

# Отчет по лабораторной работе №7

---

Перельгин Сергей Викторович

## Цель работы

---

## Цель лабораторной работы

Освоить на практике применение режима однократного гаммирования.

# **Выполнение лабораторной работы**

---

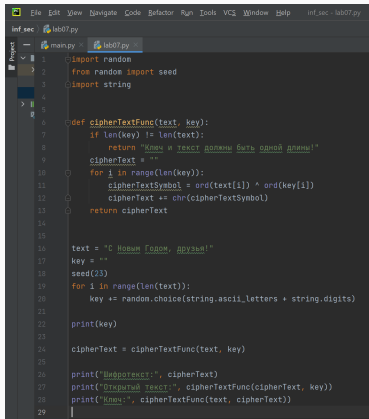
## Задачи лабораторной работы №7

1. Подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!».
2. Разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования.

Гаммирование представляет собой наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных. Иными словами, наложение гаммы — это сложение её элементов с элементами открытого (закрытого) текста по некоторому фиксированному модулю, значение которого представляет собой известную часть алгоритма шифрования.

# Функция шифрования

Создал функцию, которая осуществляет однократное гаммирование посредством побитового XOR (стр. 6-13).



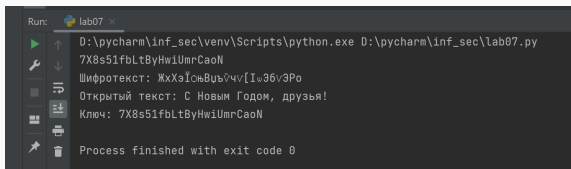
```
inf.sec | lab07.py
main.py x lab07.py
1 import random
2 from random import seed
3 import string
4
5
6 def cipherTextFunc(text, key):
7     if len(key) != len(text):
8         return "Ключ и текст должны быть одной длины!"
9     cipherText = ""
10    for i in range(len(key)):
11        cipherTextSymbol = ord(text[i]) ^ ord(key[i])
12        cipherText += chr(cipherTextSymbol)
13    return cipherText
14
15
16 text = "С Новым Годом, друзья!"
17 key = ""
18 seed(23)
19 for i in range(len(text)):
20     key += random.choice(string.ascii_letters + string.digits)
21
22 print(key)
23
24 cipherText = cipherTextFunc(text, key)
25
26 print("Шифротекст:", cipherText)
27 print("Открытый текст:", cipherTextFunc(cipherText, key))
28 print("Ключ:", cipherTextFunc(text, cipherText))
29
```

Рис. 1: Функция шифрования

Далее я создал ключ той же длины, что и открытый текст, получил шифротекст с помощью функции, созданной ранее, при условии, что известны открытый текст и ключ. После этого получил открытый текст с помощью функции, созданной ранее, при условии, что известны шифротекст и ключ. Затем я получил ключ с помощью функции, созданной ранее, при условии, что известны открытый текст и шифротекст.



# Результат работы программы



The screenshot shows a PyCharm Run console window with a dark theme. The title bar reads 'Run: lab07'. On the left is a vertical toolbar with icons for running, debugging, and other actions. The console output is as follows:

```
D:\pycharm\inf_sec\venv\Scripts\python.exe D:\pycharm\inf_sec\lab07.py
7X8s51fbLtByHwiUmrCaoN
Шифротекст: ЖхХэЇоньВцъѸчv[Iw36v3Po
Открытый текст: С Новым Годом, друзья!
Ключ: 7X8s51fbLtByHwiUmrCaoN
Process finished with exit code 0
```

**Рис. 2:** Вывод программы

## Выводы

---

В ходе выполнения данной лабораторной работы я освоил на практике применение режима однократного гаммирования.

Спасибо за внимание!