Отчёт по лабораторной работе № 8

Дисциплина: Основы информационной безопасности

Перелыгин Сергей Викторович

Содержание

# Цель работы

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

# Задание

* Сделать отчёт по лабораторной работе в формате Markdown.
* В качестве отчёта предоставить отчёты в 3 форматах: pdf, docx и md.

# Теоретическое введение

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

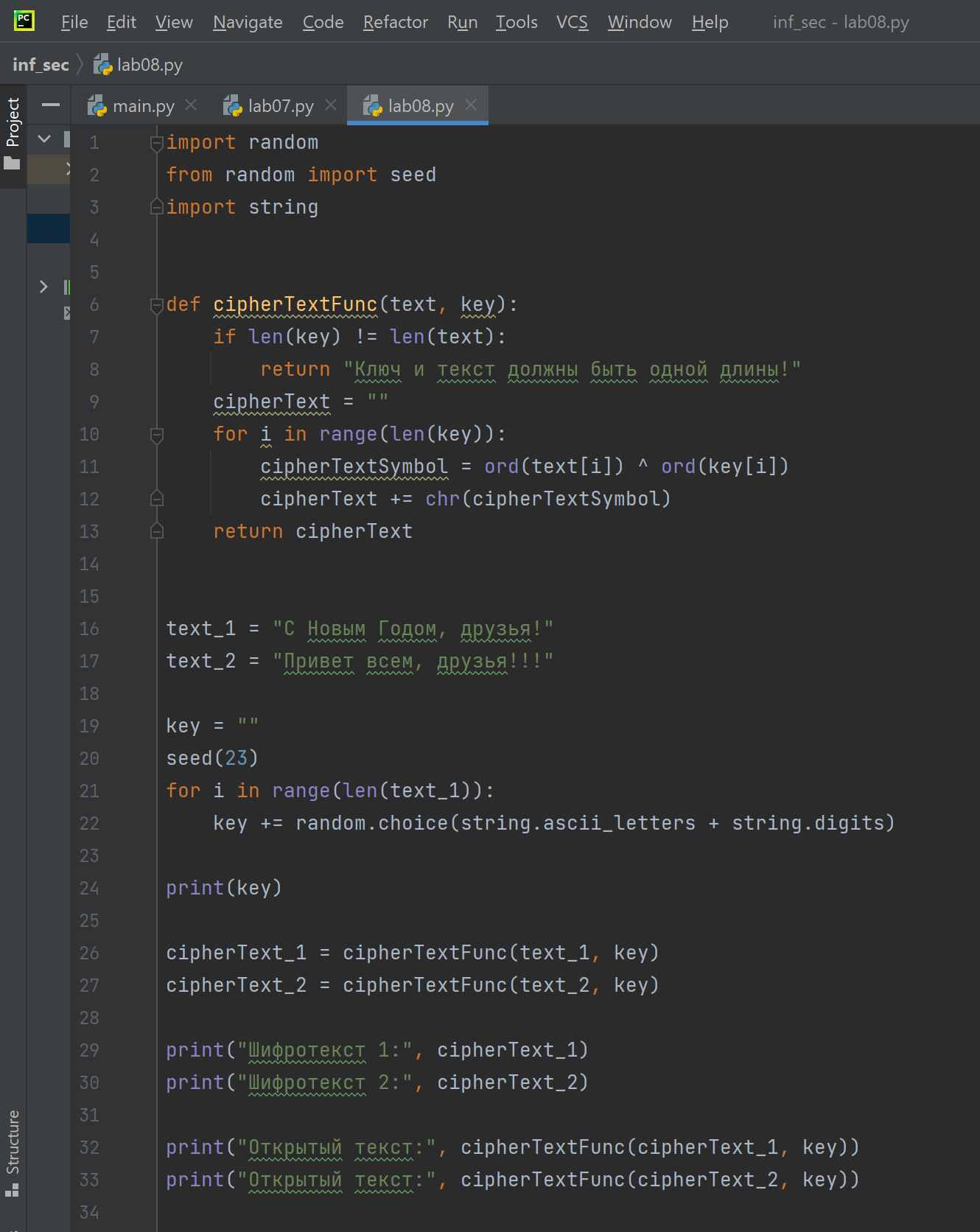
Основная формула, необходимая для реализации однократного гаммирования: Ci = Pi XOR Ki, где Ci - i-й символ зашифрованного текста, Pi - i-й символ открытого текста, Ki - i-й символ ключа.

В данном случае для двух шифротекстов будет две формулы: С1 = P1 xor K и С2 = P2 xor K, где индексы обозначают первый и второй шифротексты соответственно.

