Отчёт по лабораторной работе №2

Шифры перестановки

Волкова Дарья Александровна НПМмд-02-21

Содержание

Цель работы

Изучение шифров перестановки, а также их прогрммная реализация.

Теоретические сведения

Перестановка представляет собой способ шифрования, при котором для получения шифрограммы символы исходного сообщения меняют местами. Типичным примером перестановки являются анаграммы, ставшие популярными в XVII в. Анаграмма - литературный приём, состоящий в перестановке букв или звуков определённого слова (или словосочетания), что в результате даёт другое слово или словосочетание. Например: апельсин - спаниель, полковник - клоповник, горилка - рогалик, лепесток - телескоп.

Маршрутное шифрование

Широкое распространение получили шифры перестановки, использующие некоторую геометрическую фигуру (плоскую или объемную). Преобразования состоят в том, что в фигуру исходный текст вписывается по ходу одного маршрута, а выписывается по другому.

Маршрутное шифрование изобрел выдающийся французский математик и криптограф Франсуа Виет (1540-1603).

Пусть m и n – некоторые натуральные (т.е. целые положительные) числа, каждое больше 1. Открытый текст последовательно разбивается на части (блоки) с длиной, равной произведению m*n (если в последнем блоке не хватает букв, можно дописать до нужной длины произвольный их набор). Блок вписывается построчно в таблицу размерности m×n (т.е. m строк и n столбцов). Криптограмма получается выписыванием букв из таблицы в соответствии с некоторым маршрутом. Этот маршрут вместе с числами m и n составляет ключ шифра.

Чаще всего буквы выписывают по столбцам, которые упорядочиваются в соответствии с паролем: под таблицей подписывается слово, состоящее из n неповторяющихся букв, и столбцы таблицы нумеруются по алфавитному порядку букв пароля. Например, для шифрования открытого текста, выражающего один из главных принципов криптологии: нельзя недооценивать противника, добавим к его 29 буквам еще одну, скажем а, возьмем m=5, n=6, впишем текст в таблицу 5×6 и выберем в качестве пароля слово п а р о л ь:

нельзя
недооц
ениват
ьпроти
вникаа
пароль

Выписывая теперь буквы по столбцам в соответствии с алфавитным порядком букв в пароле, получаем следующую криптограмму: ЕЕНПНЗОАТАЬОВОКННЕЬВЛДИРИЯЦТИА (истинные пробелы в криптографии не выставляются).

Рассмотренный способ шифрования (столбцовая перестановка) в годы первой мировой войны использовала легендарная немецкая шпионка Мата Хари.

Шифрование с помощью решеток

Этот способ шифрования предложил в 1881 году австрийский криптограф Эдуард Флейснер. Выбирается натуральное число k > 1, и квадрат размерности k×k построчно заполняется числами 1, 2, …, k. Для примера возьмем k = 2.

Квадрат поворачивается по часовой стрелке на 90° и размещается вплотную к предыдущему квадрату. Аналогичные действия совершаются еще два раза, так чтобы в результате из четырех малых квадратов образовался один большой с длиной стороны 2k.

Далее из большого квадрата вырезаются клетки с числами от 1 до k^2, для каждого числа одна клетка. Процесс шифрования происходит следующим образом. Сделанная решетка (квадрат с прорезями) накладывается на чистый квадрат 2k×2k и в прорези по строчкам (т.е. слева направо и сверху вниз) вписываются первые буквы открытого текста. Затем решетка поворачивается на 90° по часовой стрелке и накладывается на частично заполненный квадрат, вписывание продолжается.

После третьего поворота, наложения и вписывания все клетки квадрата будут заполнены. Правило выбора прорезей гарантирует, что при заполнении квадрата буква на букву никогда не попадет. Из заполненного квадрата буквы можно выписать по столбцам, выбрав подходящий пароль.

Шифрование с помощью решеток в первой половине 1917 года германская армия использовала на Восточном (против России) фронте. В 1982 году его применяли британские войска в вооруженном конфликте с Аргентиной за Фолклендские острова.

Таблица Вижинера

Шифр Виженера — метод полиалфавитного шифрования буквенного текста с использованием ключевого слова.

Этот метод является простой формой многоалфавитной замены. Шифр Виженера изобретался многократно. Впервые этот метод описал Джован Баттиста Беллазо в 1553 году, однако в XIX веке получил имя Блеза Виженера, французского дипломата. Метод прост для понимания и реализации, он является недоступным для простых методов криптоанализа.

