Отчёт по лабораторной работе 8

Радимов Игорь

18 декабря, 2021

Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

Задание

Лабораторная работа подразумевает использование языков программирования для создания программы для щифрования и дещифрования в режиме однократного гаммирования при известном ключе.

Выполнение лабораторной работы

Выполнение лабораторной работы

1. Импортируем библиотеки random,string..

```
[4]: import string
     import random
```

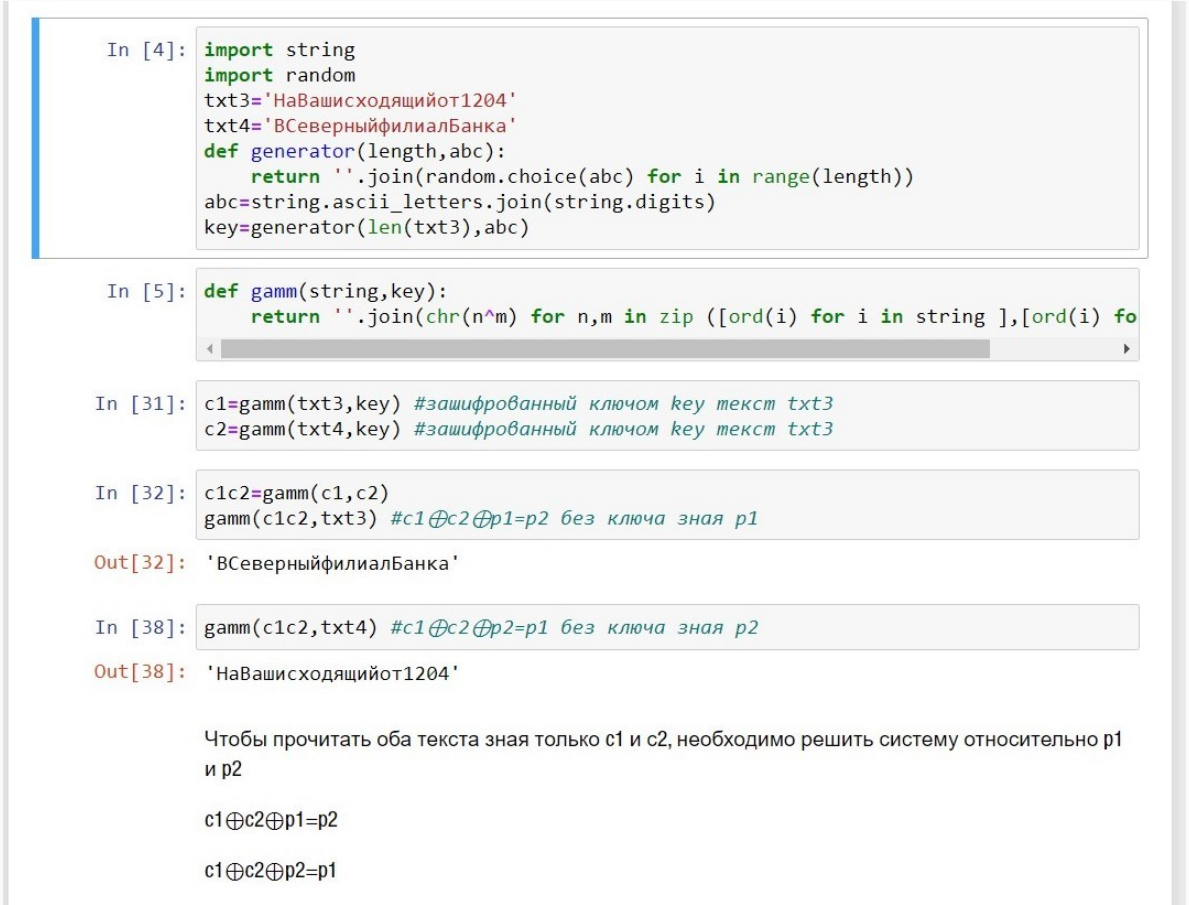
Figure 1: рис.1. Импорт библиотек.

2. Зададим строковые переменные.

```
import random
txt3='НаВашисходящийот1204'
txt4='ВСеверныйфилиалБанка'
def generator(length, abc):
```

Figure 2: рис.2. Строковые переменные.

3. Зададим функции гаммирования, и дешифрования.



In [4]:
```
import string
import random
txt3='НаВашисходящийот1204'
txt4='ВСеверныйфилиалБанка'
def generator(length,abc):
    return ''.join(random.choice(abc) for i in range(length))
abc=string.ascii_letters.join(string.digits)
key=generator(len(txt3),abc)
```

In [5]:
```
def gamm(string,key):
    return ''.join(chr(n^m) for n,m in zip ([ord(i) for i in string ],[ord(i) fo
```

In [31]:
```
c1=gamm(txt3,key) #зашифрованный ключом key текст txt3
c2=gamm(txt4,key) #зашифрованный ключом key текст txt3
```

In [32]:
```
c1c2=gamm(c1,c2)
gamm(c1c2,txt3) #c1⊕c2⊕p1=p2 без ключа зная p1
```

Out[32]: 'ВСеверныйфилиалБанка'

In [38]:
```
gamm(c1c2,txt4) #c1⊕c2⊕p2=p1 без ключа зная p2
```

Out[38]: 'НаВашисходящийот1204'

