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 № 1
по дисциплине «Математические основы защиты информации»
Подстановочные шифры

Студент гр. БИБ201
Д.А. Морин
«9» 04.2022 г.

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

Москва 2022

Содержание

1. Краткие теоретические сведения

Шифр - система обратимых преобразований, зависящая от некоторого секретного параметра (ключа) и предназначенная для обеспечения секретности передаваемой информации.

Ключ - это часть информации, обычно представляющая собой строку цифр или букв, хранящуюся в файле, которая при обработке с помощью криптографического алгоритма может кодировать или декодировать криптографические данные.

Шифрование (зашифрование) - обратимое преобразование информации в целях сокрытия от неавторизованных лиц с предоставлением в это же время авторизованным пользователям доступа к ней.

Расшифрование - процесс преобразования зашифрованных данных в открытые данные при помощи шифра.

Дешифрование (дешифровка) - процесс извлечения открытого текста без знания криптографического ключа на основе известного шифрованного.

Открытый текст - в криптографии исходный текст, подлежащий шифрованию, либо получившийся в результате расшифровки. Может быть прочитан без дополнительной обработки (без расшифровки).

Шифротекст, шифртекст, криптограмма - результат операции шифрования.

Шифр Хилла — полиграммный шифр подстановки, основанный на линейной алгебре и модульной арифметике. полиграммный подстановочный шифр - это шифр, который блоки символов шифрует по группам. Рекуррентный шифр Хилла - усиление шифра Хилла, когда для каждого блока открытого текста
вычисляется новое ключевое значение на основе двух предыдущих.

Частотный анализ, частотный криптоанализ - один из методов криптоанализа, основывающийся на предположении о существовании нетривиального статистического распределения отдельных символов и их последовательностей, как в открытом тексте, так и в шифротексте, которое, с точностью до замены символов, будет сохраняться в процессе шифрования и дешифрования. Частотный анализ предполагает, что частотность появления заданной буквы алфавита в достаточно длинных текстах одна и та же для разных текстов одного языка.

Метод «грубой силы», полный перебор предполагает перебор всех возможных вариантов ключа шифрования до нахождения искомого ключа.

2. “Ручное” шифрование и расшифрование

Для того, чтобы было легче искать порядок букв в английском алфавите, воспользуемся рисунком 1.

A	0	N	13
B	1	O	14
C	2	P	15
D	3	Q	16
E	4	R	17
F	5	S	18
G	6	T	19
H	7	U	20
I	8	V	21
J	9	W	22
K	10	X	23
L	11	Y	24
M	12	Z	25

Рисунок 1 - нумерация букв в английском алфавите

1) Шифр Хилла

Открытый текст X = hello

k = ключ = | -1 1 |
| 2 -3 |

Так как мы выбрали ключ = матрицу размером 2x2, то мы разобьем текст по 2 блокам: he | ll | o и добавим на конец любую буквы, чтобы получился полный последний блок.

X = he | ll | oa

x1 = | 7 | x2 = | 11 | x3 = | 14 |
| 4 | | 11 | | 0 |

Находим определитель матрицы-ключа:

det k = 3 - 2 = 1, этот элемент принадлежит Z*(26)

y1 = k*x1 = | 23 | y2 = k*x2 = | 0 | y3 = k*x3 = | 12 |
| 2 | | 15 | | 2 |

Y = xcapmc

Последнюю букву откидываем, потому что это лишь дополнительная буква a из открытого текста X. Тогда Y = xcapm

Чтобы расшифровать данный шифртекст, необходимо найти обратную матрицу k^(-1).

A11 = (-1)^2*(-3) / det k = -3

A12 = (-1)^3*(2) / det k = -2

A21 = (-1)^3*(1) / det k = -1

A22 = (-1)^4*(-1) / det k = -1

k^(-1) = | -3 -1 |
         | -2 -1 |

x1 = k^(-1) * y1 = | 7 | x1 = k^(-1) * y1 = | 11 | x1 = k^(-1) * y1 = | 14 |
                   | 4 | | 11 | | 0 |

X = helloa

Последнюю букву откидываем, потому что это лишь дополнительная буква.

X = hello

2) Рекуррентный шифр Хилла

Открытый текст X = house

Разобьем его на блоки по 2 символа: ho | us | ea (добавил букву a, чтобы был полный блок) :

x1 = | 7 | x2 = | 20 | x3 = | 4 |
     | 14 | | 18 | | 0 |

Возьмем 2 ключа k1 = | 1 2 | и k2 = | 1 2 |
                       | 3 7 | | -2 -3 |

Зашифруем открытый текст.

y1 = k1 * x1 = | 9 | y2 = k2 * x2 = | 4 | y3 = k3 * x3
               | 15 | | 10 |

k3 = k1 * k2 = | 23 22 |
               | 15 11 |

y3 = | 14 |
     | 8 |

Y = jpeko (последнюю букву i убрал, потому что она нужна только для шифрования).

Расшифруем текст.

