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

Московский институт электроники и математики им. Тихонова Департамент электронной инженерии

ОТЧЕТ
О ПРАКТИЧЕСКОЙ РАБОТЕ № 2
по дисциплине «Математические основы защиты информации»
ТЕМА РАБОТЫ
Матричный шифр Хилла

Выполнил:
Студент группы БИБ202
Кудайбергенов Амиржан
25.04.2022г.
Руководитель
Заведующий кафедрой информационной безопасности киберфизических систем
канд. техн. наук, доцент
_____О.О. Евсютин
«___»_____ 2022 г.

Москва 2022

Содержание

1 Цель работы

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

2 Краткая теоретическая часть

2.1 Описание шифров

Шифр Хилла
Данный шифр построен на основе матричных преобразований.
Множество невырожденных квадратных матриц над кольцом классов вычетов по модулю n образует группу.
Открытый текст разбивается на блоки длиной n, и каждый блок представляется в виде n-мерного вектора.

$$X = Y = (Z_m)^n.$$

Ключом является квадратная матрица размера n×n.

$$K = GL_n(Z_n).$$

$$k = (k_{i,j}), i, j = \overline{1, n}, k_{i,j} \in Z_m.$$

Эта матрица должна быть обратима в Z_m, чтобы была возможна операция расшифрования. Матрица будет являться обратимой только в том случае, если ее детерминант не равен нулю и не имеет общих делителей с основанием модуля.

$$|k| \in Z_m^*.$$

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

$$x = (x_1, ..., x_n)^T.$$

$$y = (y_1, ..., y_n)^T = E_k(X) = k \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

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.

$$k_{i+1} = k_i k_{i-1}.$$

$$k_{i+1}^{-1} = k_{i-1}^{-1} k_i^{-1}.$$

2.2 Методы криптоанализа шифров

3 Примеры шифрования

3.1 Шифр Хилла

1. В следующем примере будем использовать латинские буквы от A до Z, соответствующие им численные значения приведены в таблице. Целесообразно добавить к алфавиту еще 3 символа чтобы длина алфавита была простым числом. Потому что для расшифровки необходимо, чтобы детерминант ключа и длина алфавита были взаимно простыми.

2. Теперь берем текст, который хотим зашифровать и кодируем его с помощью нашего алфавита. Возьмем для примера слово “KERNEL” его код: 10 4 17 13 4 11.

3. Теперь выбираем ключевое слово. Например: OPENSTACK. Получаем:

$$K = \begin{pmatrix} 14 & 15 & 4 \\ 13 & 18 & 19 \\ 0 & 2 & 10 \end{pmatrix}, P_1 = \begin{pmatrix} 10 \\ 4 \\ 17 \end{pmatrix}, P_2 = \begin{pmatrix} 13 \\ 4 \\ 11 \end{pmatrix}$$

Данная матрица обратима, так как её детерминант не равен нулю и не имеет общих делителей с основанием модуля.

$$C_1 = K * P_1 (mod 29) = \begin{pmatrix} 14 & 15 & 4 \\ 13 & 18 & 19 \\ 0 & 2 & 10 \end{pmatrix} \begin{pmatrix} 10 \\ 4 \\ 17 \end{pmatrix} (mod 29) = \begin{pmatrix} 7 \\ 3 \\ 4 \end{pmatrix},$$

$$C_2 = K * P_2 (mod 29) = \begin{pmatrix} 14 & 15 & 4 \\ 13 & 18 & 19 \\ 0 & 2 & 10 \end{pmatrix} \begin{pmatrix} 13 \\ 4 \\ 11 \end{pmatrix} (mod 29) = \begin{pmatrix} 25 \\ 15 \\ 2 \end{pmatrix}.$$

Получаем шифртекст HDEZPC

4. Расшифрование

Обратная матрица ключа:

$$K^{-1} (mod 26) = \begin{pmatrix} 1 & 28 & 16 \\ 24 & 21 & 23 \\ 1 & 19 & 10 \end{pmatrix}$$

Возьмём ранее выведенный шифртекст

$$P_1 = K^{-1} * C_1 (mod 29) = \begin{pmatrix} 1 & 28 & 16 \\ 24 & 21 & 23 \\ 1 & 19 & 10 \end{pmatrix} \begin{pmatrix} 7 \\ 3 \\ 4 \end{pmatrix} (mod 29) = \begin{pmatrix} 10 \\ 4 \\ 17 \end{pmatrix},$$

$$P_2 = K^{-1} * C_2 (mod 29) = \begin{pmatrix} 1 & 28 & 16 \\ 24 & 21 & 23 \\ 1 & 19 & 10 \end{pmatrix} \begin{pmatrix} 25 \\ 15 \\ 2 \end{pmatrix} (mod 29) = \begin{pmatrix} 13 \\ 4 \\ 11 \end{pmatrix}.$$

3.2 Рекуррентный шифр Хилла

Главное отличие рекуррентного шифра от простого состоит в том что для каждого блока открытого текста вычисляется новое ключевое значение на основе двух предыдущих. Для примера возьмем слово “TABLES” а первый два ключа: “ARCH”; “LINK”, алфавит также 29 символа.

