Лабораторная работа №2

Сапёров Максим Александрович - студент группы НПМмд-02-22

08.01.2022

Шифры перестановки

Прагматика выполнения

Умение пользоваться методами маршрутного, решеточного, Виженера шифрований

Цель выполнения лабораторной работы

Освоить на практике использование методов маршрутного, решеточного, Виженера шифрований

Задачи выполнения работы

Написать функции, которые реализуют шифрование маршрутного, решеточного, Виженера.

Результаты выполнения лабораторной работы. Написал код для зашивровки кодов Маршрутным шифрованием

```
[5]  def split(text, lenght):
       return [text[i:i+lenght] for i in range(0, len(text), lenght)]
```

```
def cipher(text, password):
  order = {
      val : num for num, val in enumerate(sorted(password))
  }
  password_order = {
      val : num for num, val in enumerate(password)
  }
  ciphertext = ''
  for letter in order.keys():
    for part in split(text, len(password)):
      try:
        ciphertext+=part[password_order[letter]]
      except:
        continue
  return ciphertext
```

Figure 1: функция шифрования Маршрутным шифрованием

Написал код для зашивровки кодов с помощью решеточного шифрования

```
[ ]    from math import *
       import numpy as np
       from os import *

       a = list(input("Enter key: "))
       b = list(input("Enter message: "))


       lenKY=ceil(sqrt(len(a)))
       lenpt=ceil(sqrt(len(b)))
```

```
[ ]    def matcal(lengthkey,lenplain, ceilky):
           column = 0
           if(lenplain%2==0):
               column = lenplain/ceilky;
               return int(ceil(column))
           else:

               lenplain+=1;
               column = lenplain/ceilky;
           return int(column)
```

Figure 2: функция шифрования решетками 1

```
column1 = matcal(len(a),len(b),lenKY)


km = [[0]*lenKY for i in range(lenKY)]
ptm = [[0]*column1 for i  in range(lenKY)]
cpm = [[0]*column1 for i in range(lenKY)]

z=97

for i in range(lenKY*lenKY):
    if((lenKY*lenKY)!=len(a)):
        a.append(chr(z))
        z=z+1

def getkeymatrix(key):
    k = 0;
    for i in range(lenKY):
        for j in range(lenKY):
            km[i][j] = ord(a[k])%97
            k+=1

#Generate Cipher Matrix
def encrypt(plaintext):
    for i in range(lenKY):
        for j in range(column1):
            cpm[i][j] = 0
            for x in range(lenKY):
                cpm[i][j] += (km[i][x] * ptm[x][j])
            cpm[i][j] = cpm[i][j] %26
    return cpm
```

Figure 3: функция шифрования решетками 2

```
[ ]    def GrillCipher(message, key):
           getkeymatrix(a)
           mat_b=ptm
           for i in range(len(b)):
               mat_b[i%lenKY][floor(i/lenKY)] = ord(b[i]) % 97
           cpm = encrypt(ptm)
           cpt = []
           for i in range(column1):
               for j in range(lenKY):
                   cpt.append(chr(cpm[j][i] + 97))

           print("Ciphertext: ", "".join(cpt))
```

Figure 4: функция шифрования решетками 3

Написал код для зашивровки кодов с помощью таблицы Виженера

```
[91]  def form_dict():
        d = {}
        iter = 0
        for i in range(97,123):
          d[iter] = chr(i)
          iter += 1
        return d
```

```
[82]  def encode_val(text):
        list_code = []
        l = len(text)
        d = form_dict()

        for i in range(l):
          for value in d:
            if text[i] == d[value]:
              list_code.append(value)
        return list_code
```

```
[83]  def comparator(value, key):
        len_key = len(key)
        dic = {}
        iter = 0
        full = 0

        for i in value:
          dic[full] = [i,key[iter]]
          full +=1
          iter +=1
          if iter>=len_key:
            iter=0
        return dic
```

Figure 5: зашивровки кодов с помощью таблицы Виженера

Результаты тестов.

```
[108]   cipher('нельзянедооцениватьпротивникаа','пароль')

'еенпнзоатаьовокннеьвлдирияцтиа'

[109]   Vig_cipher(encode_val('hello'), encode_val('key'))

'rijvs'

[112]   GrillCipher('hello', 'key')

Ciphertext:  imyeky
```

Figure 6: Результаты тестов

Выводы

Освоил на практике применение методов маршрутного, решеточного, Виженера шифрований