**Лабораторная работа №8. Python. Простые методы шифрования: метод Цезаря, Полибианский квадрат, метод Вижинера**

**Цель работы:** приобретение навыков работы по трем методам простого шифрования.

### 7.1 Рабочее задание

Реализовать программы кодирования и декодирования:

1) Методом Цезаря (ключ = порядковый номер студента по списку группы, фраза для шифрования = любое словосочетание);
2) Полибианским квадратом (в начале пишется фамилия и имя студента, фраза для шифрования = любое словосочетание);
3) Методом Вижинера (ключ = фамилия и имя студента, фраза для шифрования = любое словосочетание).

### 7.2 Методические указания к выполнению лабораторной работы

1. Метод Цезаря. В примере на рисунке 14 показан результат кодирования фразы «криптография, это наука» с ключом = -1. Необходимо также написать программу декодирования (преподавателем дается фраза для декодирования; определить ключ и фразу, подвергшуюся шифрованию).

```
Вариант 23: СИБ-15-1, студент Иванов И.И.
----------------------------------------
Это программа КОДИРОВАНИЯ методом Цезаря
введите текст для шифрования:криптография - это наука
вы ввели: криптография - это наука   ключ шифрования= -1
посимвольная разбивка и расшифровка:
к = 1082
р = 1088
и = 1080
п = 1087
т = 1090
о = 1086
г = 1075
р = 1088
а = 1072
ф = 1092
и = 1080
я = 1103
  = 32
- = 45
  = 32
э = 1101
т = 1090
о = 1086
  = 32
н = 1085
а = 1072
у = 1091
к = 1082
а = 1072
После наложения ключа, ответ:
йпзоснвпяузю , ьсн мятйя
```

Рисунок 14 – Принскрин работы программы по шифрованию методом Цезаря

2. Полибианский квадрат (прямоугольник).

На рисунке 15а показан листинг и результат работы программы на абстрактной матрице размером 7·5; студенту при выполнении задания необходимо ее под себя подкорректировать, вписав в начало таблицы буквы своих фамилии и имени без повторения, как, например, показано в таблице 4. Далее необходимо все полученные цифры при кодировании из матрицы записать без скобок и знаков «,» (вспомогательный принскрин с листингом представлены на рисунке 15б). Потом надо склеить все числа в одну строку – пример результата показан на рисунке 15в. Это и есть закодированная фраза с помощью квадрата Полибия.

Таблица 4 – Пример заполнения данными квадрата Полибия

| | **1** | **2** | **3** | **4** | **5** | **6** |
|---|---|---|---|---|---|---|
| **1** | З | У | Е | В | А | К |
| **2** | Т | Р | И | Н | Б | Г |
| **3** | Д | Ж | Л | М | О | П |
| **4** | Р | С | Т | Ф | Х | Ц |
| **5** | Ч | Ш | Щ | Ъ | Ь | Э |
| **6** | Ю | Я | - | , | . | ␣ |

```
matrix = [['а','б','в','г','д'],
          ['е','ж','з','и','к'],
          ['л','м','н','о','п'],
          ['р','с','т','у','ф'],
          ['х','ц','ч','ш','щ'],
          ['ъ','ы','ь','э','ю'],
          ['я','-',',','.',' ']]
def polibii(bukva):
    for i in range(len(matrix)):
        for j in  range(len(matrix[i])):
            if bukva ==  matrix[i][j]:
                return i+1, j+1
print("Вариант 23: СИБ-15-1, студент Иванов И.И.
print("----------------------------------------")
print("Это программа КОДИРОВАНИЯ Полибианским квадратом")
text=input("введите текст для шифрования:")
print("вы ввели фразу:",text)
for bukva in text.lower().replace('j','i'):
    print (polibii(bukva),end='')
```

а)

```
Вариант 23: СИБ-15-1, студент Иванов И.И.
----------------------------------------
Это программа КОДИРОВАНИЯ Полибианским квад
ратом
введите текст для шифрования:абвгдежзиклм
вы ввели фразу: абвгдежзиклм
(1, 1)(1, 2)(1, 3)(1, 4)(1, 5)(2, 1)(2, 2)(
2, 3)(2, 4)(2, 5)(3, 1)(3, 2)
```

```
import re
var = u'abce4387def..//-+,,,,zzqw5>?'
print("первоначальная строка:", var)
result=re.sub(u'[^a-z\s]*', u'', var)
print("полученная строка:", result)
```

б)

```
>>>
первоначальная строка: abce4387def..//-+,,,,zzqw5>
полученная строка: abcedefzzqw
```

в)

```
Результат шифрования - строка: 1112131415212222425313 2
```

Рисунок 15 – Листинг и результат работы алгоритма по абстрактной матрице

Декодирование. Дается некоторая строка чисел (подобно данным рисунка 15в) и, имея матрицу значений (подобно таблице 4), надо определить, какая фраза была зашифрована. Учитывая, что все числа состоят из одной цифры, обратная процедура декодирования (разбивки по парам) будет однозначной. Пример принскрина работы декодирования приведен на рисунке 16.

```
Вариант 23: СИБ-15-1, студент Иванов И.И.
----------------------------------------
Программа ДЕКОДИРОВАНИЯ Полибианским квадратом
введите строку для дешифрования:3511411115342542
вы ввели цифры: 3511411115342542
разбивка по парам: 3,5 1,1 4,1 1,1 1,5 3,4 2,5 4,2
ОТВЕТ - задуманная фраза: парадокс
```

Рисунок 16 – Пример работы программы декодирования

3. Шифр Вижинера.

