**СОДЕРЖАНИЕ**

[1 Задание на практическую работу 3](#_Toc119240564)

[2 Краткая теоретическая часть 4](#_Toc119240565)

[2.1 Описание шифров 4](#_Toc119240566)

[2.2 Методы криптоанализа шифров 5](#_Toc119240567)

[3 Примеры шифрования 6](#_Toc119240568)

[4 Программная реализация шифров 11](#_Toc119240569)

[5 Примеры криптоанализа 14](#_Toc119240570)

[6 Выводы о проделанной работе 18](#_Toc119240571)

[7 Список использованных источников 19](#_Toc119240571)

# 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;

1. изучить методы криптоанализа блочных шифров с использованием дополнительных источников;
2. провести криптоанализ данных шифров.

Программа должна обладать следующей функциональностью для каждого из реализованных в ней шифров:

1. принимать на вход произвольную последовательность символов, вводимую пользователем в качестве открытого текста или шифртекста;
2. принимать на вход секретный ключ вида, соответствующего конкретному шифру;
3. осуществлять зашифрование или расшифрование введенного текста по выбору пользователя.

# 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 мощностью , которые представляются элементами множества . Перед зашифрованием открытый текст разбивается на блоки длиной , и каждый блок представляется в виде -мерного вектора.

Ключом шифра является квадратная матрица размера , составленная из элементов множества : , . Эта матрица должна быть обратима в , чтобы была возможна операция расшифрования. Матрица будет являться обратимой только в том случае, если ее детерминант удовлетворяет следующим двум условиям: и .

Операция зашифрования заключается в том, что ключевая матрица умножается на вектор–столбец , соответствующий блоку открытого текста:

.

Для того, чтобы расшифровать шифртекст, необходимо разбить его на блоки длиной , представить каждый блок в виде вектора и выполнить обратное умножение:

.

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

.

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

.

## 2.2 Методы криптоанализа шифров.

1) Метод перебора. Атаковать “грубой силой” шифр Хилла сложно. Если размерность матрицы – ключа n x n, то всего существует 26n^2 таких матриц [1].

2) Частотный криптоанализ. Многие блочные шифры в том числе, и шифр Хилла, и рекуррентный шифр Хилла устойчивы к простому частотному криптоанализу на основе подсчета частоты встречаемости отдельных символов.

3) Шифр Хилла уязвим перед 𝑛-граммным (поблочным) частотным криптоанализом. Рекуррентный шифр Хилла – это усиление шифра Хилла, который не обладает уязвимостью поблочного криптоанализа. Например, на рисунке 1 представлена частота встречаемости биграмм в английском языке

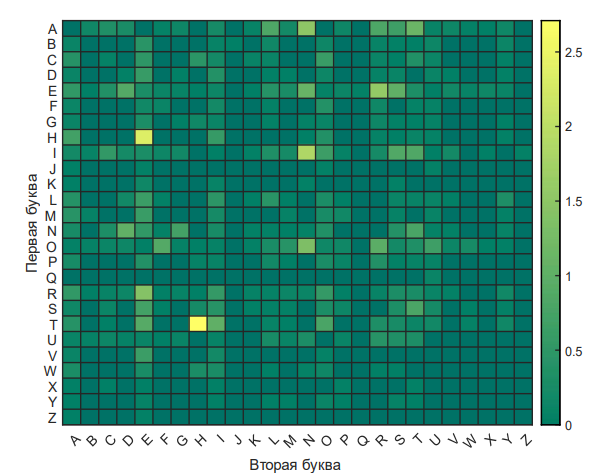


Рисунок 1 – Частота встречаемости биграмм в английском языке

4) Шифр Хилла также уязвим для атаки по открытому тексту, так как в нем используются линейные операции [1].

# 3 Примеры шифрования.

3.1 «Ручное» шифрование и расшифрование шифра Хилла:

Для того, чтобы разобрать шифрование шифра Хила, возьмём слово “GEORGYSAZ” за открытый текст. Мощность алфавита будет равна 26. Ключ возьмём равный (1):

, (1)

Убеждаемся, что матрица обратима в . Определитель матрицы равен (2):

(2)

Находим порядковые номера всех символов из алфавита в открытом тексте: “6, 4, 14, 17, 6, 24, 18, 0, 25”. Затем разобьём на 3 блока порядковые номера открытого текста и получим (3):

, , , (3)

Теперь находим блоки шифртекста (4), (5), (6):

, (4)

, (5)

, (6)

Получаем порядковые номера символов шифртекста – “24, 12, 2, 21, 24, 13, 17, 9, 9”. Это соответствует сообщению “YMCVYNRJJ”

Для того, чтобы разобрать расшифрование шифра Хилла, возьмём слово “YMCVYNRJJ” и ключ k, который использовался раннее в процессе шифрования (1). Также необходимо найти обратную матрицу ключу k. Для этого сначала находим алгебраические дополнения для каждого элемента:

Далее записываем алг. дополнения в матрицу и затем транспонируем её и делим на определитель -5 (7):

, (7)

Далее находим обратную матрицу по модулю 26. Для этого находим для каждого элемента матрицы элемент по модулю 26. Если встречается дробное число тогда новый элемент рассчитывается по следующим формулам (8), (9):

Для отрицательной дроби (8)

Для положительной дроби (9)

Пользуясь формулами (8), (9) получаем (10):

, (10)

Находим порядковые номера шифртекста и делим их на три блока (11):

, , , (11)

Теперь находим блоки исходного сообщения (12), (13), (14):

, (12)

, (13)

,(14)

Получаем порядковые номера символов исходного сообщения – “6, 4, 14, 17, 6, 24, 18, 0, 25”. Значит открытый текст = “GEORGYSAZ”.