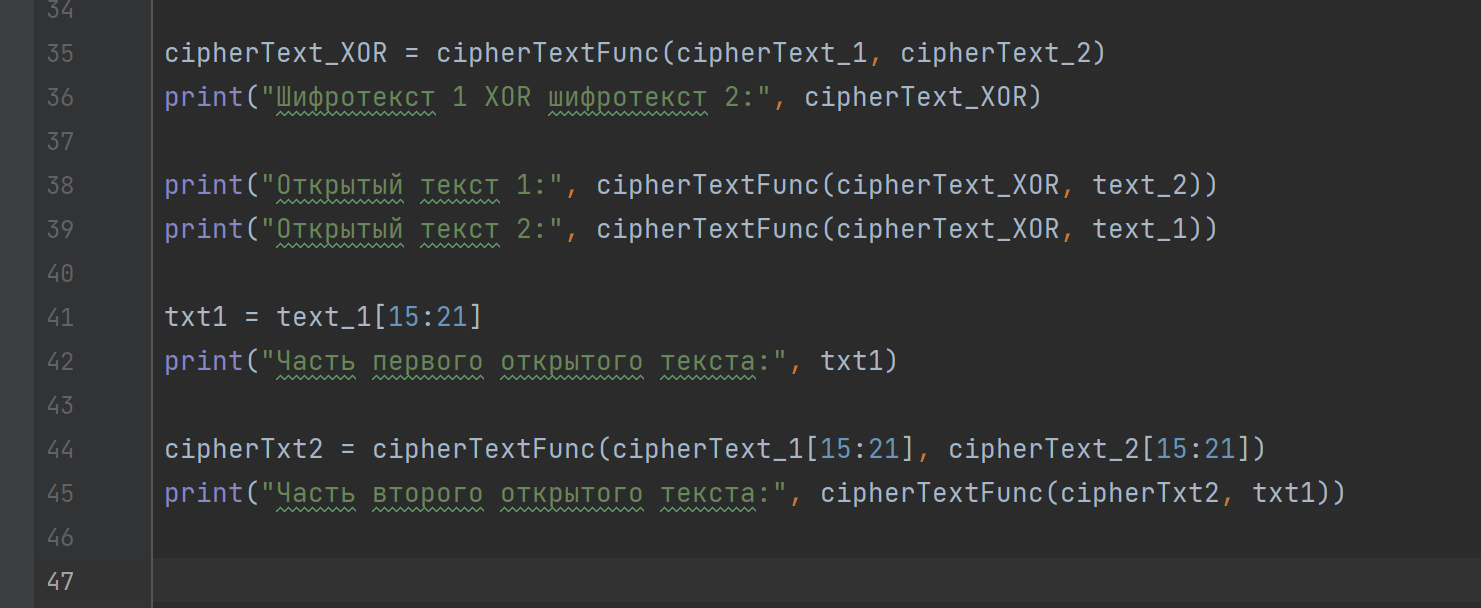
Если нам известны оба шифротекста и один открытый текст, то мы можем найти другой открытый текст, это следует из следующих формул: C1 xor C2 = P1 xor K xor P2 xor K = P1 xor P2, C1 xor C2 xor P1 = P1 xor P2 xor P1 = P2.

