

# Основы информационной безопасности

---

Колчева Юлия Вячеславовна

16 Октября 2023

РУДН, Москва, Россия

# **Лабораторная работа №8**

---

# Код программы

```
C:\Users\Юлия\untitled1.py
untitled0.py* X  untitled1.py* X

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     key = ""
12     text1 = "С Новым годом, друзья!"
13     text2 = "С удачно сданной сесс!"
14     random.seed(35)
15     for i in range (22):
16         key += random.choice(string.ascii_letters + string.digits)
17
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. 1: Код программы на Python

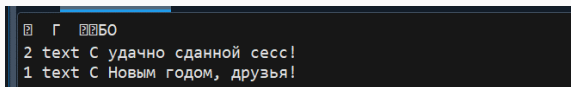
```
In [18]: runfile('C:/Users/Юлия/untitled1.py', wdir='C:/
Users/Юлия')
Текст 1: С Новым годом, друзья!
Текст 2: С удачно сданной сесс!
Ключ: JvWiVv3jsB9qKdVHW37ZrP
Зашифрованный текст 1: жVъіКєЦЈрЎЙяЎHvЎЗΨЁЖнq
Зашифрованный текст 2: жVдйАбУёSfЙсVъмψwӨБЛg
Дешифрованный текст 1: С Новым годом, друзья!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

Рис. 2: Вывод программы

```
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:** Осуществление операции XOR

# Результат “взлома”

A screenshot of a terminal window with a dark background. The prompt is a green character followed by a space, a green 'Г', a space, and '??B0'. The output consists of two lines: '2 text С удачно сданной сесс!' and '1 text С Новым годом, друзья!'.

```
?? Г ??B0  
2 text С удачно сданной сесс!  
1 text С Новым годом, друзья!
```

Рис. 4: Вывод программы

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

**Спасибо за внимание!**