В шифре Цезаря каждая буква алфавита сдвигается на несколько строк; например в шифре Цезаря при сдвиге +3, A стало бы D, B стало бы E и так далее. Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов, называемая tabula recta или квадрат (таблица) Виженера. Применительно к латинскому алфавиту таблица Виженера составляется из строк по 26 символов, причём каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 26 различных шифров Цезаря. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова.

Выполнение работы

Реализация алгоритмов на языке Python

```
# Маршрутное шифрование

message = input('Введите строку: ').lower()
password = str(input('Введите пароль: ')).lower()

message=''.join(message.split())

n = len(password)
m=len(message)

message += 'a'*(n-m%n)

password_sort = ''.join(sorted(password))
index_list = []
for i in range (n):
    f_index = password.find(password_sort[i])
```

```
    index_list.append(f_index)

encrypted = ''
for i in index_list:
    for j in range(m//n):
        encrypted += message[j*n+i]

print("Криптограмма: ",encrypted)

# Таблица Вижинера

alphabet = 'абвгдежзийклмнопрстуфхцчшщьыэюя'

message = input('Введите строку: ').lower()
password = str(input('Введите пароль: ')).lower()

message=''.join(message.split())

n = len(password)
m=len(message)
k = (m % n)

password_len = '' + password * (m // n) + password[:k]
print(message, password_len, sep='\n')

shifr_visinera = []
slovar_i = 'абвгдежзийклмнопрстуфхцчшщьыэюя

import numpy as np

for i in range(len(alphabet)):
    shifr_visinera.append(slovar_i)
    new = slovar_i[1:] + slovar_i[0]
    slovar_i = new
shifr_visinera=np.array(shifr_visinera)
print("Квадрат вижинера:", shifr_visinera.reshape(31,1))

encrypted = ''

for i in range(m):
    f_index1 = alphabet.find(message[i])
    f_index2 = alphabet.find(password_len[i])
    encrypted += shifr_visinera[f_index1][f_index2]

print('Криптограмма:', encrypted)
```

Контрольный пример

```
# Маршрутное шифрование
```

```
message = input('Введите строку: ').lower()
password = str(input('Введите пароль: ')).lower()
```

```
Введите строку: нельзя недооценивать противника
Введите пароль: пароль
```

```
message=''.join(message.split())
```

```
n = len(password)
m=len(message)
```

```
message += 'a'*(n-m%n)
```

```
password_sort = ''.join(sorted(password))
index_list = []
for i in range (n):
    f_index = password.find(password_sort[i])
    index_list.append(f_index)
```

```
encrypted = ''
for i in index_list:
    for j in range(m//n):
        encrypted += message[j*n+i]
```

```
print("Криптограмма: ",encrypted)
```

```
Криптограмма:  еенпзоатьовоннеьлдиряцти
```

Пример работы алгоритма маршрутное шифрование

```
# Таблица Вижинера
```

```
alphabet = 'абвгдежзийклмнопрстуфхцчшщьыэюя'
```

```
message = input('Введите строку: ').lower()
password = str(input('Введите пароль: ')).lower()
```

```
Введите строку: криптография серьезная нпука
Введите пароль: математика
```

```
message=''.join(message.split())
```

```
n = len(password)
m=len(message)
k = (m % n)
```

```
password_len = '' + password * (m // n) + password[:k]
print(message, password_len, sep='\n')
```

```
криптографиясерьезнаянпука
математикаматематикаматема
```

```
shifr_visinera = []
slovar_i = 'абвгдежзийклмнопрстуфхцчшщьыэюя'
```

```
import numpy as np
```

```
for i in range(len(alphabet)):
    shifr_visinera.append(slovar_i)
    new = slovar_i[1:] + slovar_i[0]
    slovar_i = new
shifr_visinera=np.array(shifr_visinera)
#print("Квадрат Вижинера:", shifr_visinera.reshape(31,1))
```

```
encrypted = ''
```

```
for i in range(m):
    f_index1 = alphabet.find(message[i])
    f_index2 = alphabet.find(password_len[i])
    encrypted += shifr_visinera[f_index1][f_index2]
```

```
print('Криптограмма:', encrypted)
```

```
Криптограмма: црьфяохшкффядкэьчпчалнвшца
```

Пример работы алгоритма таблица Вижинера

Выводы

В ходе выполнения работы удалось изучить шифры перестановки, а также реализовать данные алгоритмы программно на языке Python.

Список литературы

1. Перестановочные шифры
2. Шифр Виженера
3. Шифр Виженера
4. ШИФРЫ ПЕРЕСТАНОВКИ