Отчёт по лабораторной работе №2

Шифры перестановки

Александр Олегович Воробьев

Содержание

List of Figures

List of Tables

1 Цель работы

Приобрести практические навыки реализации шифров перестановки.

2 Выполнение лабораторной работы

1. На языке Python реализовал маршрутное шифрование.

```
[2]  rus = "абвгдеёжзийклмнопрстуфхцчшщъыьэюя"

[ ]  def marshrut(text, key, m, n):
       global rus
       textws = text.replace(" ", "")
       if len(textws) < m * n:
         textws += rus[:m*n - len(textws)]
       t = iter(textws)
       matrix = [[next(t) for y in range(m)] for x in range (n)]
       ps = [rus.index(x) for x in key]
       pss = sorted(ps)
       output = ""
       for letter in pss:
         for x in range(n):
           output += matrix[x][ps.index(letter)]
       return output

[ ]  print((marshrut("нельзя недооценивать противника", "пароль", 6, 5)))

     еенпнзоатаьовокннеьвлдирияцтиа
```

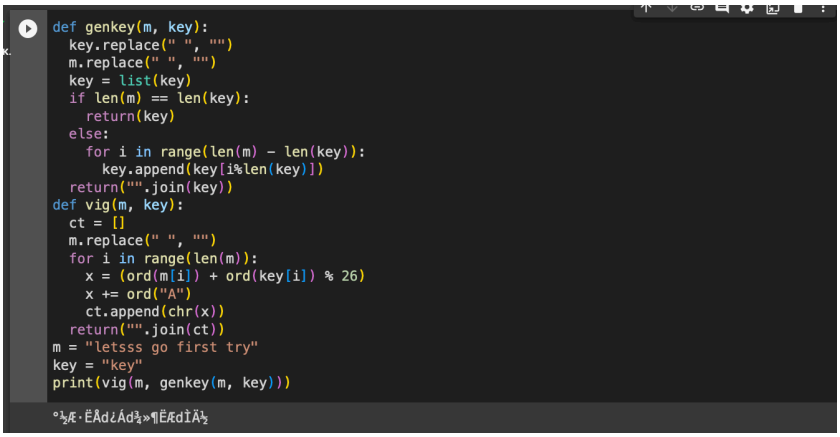
Figure 2.1: Маршрутный шифр

2. Аналогично на языке Python реализовал шифрование с помощью решеток.

```
import numpy as np

k = 2
k_2 = [x + 1 for x in range(k ** 2)]
matrix = [[0 for x in range(2 * k)] for y in range(2 * k)]
matrix = np.array(matrix)

for x in range(k ** 2):
  c = 0
  for x in range(k):
    for y in range(k):
      matrix[x][y] = k_2[c]
      c += 1
  matrix = np.rot90(matrix)

ds = {k: 0 for k in k_2}
dss = {1:2, 2:4, 3:3, 4:3}

for x in range(k ** 2):
  for y in range(k ** 2):
    ds[matrix[x][y]] += 1
    if ds[matrix[x][y]] != dss[matrix[x][y]]:
      matrix[x][y] = -1
    else:
      matrix[x][y] = 0
text = "договороподписали"
key = "шифр"

ct = 0
t = iter(text)
matrixt = [["o" for y in range(k ** 2)] for x in range(k ** 2)]
for d in range(4):
  for x in range(k ** 2):
    for y in range(k ** 2):
      if matrix[x][y] == 0:
        matrixt[x][y] = text[ct]
        ct += 1
  matrix = np.rot90(matrix, -1)
ps = [rus.index(x) for x in key]
pss = sorted(ps)
output = ""
for letter in pss:
  for x in range(k ** 2):
    output += matrixt[x][ps.index(letter)]
print(output)

овордлгпаиосдои
```

Figure 2.2: Реализация шифрования с помощью решеток

3. Реализовал шифр Виженера.



```
def genkey(m, key):
  key.replace(" ", "")
  m.replace(" ", "")
  key = list(key)
  if len(m) == len(key):
    return(key)
  else:
    for i in range(len(m) - len(key)):
      key.append(key[i%len(key)])
  return("".join(key))
def vig(m, key):
  ct = []
  m.replace(" ", "")
  for i in range(len(m)):
    x = (ord(m[i]) + ord(key[i]) % 26)
    x += ord("A")
    ct.append(chr(x))
  return("".join(ct))
m = "letsss go first try"
key = "key"
print(vig(m, genkey(m, key)))
```

```
°½Æ·ËÅd¿Ád¾»¶ËÆdÌÄ½
```

Figure 2.3: Реализация шифра Виженера

3 Выводы

Приобрел практические навыки реализации шифров перестановки.

Список литературы

1. Кулябов Д.С. Лабораторная работа No 2. Шифры перестановки [Электронный ресурс] - 4 с.