**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ**
**Факультет физико-математических и естественных наук**

**Кафедра прикладной информатики и теории вероятностей**

# Отчёт по лабораторной работе 2

*Дисциплина*: *Математические основы защиты информации и информационной безопасности*

Студент: Румянцева Александра Сергеевна, 1132223493
Группа: НПМмд-02-22
Преподаватель: Кулябов Дмитрий Сергеевич,
д-р.ф.-м.н., проф.

Москва 2022

# Содержание

# List of Figures

# List of Tables

# 1 Цель работы

Целью данной лабораторной работы является ознакомление с тремя методами шифрования: маршрутным шифрованием, шифрованием с помощью решеток, таблицей Виженера, а так же их реализация на произвольном языке программирования.

# 2 Задание

1. Реализовать метод маршрутного шифрования.
2. Реализовать метод шифрования с помощью решеток.
3. Реализовать метод таблицы Вижера.

# 3 Теоретическое введение

Математическая часть подробно описана в задании к лабораторной работе. Я поставила перед собой задачу найти исторические сведения, факты о методах шифрования.

**Шифр перестановки** — это метод симметричного шифрования, в котором элементы исходного открытого текста меняют местами. Элементами текста могут быть отдельные символы, пары букв, тройки букв, комбинирование этих случаев и так далее. Типичными примерами перестановки являются анаграммы. В классической криптографии шифры перестановки можно разделить на два класса:

1. Шифры одинарной (простой) перестановки — при шифровании символы открытого текста перемещаются с исходных позиций в новые один раз.

2. Шифры множественной (сложной) перестановки — при шифровании символы открытого текста перемещаются с исходных позиций в новые несколько раз.

Метод **маршрутного шифрования** изобрел французский математик и криптограф Франсуа Виет. Этот способ относится к перестановочным шифрам. Шифр называется перестановочным, если все связанные с ним криптограммы получаются из соответствующих открытых текстов перестановкой букв. Способ, каким при шифровании переставляются буквы открытого текста, и является ключом шифра. Такой метод шифрования (столбцовая перестановка) в годы первой мировой войны использовала легендарная немецкая шпионка Мата Хари.

**Шифровальная решётка** — трафарет с прорезями-ячейками (из бумаги, картона или аналогичного материала), использовавшийся для шифрования открытого текста. Текст наносился на лист бумаги через такой трафарет по определённым правилам, и расшифровка текста была возможна только при наличии такого же трафарета.

**Вращающаяся решетка**: Прямоугольные решётки Кардано можно размещать в четырёх позициях. Шифр с сеткой в виде шахматной доски имеет только две позиции, но именно этот вариант вращающейся решётки послужил для разработки более сложной решётки с четырьмя позициями, которую можно вращать в двух направлениях.

**Шифр Виженера** является простой формой многоалфавитной замены. Шифр Виженера изобретался многократно. Впервые этот метод описал Джован Баттиста Беллазо (итал. Giovan Battista Bellaso) в книге La cifra del. Sig. Giovan Battista Bellaso в 1553 году, однако в XIX веке получил имя Блеза Виженера, французского дипломата. Метод прост для понимания и реализации, он является недоступным для простых методов криптоанализа.

# 4 Выполнение лабораторной работы

## 4.1 Маршрутное шифрование

В соответствии с заданием, первой была написана программа для маршрутного шифрования (рис. 1-2). В качестве параметров системы были взяты данные из описательной части лабораторной работы портала ТУИС.

*Примечание:* комментарии по коду ализации маршрутного шифрования представлены на скриншотах.

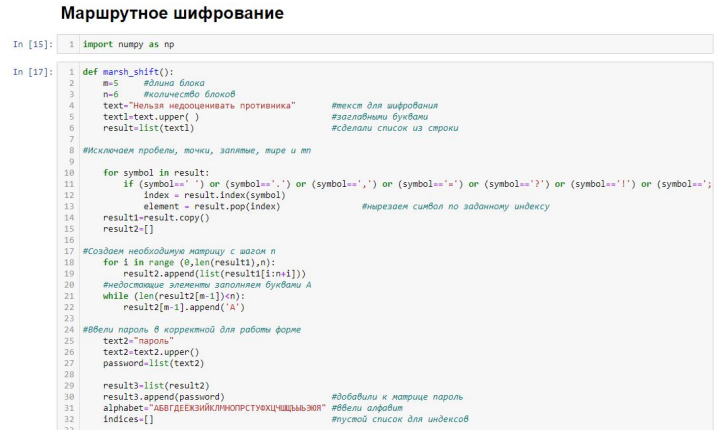



Figure 4.1: Рис. 1. 1 часть программного кода реализации маршрутного шифрования.