3.2 «Ручное» шифрование и расшифрование рекуррентного шифра Хила:

Для того, чтобы разобрать шифрование шифра Хилла, снова возьмём слово “GEORGYSAZ” за открытый текст. Мощность алфавита будет равна 26. Разбиваем порядковые номера символов открытого текста на 3 блока (17):

, , , (15)

В данном случае также потребуется 3 ключа k. Первые два необходимо задать (16), (17), а третий можно найти по формуле (18):

, (16)

, (17)

, (18)

Заметим, что матрицы k1, k2 обратимы в , так как | k1 | = 21, | k2 | = 21. Теперь находим блоки шифртекста (19), (20), (21):

, (19)

, (20)

,(21)

Получаем “24, 12, 2, 21, 25, 16, 8, 25, 6”, шифртекст – “YMCVZQIZG”.

Для того, чтобы разобрать расшифрование рекуррентного шифра Хилла, возьмём слово “ YMCVZQIZG” и те же самые ключи k, которые использовались раннее в процессе шифрования (16), (17), (18). Для начала необходимо найти обратные матрицы для всех ключей. Для этого находим обратную матрицу по модулю 26, процесс нахождения которых был описан раннее в пункте 3.1. Получаем (22, 23, 24):

Для , (22)

Для , (23)

Для , (24)

Находим порядковые номера шифртекста и делим их на три блока (25):

, , , (25)

Теперь находим блоки исходного сообщения (26), (27), (28):

, (26)

,(27)

, (28)

Получаем порядковые номера символов исходного сообщения – “6, 4, 14, 17, 6, 24, 18, 0, 25”. Значит открытый текст = “GEORGYSAZ”.

# 4 Программная реализация шифров.

Программная реализация шифра Хилла показана на рисунке 2, на рисунке 3 и на рисунке 4:

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 2 – Программная реализация шифрования шифра Хилла. Часть 1

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 3 – Программная реализация шифрования шифра Хилла. Часть 2

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 4 – Программная реализация шифрования шифра Хилла. Часть 3

Функция “encryption” принимает на вход 2 значения – текст и ключ.

На 14 строке исходный текст записывается в виде списка порядковых номеров элементов.

На 21 строке происходит транспонирование получившийся матрицы.

На 25 строке высчитывается значение перемножения ключа и блоков текста.

На 35 строке происходит транспонирование получившийся матрицы.

На 39 строке происходит итоговое преобразование в шифртекст.

На 42 строке оператор “return” возвращает результат шифрования.

Функция “decryption” принимает на вход 2 значения – шифртекст и ключ.

На 50 строке шифртекст записывается в виде списка порядковых номеров элементов.

На 57 строке высчитывается обратная матрица для ключа k.

На 67 строке происходит транспонирование матрицы порядковых номеров элементов шифртекста.

На 71 строке высчитывается значение перемножения ключа и блоков шифртекста.

На 81 строке происходит транспонирование получившийся матрицы.

На 85 строке происходит итоговое преобразование шифртекста в исходный текст.

На 88 строке оператор “return” возвращает результат расшифрования.

Функция “print” на 91 строке выводит результат шифрования для функции “encryption” с заданными значениями.

Функция “print” на 92 строке выводит результат расшифрования для функции “decryption” с заданными значениями.

Заметим, что результат работы программы совпал с “ручным” шифрованием, выполненным раннее в пункте 3.1.

**5 Примеры криптоанализа.**

Рассмотрим один из способов криптоанализа - атаку по открытому тексту. Шифр Хилла и рекуррентный шифр Хилла уязвимы к данному способу, так как в них используются линейные операции.

5.1 Криптоанализ шифра Хилла [2].

Пусть злоумышленнику известен следующий шифртекст:

“P JKRHZTT.BEQWSGWXDVIFEAHAIXFTA,LGZQM,XAPDBUWKFRJVYKYGWRXIZUEUBFFUQDGWRRCHSO SX,BFFKHYUXGBG,NDV. CBFFSO V RJPCWBKX,XUSNJSSMAEAE XGVAHAIXFYTV.KYX.NE.PVMPPOJRCGCARQAIVEJXAPONJSCLXAP YCZJCN. S,NAXF,AS,G FRTFONSSRHXLTCALJJGFLJDATJ,”

И пусть также известно, что часть исходного сообщения “MOSCOW ZO” соответствует шифртексту “ P JKRHZT”.

