\ 2\ -\ 1)$

$K_2^{-1} = (-\ 4\,3;\ 3\ -\ 2)$

$K_3^{-1} = K_2^{-1}K_1^{-1} = (-\ 3\,2;\ 2\ -\ 1) * (-\ 4\,3;\ 3\ -\ 2) = (18\ -\ 13;\ -\ 11\,8)$

$x_1 = (-\ 3\,2;\ 2\ -\ 1) * (10;\ 3) = (-\ 24;\ 17)\ mod\ 26 = (2;\ 17)$

$x_2 = (-\ 4\,3;\ 3\ -\ 2) * (15;\ 2) = (-\ 54;\ 41)\ mod\ 26 = (24;\ 15)$

$x_3 = (18\ -\ 11;\ -\ 13\,8) * (20;\ 5) = (305; -\ 220)\ mod\ 26 = (19;\ 14)$

$x = (2\ 17\ 24\ 15\ 19\ 14) = (c\ r\ y\ p\ t\ o)$ – полученный открытый текст.

4 Программная реализация

```
PS D:\Programs\VScode\MOZI\Practice_2> python .\hill.py -i attackatdawn -k must
Encrypted Text: iulbhjiufx.x
Decrypted Text: attackatdawn
PS D:\Programs\VScode\MOZI\Practice_2>
```

Рисунок 1. Пример программной реализации шифра Хилла.

```
PS D:\Programs\VScode\MOZI\Practice_2> python .\hill_recurrent.py -i attackatdawn -k1 must -k2 math
Encrypted Text: dnznujuviema
Decrypted Text: attackatdawn
PS D:\Programs\VScode\MOZI\Practice_2>
```

Рисунок 1. Пример программной реализации рекуррентного шифра Хилла.

5 Примеры криптоанализа

Шифр Хилла будет сложно атаковать методом грубой силы, так как стандартный шифр Хилла имеет пространство ключей n^{m^2}, где n-мощность алфавита, m-мощность ключа или сколько существует матриц m x m. А для рекуррентного шифра Хилла это будет возводиться в квадрат поэтому полный перебор не будет эффективен. Так же шифр Хилла устойчив к частотному анализу, так как не будет соответствия между одинаковыми символами даже для стандартной вариации. И поэтому будем использовать атаку по открытому тексту, потому что в нем используются линейные операции.

```
PS D:\Programs\VScode\MOZI\Practice_2> python .\hill.py -i 'test text' -k arch
Encrypted Text: genon;toah
Decrypted Text: test texta
PS D:\Programs\VScode\MOZI\Practice_2> python .\hill_open_text_analysis.py -p 'test texta' -c 'genon;toah'
Probable keys: ['p', 'arch']
The best key found is "arch", which scored 0.5 on dictionary check.
PS D:\Programs\VScode\MOZI\Practice_2>
```

Рисунок 4. Вывод криптоанализа рекуррентного шифра Хилла.

6 Выводы о проделанной работе

В данной практической работе мы усвоили новые навыки по шифру Хилла и рекуррентному шифру Хилла. научились шифровать и расшифровывать с помощью данных шифров. Посмотрели как устроены данные шифры. Хотелось бы отметить достоинства и недостатки данного шифра:

Достоинства шифра Хилла:

1) Устойчивость к частотному анализу

2)Устойчивость к полному перебору, даже при относительно небольших размерах ключа

3)Простота и скорость применения

Недостатки:

1)Уязвимость к атаке по открытому тексту

2)Высокая сложность генерации ключ – матриц, особенно больших размерностей

7 Список использованных источников

- Шифр Хилла — Википедия (wikipedia.org)

- Шифр Хила. Подробный разбор / Хабр (habr.com)

- *William Stallings.* Cryptography and Network Security: Principles and Practice.