

# Отчет по лабораторной работе №2.

Шифры перестановки

---

Alexander O. Vorobyov<sup>1</sup>

28 September, 2023

<sup>1</sup>RUDN University, Moscow, Russian Federation

## Прагматика выполнения

---

Лабораторная работа выполняется для получения знаний о шифрах перестановки и их реализации.

## Цель работы

---

Целью данной работы является приобретение практических навыков реализации маршрутного шифра, шифрования с помощью решеток и шифра Виженера.

## Задачи выполнения

---

## 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)))

еенпнзозаъавокннеъвдиряцтиа
```

- 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;6, 4;8)

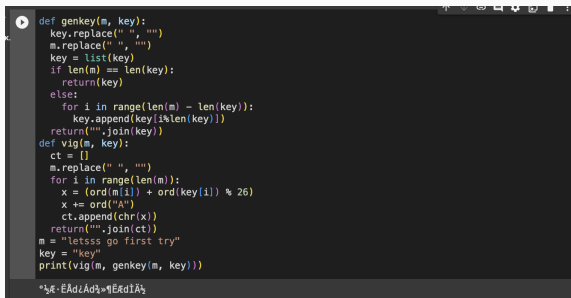
for x in range(k ** 2):
    for y in range(k ** 2):
        ds[matrix[x][y]] += 1
        if ds[matrix[x][y]] != dss[matrix[x][y]]:
            matrix[x][y] = -1
        else:
            matrix[x][y] = 0
text = "anastasiyapavlov"
key = "unsp"

ct = 0
t = iter(text)
matrix = [[0 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:
                matrix[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 += matrix[x][ps.index(letter)]
    print(output)
```

Figure 1: Реализация шифрования с помощью решеток



## 2. 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)))
```

Figure 2: Реализация шифра Виженера

## Результаты выполнения

---

В результате проделанной работы я приобрел практические навыки реализации шифров перестановки.