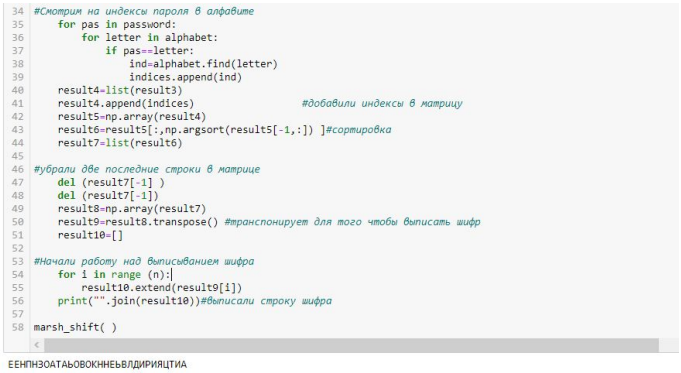



Figure 4.2: Рис. 2. 2 часть программного кода реализации маршрутного шифрования.

Результат выполнения программы видно на рис. 2. Результат можно назвать успешным, он совпадает с шифрованием из примера в ТУИСе РУДН, при этом само по себе шифрование однозначно, поэтому совпадение результата говорит о правильности выполнения работы.

## 4.2 Метод решеток

Далее была написана программа релизации шифрования методом решеток (рис. 3-6). В качестве параметров системы были взяты данные из описательной части лабораторной работы портала ТУИС.

*Примечание:* комментарии по коду рализации маршрутного шифрования представлены на скриншотах.

**Метод решеток**

In [18]:
```
import numpy as np
import random
```

In [23]:
```
def turning_grille():
    k=2       #вводим k

    #заполняем маленькую матрицу
    osnova=np.linspace(1,k**2,k**2)
    result=[]
    for i in range(0,len(osnova),k):
        result.append(list(osnova[i:i+k]))

    #вводим функцию для поворота матрицы
    def rot90(matrix):
        return [list(reversed(col)) for col in zip(*matrix)]

    matrix=np.full((2*k,2*k),0)        #создали и заполнили нулями матрицу 2k x 2k

    #заполняем матрицу matrix по четвертям
        #1 четверть
    matrix[:k,:k]=result
        #2 четверть
    result2=rot90(result)
    matrix[:k,k:2*k]=result2
        #3 четверть
    result3=rot90(result2)
    matrix[k:2*k,k:2*k]=result3
        #4 четверть
    result4=rot90(result3)
    matrix[k:2*k,:k]=result4
```

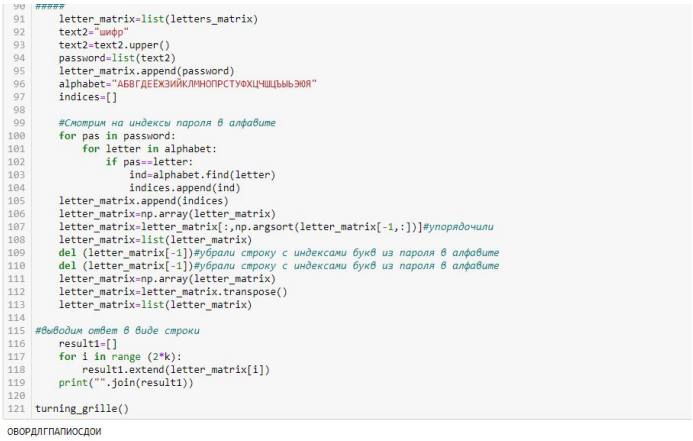
Figure 4.3: Рис. 3. 1 часть программного кода реализации шифрования с помощью метода решеток.

```
#работа с отверстиями (определение координат)
holes=[]
for i in range (1,k**2+1):#прогонка по отдельному числу, например, по единичкам
    indexes=[ ]
    for m in range(0,2*k):#прогонка по строкам
        for j in range(0,2*k):#прогонка по столбцам
            if matrix[m][j]==i:
                coords=tuple([m, j])
                indexes.append(coords)
    find=random.randint(0,3)#выбираем 1 из 4 координат
    holes.append(indexes[find])

#работа с отверстиями (продолжение) визуализация поворотов и случаев размещений отверстий
template=np.full((2*k,2*k),0)
for d in range (k**2):
    template[holes[d][0],holes[d] [1]] =1
#1 поворот
template1=rot90(template)
#2 поворот
template2=rot90(template1)
#3 поворот
template3=rot90(template2)
text="ДОГОВОРПОДПИСАЛИ"
```

Figure 4.4: Рис. 4. 2 часть программного кода реализации шифрования с помощью метода решеток.

```
    #прогоняем templates для нахождения координат для заполнения буквами
    #1 поворот
    indexes1=[]
    for m1 in range (0,2*k):
        for j1 in range (0,2*k):
            if template1[m1][j1]==1:
                coords1=tuple([m1,j1])
                indexes1.append(coords1)
    #2 поворот
    indexes2=[]
    for m2 in range (0,2*k):
        for j2 in range (0,2*k):
            if template2[m2][j2]==1:
                coords2=tuple([m2,j2])
                indexes2.append(coords2)
    #3 поворот
    indexes3=[]
    for m3 in range (0,2*k):
        for j3 in range (0,2*k):
            if template3[m3][j3]==1:
                coords3=tuple([m3,j3])
                indexes3.append(coords3)

    #Переходим к образованию матрицы с буквами
    letters_matrix=np.full((2*k,2*k),'O')
    #0
    for d in range (k**2):
        letters_matrix[holes[d][0], holes[d][1]]=text[d]
    #1
    for d in range (k**2):
        letters_matrix[indexes1[d][0],indexes1[d][1]]=text[d+k**2]
    #2
    for d in range (k**2):
        letters_matrix[indexes2[d][0], indexes2[d][1]]=text[d+2*(k**2)]
    #3
    for d in range (k**2):
        letters_matrix[indexes3[d][0],indexes3[d][1]]=text[d+3*(k**2)]
#####
```