Для этого найдем обратные матрицы для k1, k2, k3.

k1^(-1):

det k1 = 7 - 6 = 1

A11 = (-1)^2*(7) / det k1 = 7

A12 = (-1)^3*(3) / det k1 = -3

A21 = (-1)^3*(2) / det k1 = -2

A22 = (-1)^4*(1) / det k1 = 1

k1^(-1) = | 7 -2 |
| -3 1 |

k2^(-1):

det k2 = -3 + 4 = 1

A11 = (-1)^2*(-3) / det k2 = -3

A12 = (-1)^3*(-2) / det k2 = 2

A21 = (-1)^3*(2) / det k2 = -2

A22 = (-1)^4*(1) / det k2 = 1

k1^(-1) = | 7 -2 |
| -3 1 |

k3^(-1):

det k3 = 23*11 - 15*22 = -77 = 1

A11 = (-1)^2*(11) / det k3 = 11

A12 = (-1)^3*(15) / det k3 = -15

A21 = (-1)^3*(22) / det k3 = -22

A22 = (-1)^4*(23) / det k3 = 23

k1^(-1) = | 11 -22 |
| -15 23 |

x1 = k1^(-1) * y1 = | 7 | x2 = k2^(-1) * y2 = | 20 | x3 = k3^(-1) * y3 = | 4 |
| 14 | | 18 | | 0 |

X = house

3. Программная реализация зашифрования и расшифрования

Шифр Хилла.

Ответ программы шифр хилла.py (рисунок 2):

```
Введите текст:
hello
Введите ключ по строкам матрицы через пробел:
-1 1 2 -3
enc or dec:
enc
det k = 1, OK!
[7, 4, 11, 11, 14, 0]
[23, 2, 0, 15, 12, 2]
Шифртекст:
xcapm
```

Рисунок 2 - результат программы зашифрования и расшифрования текста

Рекуррентный шифр Хилла.

Ответ программы рекур шифр.py (рисунок 3):

```
Введите слово:
house
Введите ключ по строкам матрицы через пробел:
1 2 3 7
Введите ключ по строкам матрицы через пробел:
1 2 -2 -3
enc or dec:
enc
[7, 14, 20, 18, 4, 0]
[9, 15, 4, 10, 14, 8]
Результат:
jpeko
```

Рисунок 3 - результат программы зашифрования и расшифрования текста

4. Криптоанализ вышеупомянутых шифров

Сложно атаковать шифр Хилла методом грубой силы, ведь всего матриц существует 26^(n^2), где n - размер квадратичной матрицы. Хотя не каждая матрица обратима, все равно перебор кажется чересчур сложным подходом к поиску ключа.

Шифр Хилла не поддается частотному анализу,ведь каждый символ открытого текста принимает участие в шифровании. Как приводился пример со словом hello, буква l преобразовалась сначала в a, потом в p.

Зато шифр Хилла уязвим для атаки по открытому тексту, так как в нем используются линейные операции. Если известно m пар “открытое сообщение”/ “зашифрованное сообщение”, то можно вычислить ключ. Предположим, мы знаем, что ключ это матрица 2x2, а также “открытое сообщение”/ “зашифрованное сообщение” (данные взял с помощью примера, зашифрование которого изображено на рисунке 4) :

(7, 4) ⇔ (15, 8)

(11, 11) ⇔ (7, 25)

```
Введите текст:
hellodearfriend
Введите ключ по строкам матрицы через пробел:
1 2 2 5
enc or dec:
enc
det k = 1, OK!
[7, 4, 11, 11, 14, 3, 4, 0, 17, 5, 17, 8, 4, 13, 3, 0]
[15, 8, 7, 25, 20, 17, 4, 8, 1, 7, 7, 22, 4, 21, 3, 6]
Шифртекст:
pihzureibhhwevd
```

Рисунок 4 - зашифрование текста (шифром Хилла)

Тогда составляем матрицы :

P = | 7 4 | C = | 11 11 |
| 11 11 | | 7 25 |

P^(-1) = | 1/3 -4/33 |
|-1/3 7/33 |

(det P = 77 - 44 = 33)

Тогда k = P^(-1) * C = | 137/33 -12/33 | = | 1 2 |
| -116/33 87/33 | | 2 5 |

Как мы видим, при зашифровании текста (рисунок 1), мы использовали именно такой ключ, с помощью которого можно расшифровать остальную часть сообщения.

Насчет рекуррентного шифра Хилла можно попробовать перебором найти два “соседних” ключа, зная части открытого и зашифрованногор текст, что матрица размером 2x2 и имея уравнения :

K(n) * (n-ый блок открытого текста) = n-ый блок шифротекста

K(n+1) * ((n+1)-ый блок открытого текста) = (n+1)ый блок шифротекста

Таким образом, можно находить ключи, которые предшествовали до них и которые идут после: K(n+2) = K(n) * K(n+1)... и K(n+1) = K(n-1) * K(n) => K(n-1) = K(n+1) * K(n)^(-1). Если знать ещё и K(n+2), то можно сразу проверить правильность подобранных ключей K(n) и K(n+1) и таким образом найти изначальные ключи K1 и K2.

5. Выводы о проделанной работе

Проделав данную работу, я приобрел больше навыков в работе с шифром Хилла и рекуррентным шифром Хилла, узнал о том, что этот шифр уязвим для атак по открытому тексту и достаточно стойкий для взлома методом грубой силы и частотному анализу.

6. Список использованных источников

1. Обзор шифра Хилла. URL: https://habr.com/ru/sandbox/163045/