$$k_1 = \begin{pmatrix} 0 & 17 \\ 2 & 7 \end{pmatrix}, k_2 = \begin{pmatrix} 11 & 8 \\ 13 & 10 \end{pmatrix}, P_1 = \begin{pmatrix} 19 \\ 0 \end{pmatrix}, P_2 = \begin{pmatrix} 1 \\ 11 \end{pmatrix}, P_3 = \begin{pmatrix} 4 \\ 18 \end{pmatrix}$$

Зашифруем:

$$C_1 = \begin{pmatrix} 0 & 17 \\ 2 & 7 \end{pmatrix} \begin{pmatrix} 19 \\ 0 \end{pmatrix} (mod 29) = \begin{pmatrix} 0 \\ 9 \end{pmatrix}$$

$$C_2 = \begin{pmatrix} 11 & 8 \\ 13 & 10 \end{pmatrix} \begin{pmatrix} 1 \\ 11 \end{pmatrix} (mod 29) = \begin{pmatrix} 12 \\ 7 \end{pmatrix}$$

$$C_3 = \begin{pmatrix} 11 & 8 \\ 13 & 10 \end{pmatrix} \begin{pmatrix} 0 & 17 \\ 2 & 7 \end{pmatrix} \begin{pmatrix} 4 \\ 18 \end{pmatrix} (mod 29) = \begin{pmatrix} 16 & 243 \\ 20 & 291 \end{pmatrix} \begin{pmatrix} 4 \\ 18 \end{pmatrix} (mod 29) = \begin{pmatrix} 1 \\ 11 \end{pmatrix}$$

Обратные матрицы ключей:

$$k_1^{-1} = \begin{pmatrix} 16 & 15 \\ 12 & 0 \end{pmatrix}, k_2^{-1} = \begin{pmatrix} 21 & 18 \\ 22 & 26 \end{pmatrix}, k_3^{-1} = \begin{pmatrix} 666 & 678 \\ 252 & 216 \end{pmatrix}$$

Дешифруем:

$$P_1 = \begin{pmatrix} 16 & 15 \\ 12 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 9 \end{pmatrix} (mod 29) = \begin{pmatrix} 19 \\ 0 \end{pmatrix},$$

$$P_2 = \begin{pmatrix} 21 & 18 \\ 22 & 26 \end{pmatrix}, \begin{pmatrix} 12 \\ 7 \end{pmatrix} (mod 29) = \begin{pmatrix} 1 \\ 11 \end{pmatrix}$$

$$P_3 = \begin{pmatrix} 666 & 678 \\ 252 & 216 \end{pmatrix} \begin{pmatrix} 1 \\ 11 \end{pmatrix} (mod 29) = \begin{pmatrix} 4 \\ 18 \end{pmatrix}$$

4 Программная реализация шифров

Реализация представляет собой 2 отдельных файла. У каждого шифра есть два режима работы: либо используется ввод строки с дальнейшим выводом в терминал, либо режим работы с файлом где вывод сохраняется в двух отдельных файлах. В реализации представлены вывод шифртекста и расшифрованный текст по шифртексту. Исходный код можно посмотреть в репозитории `https://github.com/kud-aa/mozi_practics`

```
[I] legion@legion ~/P/mozi_practics (hill)> python hill.py -i test.txt -k arch
Encrypted text in output/hill_enc_out.txt file
Decrypted ciphertext in output/hill_dec_out.txt file
[I] legion@legion ~/P/mozi_practics (hill)> cat output/hill_enc_out.txt
;dnonom.jg
[I] legion@legion ~/P/mozi_practics (hill)> cat output/hill_dec_out.txt
juststring
[I] legion@legion ~/P/mozi_practics (hill)> python hill.py -i 'Juststring' -k arch
Encrypted Text: ;dnonom.jg
Decrypted Text: juststring
```

Рис. 1: вывод шифра Хилла

```
[I] legion@legion ~/P/mozi_practics (hill)> python hill_recursive.py -i test.txt -k1 arch -k2 disk
Encrypted text in output/rec_hill_enc_out.txt file
Decrypted ciphertext in output/rec_hill_dec_out.txt file
[I] legion@legion ~/P/mozi_practics (hill)> cat output/rec_hill_enc_out.txt
;dus?cvabt
[I] legion@legion ~/P/mozi_practics (hill)> cat output/rec_hill_dec_out.txt
juststring
[N] legion@legion ~/P/mozi_practics (hill)> python hill_recursive.py -i 'notrecursivestring' -k1 arch -k2 disk
Encrypted Text: vahq; q ?ia;y;.yfl
Decrypted Text: notrecursivestring
```

Рис. 2: вывод рекуррентного шифра Хилла

5 Примеры криптоанализа

6 Выводы о проделанной работе

В процессе изучения программной реализации и криптоанализа шифра Хилла и его рекуррентной версии. Сделан вывод о их нестойкости (за исключением последнего при условии достаточно большого алфавита) к методам современной криптографии.