Отчет по лабораторной работе 8

Радимов Игорь

Содержание

List of Tables

List of Figures

1 Цель работы

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

2 Задание

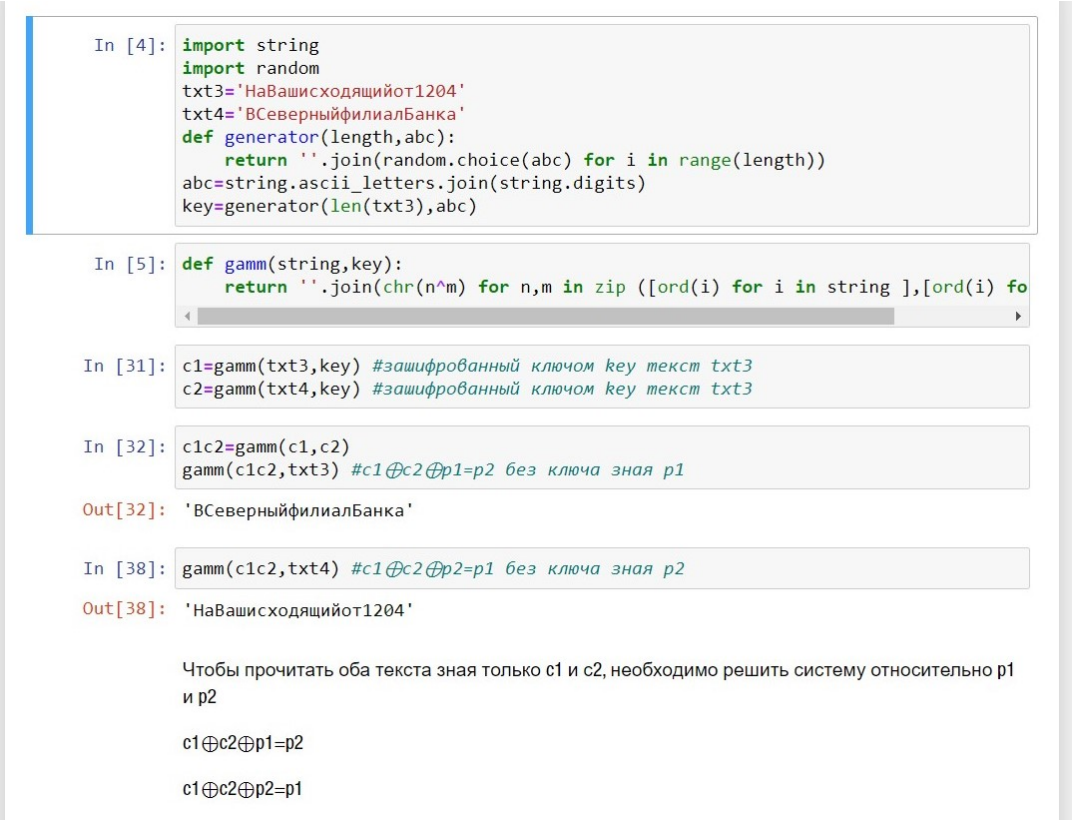
Лабораторная работа подразумевает использование языков программирования для создания программы для щифрования и дещифрования в режиме однократного гаммирования при известном ключе.

3 Теория

Гаммирование, или Шифр XOR, — метод симметричного шифрования, заключающийся в «наложении» последовательности, состоящей из случайных чисел, на открытый текст. Последовательность случайных чисел называется гамма-последовательностью и используется для зашифровывания и расшифровывания данных.

4 Выполнение работы

1. Разработаем приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования и расшифруем два текста, зная только один из них и не зная ключа.(рис 1-2)



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 4.1: рис.1. Программа, часть 1.

5 Библиография

1. ТУИС РУДН

2. Статья на сайте “https://ru.wikipedia.org/wiki/%D0%93%D0%B0%D0%BC%D0%BC%D0%B8

6 Выводы

Во время выполнения лабораторной работы я освоил на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.