Для того, чтобы узнать ключ представим исходный текст и шифртекст в виде матриц порядковых чисел символов (29), (30):

, (29)

, (30)

Чтобы узнать ключ, нужно воспользоваться формулой (31):

(31)

Получаем (32):

, (32)

Транспонируем получившуюся матрицу и получаем ключ k, с помощью которого можно расшифровать всё сообщение (33):

, (33)

Чтобы получить открытый текст, воспользуемся раннее написанной программой (пункт 4). Для этого воспользуемся функцией print(decryption("ШИФРТЕКСТ", [[1, 1, 1], [2, 3, 1], [5, 2, 3]]) и получим результат следующий результат, представленный на рисунке 5.

Изображение выглядит как текст, внутренний, экран, снимок экрана

Автоматически созданное описание

Рисунок 5 – Результат расшифровки

В итоге злоумышленник узнал весь открытый текст: “MOSCOW ZOO IS SITUATED IN THE CENTRE OF THE CITY. WHEN YOU GET THERE, YOU ARE IN THE ANIMAL WORLD. THERE ARE TWO LARGE TERRITORIES IN THE ZOO WITH A HIGH BRIDGE BETWEEN THEM. IN THE ZOO PONDS YOU CAN SEE BEAUTIFUL WATER BIRDS.ZZ”

5.2 Криптоанализ рекуррентного шифра Хилла.

Пусть злоумышленнику известен следующий шифртекст:

“BFFFAHVALBWSM.XEBYRBZFXX,KHGTCFIWXNC,JDKOCIZEJIC,TIOCXWYCAY UWORYXGRRMMBDZJWUGEGNFLSQCJQDFNUVGRLP.OXIVLFTDNFPPYZH,PDOAEELSBUZPNNFKXYQFWUAHJNOBSPIBPIIQXLJCW UK CES VRHB IFUSRTFLKJMCNP.W BZPKMVZHWULWBQVBWM ZPNGDECONVC,EAMXT,URTGKLQFLUEDPNLBEQSUEEVPLCC”

И пусть также известно, что часть исходного сообщения “THE RULES OF FOOTB” соответствует шифртексту “ BFFFAHVALBWSM.XEBY”. Чтобы узнать ключи потребуется представить в виде матриц порядковых значений символов шифртекста и исходного сообщения (34) и (35):

при k1, (34)

, при k2, (35)

Значит ключи k1, k2 равны (36), (37):

, (36)

, (37)

Теперь чтобы получить открытый текст, воспользуемся раннее написанной программой (пункт 4). Для этого воспользуемся функцией print(decryption("ШИФРТЕКСТ", [[1, 1, 1], [2, 3, 1], [5, 2, 3]], [[1, 1, 1], [3, 5, 2], [4, 1, 3]])) и получим результат следующий результат, представленный на рисунке 6.

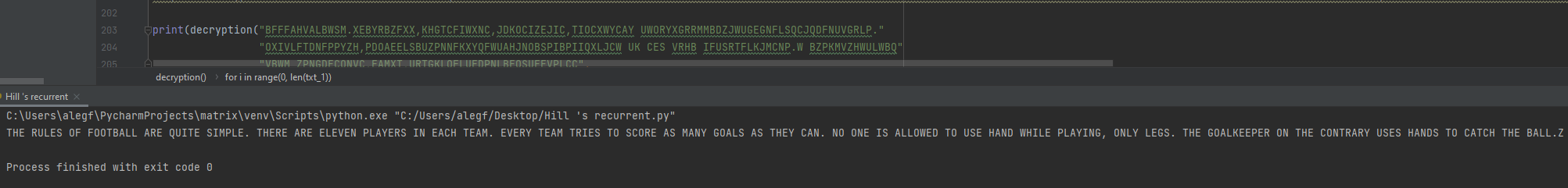


Рисунок 6 – Результат расшифровки

В итоге злоумышленник узнал полностью исходное сообщение: “THE RULES OF FOOTBALL ARE QUITE SIMPLE. THERE ARE ELEVEN PLAYERS IN EACH TEAM. EVERY TEAM TRIES TO SCORE AS MANY GOALS AS THEY CAN. NO ONE IS ALLOWED TO USE HAND WHILE PLAYING, ONLY LEGS. THE GOALKEEPER ON THE CONTRARY USES HANDS TO CATCH THE BALL.Z”

**6 Выводы о проделанной работе.**

В процессе выполнения практической работы были рассмотрены блочные перестановочные шифры такие как шифр Хилла и рекуррентный шифр Хилла, а также их криптоанализ. Также был получен навык программной реализации этих шифров.

Одним из преимуществ шифра Хилла и рекуррентного шифра Хилла является устойчивость к простому частотному криптоанализу на основе подсчета частоты встречаемости отдельных символов. Однако, шифр Хилла уязвим перед поблочным частотным криптоанализом, а рекуррентный шифр Хилла не обладает этой уязвимостью.

# Список использованных источников.

1. Обзор шифра Хилла. – URL: https://habr.com/ru/post/710890/ (дата обращения 26.02.23)
2. Традиционные шифры с симметричным ключом. – URL: https://intuit.ru/studies/courses/552/408/lecture/9355?page=5 (дата обращения 25.03.23)