

# **Лабораторная работа №8**

**Основы информационной безопасности**

Колчева Юлия Вячеславовна

# Содержание

1	Цель работы	5
2	Теоритическое введение	6
3	Выполнение лабораторной работы	7
4	Выводы	9
5	Список литературы	10

## Список иллюстраций

3.1	Код программы . . . . .	7
3.2	Результат работы . . . . .	8
3.3	“Взлом” текстов . . . . .	8
3.4	“Взлом” текстов . . . . .	8

## Список таблиц

# 1 Цель работы

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

## 2 Теоритическое введение

Гаммирование - наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных.

Основная формула, необходимая для реализации однократного гаммирования:  $C_i = P_i \text{ XOR } K_i$ , где  $C_i$  -  $i$ -й символ зашифрованного текста,  $P_i$  -  $i$ -й символ открытого текста,  $K_i$  -  $i$ -й символ ключа.

В данном случае для двух шифротекстов будет две формулы:

$$C1 = P1 \text{ xor } K \text{ и } C2 = P2 \text{ xor } K,$$

где индексы обозначают первый и второй шифротексты соответственно.

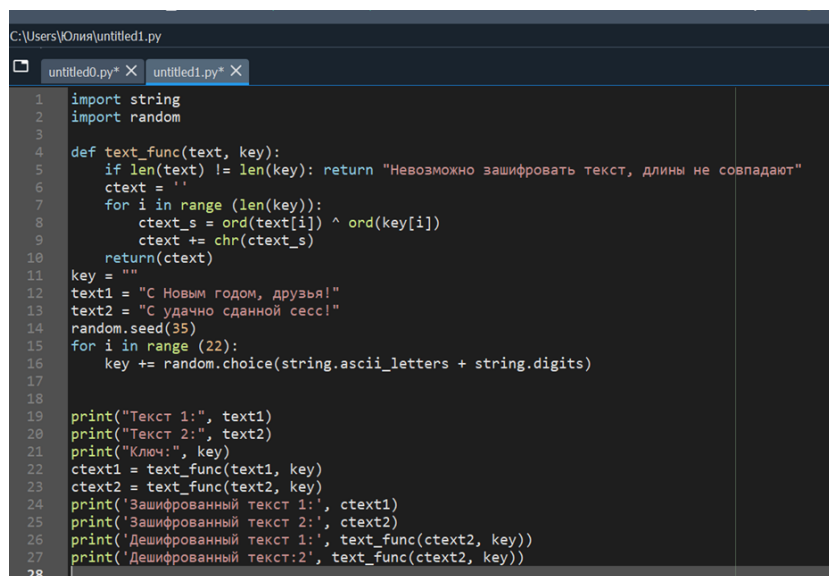
Если нам известны оба шифротекста и один открытый текст, то мы можем найти другой открытый текст, это следует из следующих формул:

$$C1 \text{ xor } C2 = P1 \text{ xor } K \text{ xor } P2 \text{ xor } K = P1 \text{ xor } P2,$$

$$C1 \text{ xor } C2 \text{ xor } P1 = P1 \text{ xor } P2 \text{ xor } P1 = P2.$$

### 3 Выполнение лабораторной работы

Код программы для выполнения задания.(рис. [3.2])



```
1 import string
2 import random
3
4 def text_func(text, key):
5     if len(text) != len(key): return "Невозможно зашифровать текст, длины не совпадают"
6     ctext = ''
7     for i in range (len(key)):
8         ctext_s = ord(text[i]) ^ ord(key[i])
9         ctext += chr(ctext_s)
10    return(ctext)
11
12 key = ""
13 text1 = "С Новым годом, друзья!"
14 text2 = "С удачно сданной сесс!"
15 random.seed(35)
16 for i in range (22):
17     key += random.choice(string.ascii_letters + string.digits)
18
19 print("Текст 1:", text1)
20 print("Текст 2:", text2)
21 print("Ключ:", key)
22 ctext1 = text_func(text1, key)
23 ctext2 = text_func(text2, key)
24 print('Зашифрованный текст 1:', ctext1)
25 print('Зашифрованный текст 2:', ctext2)
26 print('Дешифрованный текст 1:', text_func(ctext2, key))
27 print('Дешифрованный текст:2', text_func(ctext2, key))
28
```

Рис. 3.1: Код программы

1-2 строки: импорт необходимых библиотек

4-10 строки: функция, реализующая сложение по модулю два двух строк

12-13: открытые/исходные тексты

15-16: создание ключа той же длины, что и открытый текст

22-23: получение шифротекстов с помощью функции, созданной ранее, при условии, что известны открытые тексты и ключ

26-27: получение открытых текстов с помощью функции, созданной ранее, при условии, что известны шифротексты и ключ

Результат работы программы можно увидеть на следующем скриншоте (рис. [3.3])

```
In [18]: runfile('C:/Users/Юлия/untitled1.py', wdir='C:/
Users/Юлия')
Текст 1: С Новым годом, друзья!
Текст 2: С удачно сданной сесс!
Ключ: JvWiVv3jsB9qKdVHW37ZrP
Зашифрованный текст 1: жVъїКнЦЈрЌЙяЎНџЗΨЁЖнq
Зашифрованный текст 2: жVДйАбЎеSГЙсЎьмфwӨБЛгq
Дешифрованный текст 1: С Новым годом, друзья!
Дешифрованный текст:2 С удачно сданной сесс!
```

Рис. 3.2: Результат работы

Теперь попробуем реализовать “взлом” текстов при помощи операции XOR и без использования ключа. (рис. [??])

```
31 ctext_xor = text_func(ctext1,ctext2)
32 print('XOR', ctext_xor)
33 print('2 text', text_func(ctext_xor, text1))
34 print('1 text', text_func(ctext_xor, text2))
35
```

Рис. 3.3: “Взлом” текстов

31: сложение по модулю два двух шифротекстов с помощью функции, созданной ранее.

33-34: получение открытых текстов с помощью функции, созданной ранее, при условии, что известны оба шифротекста и один из открытых текстов.

Как видно на скриншоте, при помощи текста 1 мы можем получить текст 2 и наоборот. (рис. [3.4])

```
Г  ВВО
2 text С удачно сданной сесс!
1 text С Новым годом, друзья!
```

Рис. 3.4: “Взлом” текстов



## 4 Выводы

В ходе выполнения данной лабораторной работы я освоила на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

## 5 Список литературы

Лабораторная работа №8

Однократное гаммирование [Электронный ресурс]. URL: [https://esystem.rudn.ru/pluginfile.php/1651641/mod\\_resource/content/2/008-lab\\_cryptokey.pdf](https://esystem.rudn.ru/pluginfile.php/1651641/mod_resource/content/2/008-lab_cryptokey.pdf).