Отчет по лабораторной работе 2

Дисциплина: Математические основы защиты информации и информационной безопасности

Дяченко З. К.

30 сентября 2022

Российский университет дружбы народов, Москва, Россия

Прагматика выполнения лабораторной работы

Данная лабораторная работа выполнялась мной для приобретения практических навыков шифрования с использованием шифров перестановки.

Цель выполнения лабораторной работы

Ознакомится и реализовать шифры перестановки.

Задачи выполнения лабораторной работы

Реализовать маршрутное шифрование (рис. - fig. 1 и - fig. 2).

In [2]:
```
import numpy as np
```

In [3]:
```
message="осенняя депрессия"
```

In [4]:
```
def sh1 (message, n, m, password):
    shifr=''
    a=len(message)%n
    if (a != 0):
        for i in range(n-a):
            message=message+'a'
    message1=list(message)
    message1 = np.reshape(message1, (-1, n))
    if (len(password)==n):
        b=sorted(password)
        n_col=np.empty(n)
        j=0
        for i in b:
            n_col[j]=password.index(i)
            j+=1
        for i in n_col:
            g=message1[:,int(i)]
            d=''.join(g)
            shifr=shifr+d
        print(shifr)
        print(message1)
```

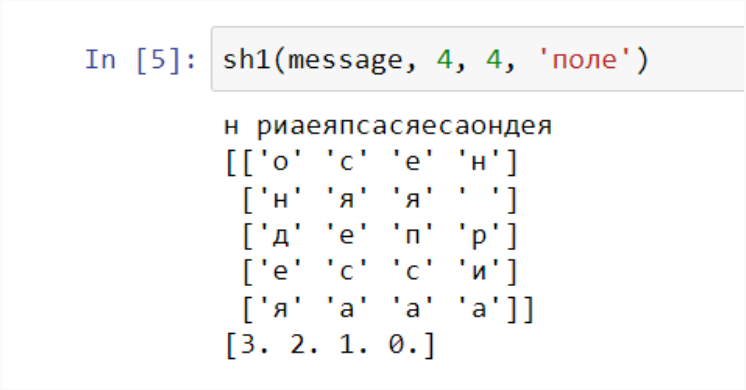

Рис. 2: Работа функции, выполняющей маршрутное шифрование

Задачи выполнения лабораторной работы

Реализовать шифрование с помощью решеток (рис. fig. 3 - fig. 5).

```
In [9]: def turn(a):
            return np.array(tuple(zip(*a[::-1])))
```

Рис. 3: Функция поворота

Задачи выполнения лабораторной работы

In [31]:

```
def sh2 (message, password):
    k=2
    shifr=''
    message1=list(message)
    a=[i for i in range(1,k*k+1)]
    a = np.reshape(a, (-1, k))
    b=turn(a)
    res1=np.concatenate((a, b), axis=1)
    c=turn(turn(b))
    d=turn(b)
    res2=np.concatenate((c, d), axis=1)
    res=np.concatenate((res1, res2), axis=0)
    res[0][3]=0
    res[2][1]=0
    res[2][3]=0
    res[3][2]=0
    krypt=np.full((2*k, 2*k), 'a')
    n=0
    l=0
    while l<4:
        for i in range(0,2*k):
            for j in range(0, 2*k):
                if (res[i][j]==0):
                    krypt[i][j]=message1[n]
                    n=n+1
                j=j+1
            i=i+1
        res=turn(res)
        l=l+1
    b=sorted(password)
    n_col=np.empty(len(password))
    j=0
    for i in b:
        n_col[j]=password.index(i)
        j+=1
    for i in n_col:
        g=krypt[:,int(i)]
        d=''.join(g)
        shifr=shifr+d
    print(res)
    print(krypt)
    print(n_col)
    print(shifr)
```

```
In [32]: sh2("договорподписали", "шифр")
```

```
[[1 2 3 0]
 [3 4 4 2]
 [2 0 4 0]
 [1 3 0 1]]
[['с' 'о' 'а' 'д']
 ['д' 'в' 'п' 'л']
 ['о' 'о' 'и' 'г']
 ['и' 'р' 'о' 'п']]
[1. 3. 2. 0.]
оворддлгпапиосдои
```

Рис. 5: Работа функции, выполняющей шифрование с помощью решеток

Реализовать шифр Виженера (рис. - fig. 6 и - fig. 7).

```
In [33]: alphabet="абвгдежзийклмнопрстуфхцчшщьыэюя"

In [55]: def table(alphabet):
             table1=list(alphabet)
             temp=table1
             for i in range(len(alphabet)):
                 temp=temp[1:]+temp[:1]
                 table1=np.concatenate((table1, temp), axis=0)
             table1=np.reshape(table1, (-1, (len(alphabet))))
             return table1
```

Рис. 6: Функция создания таблицы с алфавитом

Задачи выполнения лабораторной работы

In [56]:
```
def sh3(message, alphabet, password):
    shifr=''
    a=len(message)
    pw=password
    l_p=len(password)
    i=0
    if (a>l_p):
        while a!=l_p:
            pw=pw+pw[i]
            i=i+1
            l_p=l_p+1
    table2=table(alphabet)
    for k in range(a):
        i=alphabet.find(message[k])
        j=alphabet.find(pw[k])
        shifr=shifr+table2[i][j]
    return shifr
```

In [57]:
```
sh3("криптографиясерьезнаянаука", alphabet, "математика")
```

Out[57]:
```
'црьфяохшкффядкэьчпчалнтшца'
```

Рис. 7: Реализация шифра Виженера и результат

Результаты выполнения лабораторной работы

Результатом выполнения работы стала реализация маршрутного шифрования, шифрования с помощью решеток и шифра Виженера на Python, что отражает проделанную мной работу и полученные новые знания.