Figure 4.5: Рис. 5. 3 часть программного кода реализации шифрования с помощью метода решеток.



```
#####
    letter_matrix=list(letters_matrix)
    text2="шифр"
    text2=text2.upper()
    password=list(text2)
    letter_matrix.append(password)
    alphabet="АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ"
    indices=[]

    #Смотрим на индексы пароля в алфавите
    for pas in password:
        for letter in alphabet:
            if pas==letter:
                ind=alphabet.find(letter)
                indices.append(ind)
    letter_matrix.append(indices)
    letter_matrix=np.array(letter_matrix)
    letter_matrix=letter_matrix[:,np.argsort(letter_matrix[-1,:])]#упорядочили
    letter_matrix=list(letter_matrix)
    del (letter_matrix[-1])#убрали строку с индексами букв из пароля в алфавите
    del (letter_matrix[-1])#убрали строку с индексами букв из пароля в алфавите
    letter_matrix=np.array(letter_matrix)
    letter_matrix=letter_matrix.transpose()
    letter_matrix=list(letter_matrix)

#выводим ответ в виде строки
    result1=[]
    for i in range (2*k):
        result1.extend(letter_matrix[i])
    print("".join(result1))

turning_grille()
```

```
ОВОРДЛГПАПИОСДОИ
```

Figure 4.6: Рис. 6. 4 часть программного кода реализации шифрования с помощью метода решеток.

Результат выполнения программы видно на рис. 6. Результат можно назвать успешным, он совпадает с шифрованием из примера в ТУИСе РУДН. При этом само по себе шифрование неоднозначно, поскольку используется модуль рандом для порядка размещения символов, поэтому погли появляться и другие варианты шифрования.

## 4.3 Метод Виженера

Последним реализованным методом был метод Виженера (рис. 7). В данном методе я шифровала фразы из английского алфавита.


Figure 4.7: Рис. 7. Программного кода реализации шифра Виженера.

Далее было реализовано дешифрование текста (рис. 8). Важно отметить, что нужно использовать одинаковый ключ (кодовое слово) как для шифровки, так и для шифрования.

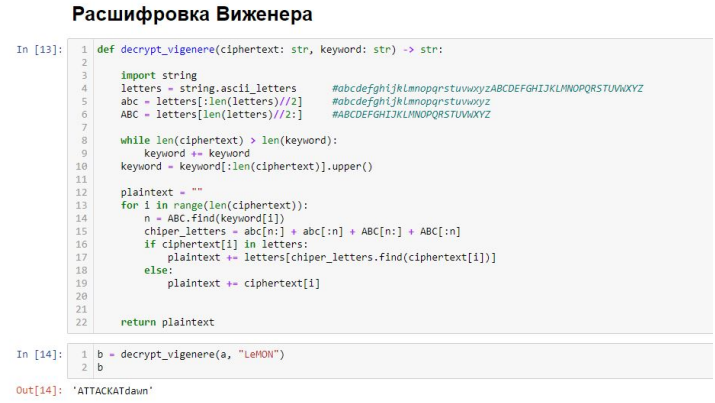



Figure 4.8: Рис. 8. Программного кода реализации расшифровки шифра Виженера.

Как можно видеть, расшифровка совпадает с изначальным текстом на рис. 7, что говорит об успешной реализации метода.

# 5 Библиография


1. ТУИС РУДН

2. Википедия. Перестановочный шифр [Электронный ресурс]. Википедия, свободная энциклопедия, 2021. URL: https://en.wikipedia.org/wiki/Transposition_cipher.

3. VK. Метод маршрутного шифрования [Электронный ресурс]. VK, 2018. URL: https://vk.com/@cryptandcod-metod-marshrutnogo-shifrovaniya.

4. Википедия. Шифровальная решетка [Электронный ресурс]. Википедия, свободная энциклопедия, 2021. URL: https://en.wikipedia.org/wiki/Grille_(cryptography).

5. Wix. Криптография [Электронный ресурс]. Wixsite, 2021. URL: https://en.wikipedia.org/wiki/Grille_(cryptography).

6. Википедия. Шифр Виженера [Электронный ресурс]. Википедия, свободная энциклопедия, 2021. URL: https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher.

# 6 Выводы

Таким образом, была достигнута цель, поставленная в начале лабораторной работы: я ознакомилась с тремя методами шифрования – маршрутным шифрованием, шифрованием с помощью решеток, таблицей Виженера, а так же мне удалось реализовать их на языке программирования Python.