

# **Отчет по лабораторной работе номер 2**

Хамбалеев Булат Галимович

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Задание</b>	<b>6</b>
<b>3</b>	<b>Теория</b>	<b>7</b>
<b>4</b>	<b>Выполнение работы</b>	<b>8</b>
<b>5</b>	<b>Библиография</b>	<b>12</b>
<b>6</b>	<b>Выводы</b>	<b>13</b>

# List of Tables

## List of Figures

4.1	рис.1. Класс marshrut. . . . .	9
4.2	рис.2. Маршрутное шифрование в действии. . . . .	10
4.3	рис.3. Класс Вижнер. . . . .	11
4.4	рис.4. Шифр Вижнера в действии. . . . .	11

# 1 Цель работы

Реализовать программно алгоритмы маршрутного шифрования и шифра Виженера.

## 2 Задание

Задание подразумевает реализацию алгоритма шифров на языке программирования.

## 3 Теория

Шифр Виженера это метод полиалфавитного шифрования буквенного текста с использованием ключевого слова. Этот метод является простой формой многоалфавитной замены.

## 4 Выполнение работы

1. Реализуем класс `marshrut` маршрутного шифрования.(рис. 1)



```

class marshrut():

    def __init__(self,password):
        self.m = 0
        self.n = len(password)
        self.password = password
        self.table = []

    def code(self, text):
        table = []
        while text:
            table.append(list(text[:self.n]))
            text = text[self.n:]
        while len(table[-1])<self.n:
            table[-1].append('a')
        self.m = len(table)
        self.table = table

        d = {k:v for k,v in zip(self.password,range(self.n))}
        a = sorted(d)
        b = [d[i] for i in a]
        ans = []

        for j in b:
            for i in range(self.m):
                ans.append(self.table[i][j])
        ans = ''.join(ans)

        return ans,self.m,self.n

    def decode(self,text,key,m,n):
        d = {k:v for k,v in zip(key,range(n))}
        a = sorted(d)
        b = [d[i] for i in a]

        table = [['_' for i in range(n)] for j in range(m)]
        k=0

        for j in b:
            for i in range(m):
                table[i][j]=text[k]
                k+=1

        return ''.join([''.join(l) for l in table])

```

Figure 4.1: рис.1. Класс marshrut.

2. Проверим работу алгоритма. (рис. 2)

```

Ввод [168]: a = marshrut('пароль')
Ввод [169]: a.code('нельзя недооценивать противника')
Out[169]: ('еенпнзоатаьовокнньвдиряцтиа', 5, 6)
Ввод [170]: a.decode('еенпнзоатаьовокнньвдиряцтиа', 'пароль', 5, 6)
Out[170]: 'нельзя недооценивать противникаа'

Ввод [ ]:
Ввод [171]: b = marshrut('булат')
Ввод [172]: b.code('пойдёмте поиграем на улице')
Out[172]: ('дпауапимимийераёеаотгнц', 5, 5)
Ввод [116]: b.status()
5 5 [['н', 'о', 'й', 'д', 'ё'], ['м', 'т', 'е', 'н', 'о'], ['и', 'г', 'р', 'а', 'е'], ['м', 'н', 'а', 'у', 'л'], ['и', 'ц', 'е', 'а', 'а']]
Ввод [173]: b.decode('дпауапимимийераёеаотгнц', 'булат', 5, 5)
Out[173]: 'пойдёмте поиграем на улицеаа'
Ввод [110]: len('пойдёмте поиграем на улице')
Out[110]: 23
Ввод [177]: c = marshrut('кулябов')
Ввод [178]: c.code('давайте побавим побольше лабораторных курс')
Out[178]: ('йвлоаемшавадпетквбарттирхааоолоуаабнс', 6, 7)
Ввод [180]: c.decode('йвлоаемшавадпетквбарттирхааоолоуаабнс', 'кулябов', 6, 7)
Out[180]: 'давайте побавим побольше лабораторных курсаа'

```

Figure 4.2: рис.2. Маршрутное шифрование в действии.

### 3. Реализуем класс шифра Виженера. (рис. 3)

```

Ввод [317]: class Vigener():
    def __init__(self):
        self.string = 'АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЬЪЮЯ'
        string = 'АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЬЪЮЯ'
        abc = []
        for i in range(32):
            abc.append(list(string))
            string = string[1:] + string[0]

        self.abc = abc

    def code(self, text, password):
        text = text.upper()
        password = password.upper()
        while ' ' in text:
            text = text.replace(' ', '')
        s = ''
        if len(text) > len(password):
            while len(text) > len(password):
                password += password
            while len(password) > len(text):
                password = password[:-1]
            i = [self.string.find(password[k]) for k in range(len(password))]
            j = [self.string.find(text[k]) for k in range(len(text))]

            return ''.join([self.abc[a][b] for a, b in zip(j, i)])

    def decode(self, text, password):
        password = password.upper()
        if len(text) > len(password):
            while len(text) > len(password):
                password += password
            while len(password) > len(text):
                password = password[:-1]

            i = [self.string.find(password[k].upper()) for k in range(len(password))]
            j = [self.abc[k].index(p) for k, p in zip(i, text)]
            return ''.join([self.string[l] for l in j])

```

Figure 4.3: рис.3. Класс Виженер.

## 2. Проверим работу алгоритма.(рис. 4)

```

Ввод [2]: l = Vigener()

Ввод [3]: l.code('криптографиясерьезнаянаука', 'математика')
Out[3]: 'ЦРЬФЮХЩКФЯГКБЪЧПЧЛНТЩЦА'

Ввод [4]: l.decode('ЦРЬФЮХЩКФЯГКБЪЧПЧЛНТЩЦА', 'математика')
Out[4]: 'КРИПТОГРАФИЯСЕРЬЕЗНАЯНАУКА'

Ввод [5]: l.code('я с удовольствием провел время', 'булат')
Out[5]: 'АДЮДАГБЦЬГУХУЕКРГШВЧФХЫЕЮА'

Ввод [6]: l.decode('АДЮДАГБЦЬГУХУЕКРГШВЧФХЫЕЮА', 'булат')
Out[6]: 'ЯСУДОВЛЬСТВИЕМПРОВЕЛВРЕМЯ'

Ввод [7]: l.code('ялюблюхорошопокушать', 'кухнязаполнена')
Out[7]: 'ЙЮУОКЕХЭЮШХУЪОФЖНСБ'

Ввод [8]: l.decode('ЙЮУОКЕХЭЮШХУЪОФЖНСБ', 'кухнязаполнена')
Out[8]: 'ЯЛЮБЛЮХОРОШОПОКУШАТЬ'

Ввод [ ]:

```

Figure 4.4: рис.4. Шифр Виженера в действии.

## 5 Библиография

1. ТУИС РУДН
2. [https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80\\_%D0%92%D0%B8%D0%](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%92%D0%B8%D0%)

## **6 Выводы**

Во время выполнения лабораторной работы я освоил на практике маршрутное шифрование и шифр Виженера.