Ключом выступает фамилия и имя студента (без букв повторения); на фразу накладывается ключ, если же длина ключа маленькая, то ключ дублируется. На рисунке 17 представлен листинг шифрования методом Вижинера по 10-тизначному ключу («ЗуеваЕкатерина») без букв повторения: «зуевактрин». На рисунке 18 представлен принскрин осуществления шифрования по листингу с рисунка 17.

```
print("Вариант 23: СИБ-15-1, студент Иванов И.И."); print(42*"-")
print("Это программа КОДИРОВАНИЯ методом Вижинера")
a=input("введите фразу для шифрования:"); n=len(a); key=('зуевактрин')
m=len(key); d=n//m; e=n%m; print("первоначальный ключ:",key)
print("ключ накладывается",d,"раз и",e,"букв")
if e==1:
    x=key[0];
    c=d*key+x
elif e==2:
    x=key[0]+key[1]
    c=d*key+x
elif e==3:
    x=key[0]+key[1]+key[2]
    c=d*key+x
elif e==4:
    x=key[0]+key[1]+key[2]+key[3]
    c=d*key+x
elif e==5:
    x=key[0]+key[1]+key[2]+key[3]+key[4]
    c=d*key+x
elif e==6:
    x=key[0]+key[1]+key[2]+key[3]+key[4]+key[5]
    c=d*key+x
elif e==7:
    x=key[0]+key[1]+key[2]+key[3]+key[4]+key[5]+key[6]
    c=d*key+x
elif e==8:
    x=key[0]+key[1]+key[2]+key[3]+key[4]+key[5]+key[6]+key[7]
    c=d*key+x
elif e==9:
    x=key[0]+key[1]+key[2]+key[3]+key[4]+key[5]+key[6]+key[7]+key[8]
    c=d*key+x
elif e==10:
    x=key[0]+key[1]+key[2]+key[3]+key[4]+key[5]+key[6]+key[7]+key[8]+key[9]
    c=d*key+x
else:
    print(c)
print("и полученный ключ =",c); print("ОТВЕТ после наложения ключа с текстом:")
for i in range (n):
    f=ord(a[i])+ord(c[i])
    if f>1103:
        q=f-1103; w=chr(q); w.lower(); print(w.lower(),end='')
```

Рисунок 17 – Листинг осуществления шифрования

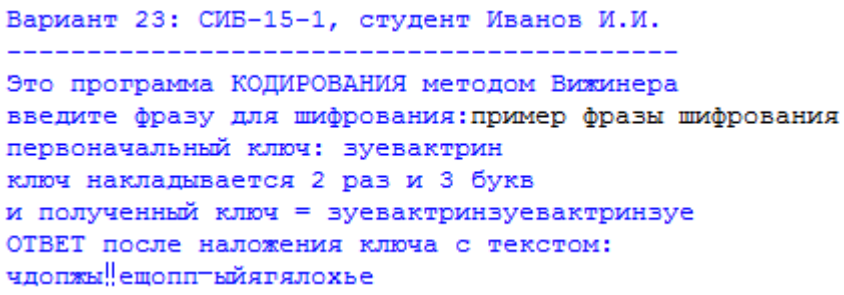


Рисунок 18 – Результат шифрования методом Вижинера

При декодировании надо, имея зашифрованную фразу и первоначальный ключ, восстановить исходный текст (пример результата работы программы декодирования представлен на рисунке 19).

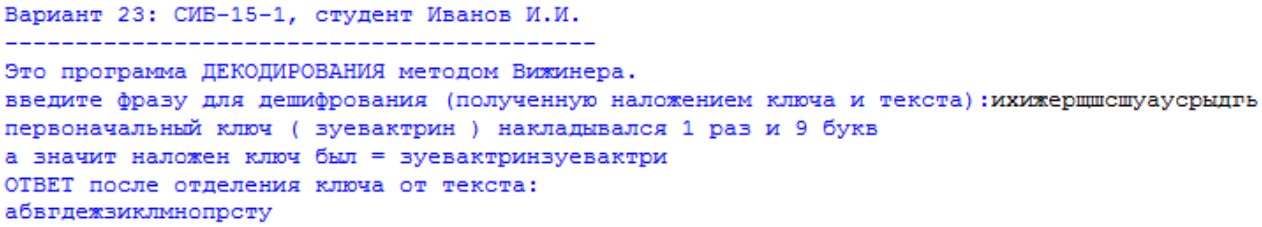


Рисунок 19 – Результат декодирования методом Вижинера

### 8.3 Список контрольных вопросов

1Какой оператор подставляет числовое значение букве, а какой представляет буквенное значение цифре?

2По таблице Ascii, в каком диапазоне лежат буквы английского алфавита?

3По таблице Ascii, в каком диапазоне лежат буквы русского алфавита?