Лабораторная работа №2 Шифры перестановки

ВОЛКОВА ДАРЬЯ АЛЕКСАНДРОВНА НПММД-02-21

Цель работы

Изучение шифров перестановки:

1. Маршрутное шифрование
2. Шифрование с помощью решеток
3. Шифр Виженера

Задачи

Программная реализация шифров перестановки :

1. Маршрутное шифрование
2. Шифрование с помощью решеток
3. Шифр Виженера

Теоретические сведения

Перестановка представляет собой способ шифрования, при котором для получения шифрограммы символы исходного сообщения меняют местами. Например: апельсин – спаниель.

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.

Шифр Виженера — метод полиалфавитного шифрования буквенного текста с использованием ключевого слова. Этот метод является простой формой многоалфавитной замены. Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов или квадрат (таблица) Виженера.

Результаты

```
# 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 Цезаря

Результаты

```
# 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 шифр Вижинера

Выводы

В ходе выполнения работы удалось изучить шифры перестановки:

1. шифр Цезаря
2. шифр Атбаш

А также реализовать данные алгоритмы программно на языке Python.