# Выполнение лабораторной работы

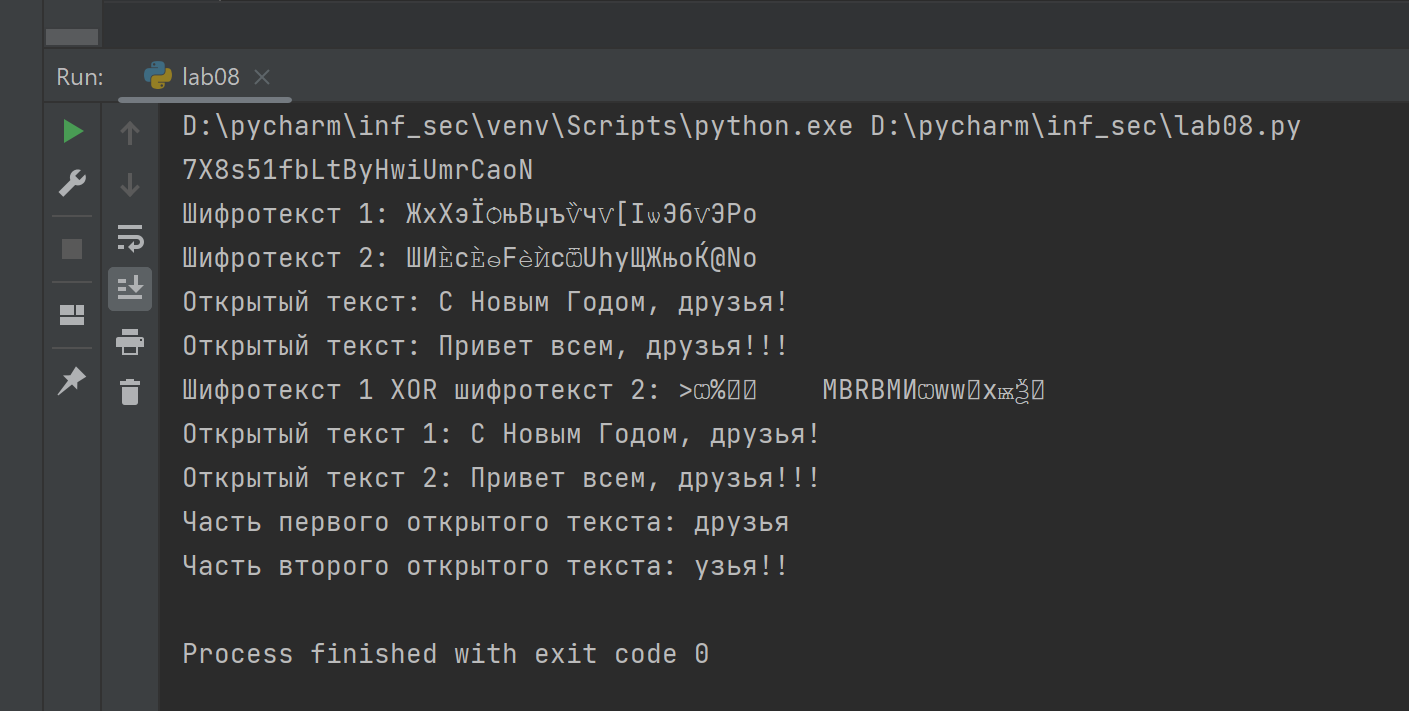
1. Код программы (рис. 4.1 и 4.2) и вывод (рис. 4.3).



Приложение, реализующее режим однократного гаммирования для двух текстов одним ключом (1)



Приложение, реализующее режим однократного гаммирования для двух текстов одним ключом (2)



Вывод программы

1. Пояснения к программе:

• Lines 1-3: импорт необходимых библиотек

• Lines 6-13: функция, реализующая сложение по модулю два двух строк

• Lines 16-17: открытые/исходные тексты (одинаковой длины)

• Lines 19-24: создание ключа той же длины, что и открытые тексты

• Lines 26-30: получение шифротекстов с помощью функции, созданной ранее, при условии, что известны открытые тексты и ключ

• Lines 32-33: получение открытых текстов с помощью функции, созданной ранее, при условии, что известны шифротексты и ключ

• Lines 35-36: сложение по модулю два двух шифротекстов с помощию функции, созданной ранее

• Lines 38-39: получение открытых текстов с помощью функции, созданной ранее, при условии, что известны оба шифротекста и один из открытых текстов

• Lines 41-42: получение части первого открытого текста (срез)

• Lines 44-45: получение части второго текста (на тех позициях, на которых расположены символы части первого открытого текста) с помощью функции, созданной ранее, при условии, что известны оба шифротекста и часть первого открытого текста

# Выводы

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

# Библиография

* Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через Internet. — НПО “Мир и семья-95”, 1997. — URL: http://bugtraq.ru/library/books/attack1/index.html
* Медведовский И.Д., Семьянов П.В., Леонов Д.Г. Атака на Internet. — Издательство ДМК, 1999. — URL: http://bugtraq.ru/library/books/attack/index.html
* Запечников С. В. и др. Информационн~пасность открытых систем. Том 1. — М.: Горячаая линия -Телеком, 2006.
* Введение в информационную безопасность. Типы уязвимостей. (Д.Гамаюнов, МГУ)
* Практические аспекты сетевой безопасности. Вводная лекция. Сетевая безопасность. Стек протоколов TCP/IP. (Д. Гамаюнов, МГУ)
* Практические аспекты сетевой безопасности. Сетевая безопасность. Межсетевые экраны. (В. Иванов, МГУ)
* Практические аспекты сетевой безопасности. Сетевая безопасность. Системы обнаружения и фильтрации компьютерных атак (IDS/IPS). (Д. Гамаюнов, МГУ)
* Практические аспекты сетевой безопасности. Контроль нормального поведения приложений. Security Enhanced Linux (SELinux) (В. Сахаров, МГУ)