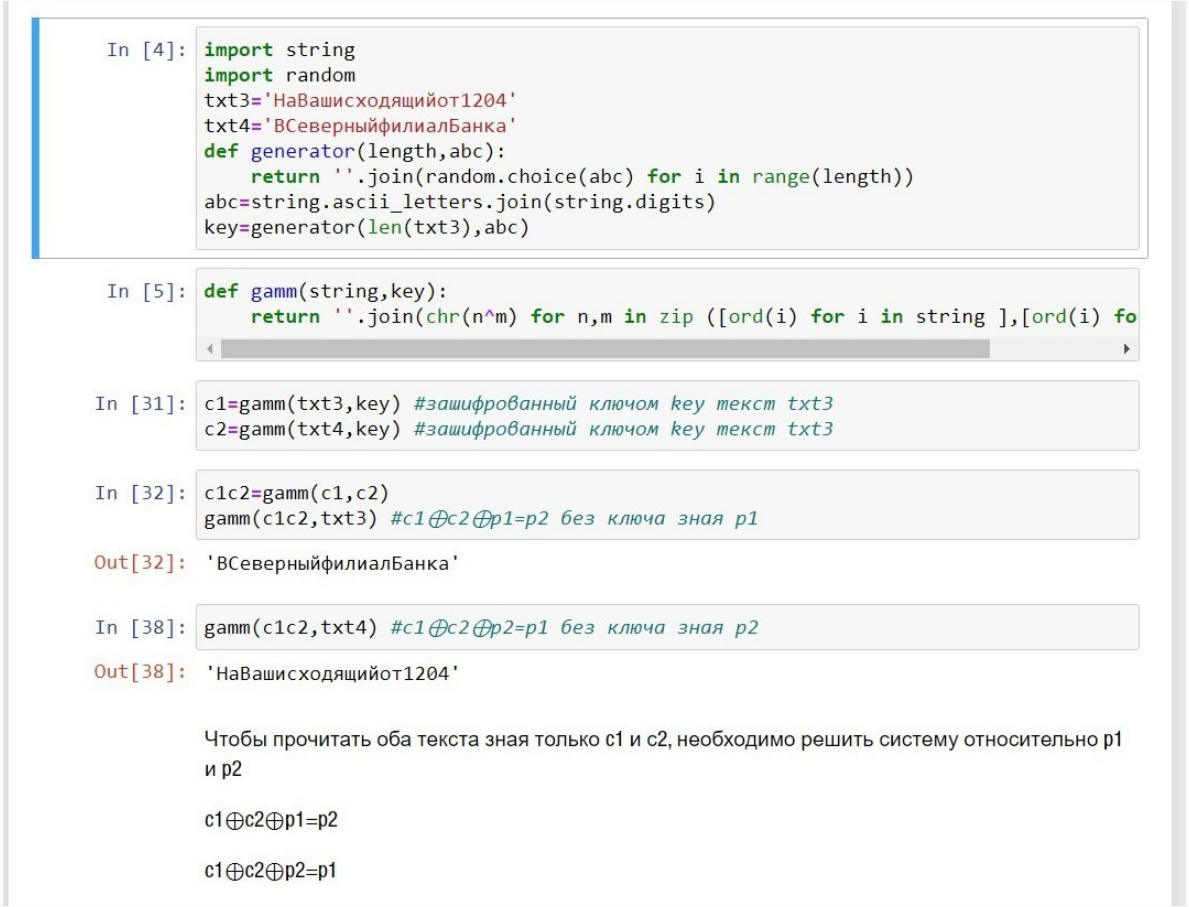
Чтобы прочитать оба текста зная только c1 и c2, необходимо решить систему относительно p1 и p2

$c1 \oplus c2 \oplus p1 = p2$

$c1 \oplus c2 \oplus p2 = p1$

Figure 3: рис.3. Функции.

4. Расшифруем каждую строку зная другую.



```
In [4]:
import string
import random
txt3='НаВашисходящийот1204'
txt4='ВСеверныйфилиалБанка'
def generator(length,abc):
    return ''.join(random.choice(abc) for i in range(length))
abc=string.ascii_letters.join(string.digits)
key=generator(len(txt3),abc)

In [5]:
def gamm(string,key):
    return ''.join(chr(n^m) for n,m in zip ([ord(i) for i in string ],[ord(i) fo

In [31]:
c1=gamm(txt3,key) #зашифрованный ключом key текст txt3
c2=gamm(txt4,key) #зашифрованный ключом key текст txt3

In [32]:
c1c2=gamm(c1,c2)
gamm(c1c2,txt3) #c1⊕c2⊕p1=p2 без ключа зная p1

Out[32]:
'ВСеверныйфилиалБанка'

In [38]:
gamm(c1c2,txt4) #c1⊕c2⊕p2=p1 без ключа зная p2

Out[38]:
'НаВашисходящийот1204'
```

Чтобы прочитать оба текста зная только c1 и c2, необходимо решить систему относительно p1 и p2

$c1 \oplus c2 \oplus p1 = p2$

$c1 \oplus c2 \oplus p2 = p1$

Figure 4: рис.4. Расшивровка.

Спасибо за внимание