Отчёт по лабораторной работе № 7

Дисциплина: Основы информационной безопасности

Перелыгин Сергей Викторович

Содержание

# Цель работы

Освоить на практике применение режима однократного гаммирования.

# 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) данны 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.

Аналогичным образом можно найти ключ: Ki = Ci XOR Pi. Необходимые и достаточные условия абсолютной стойкости шифра:

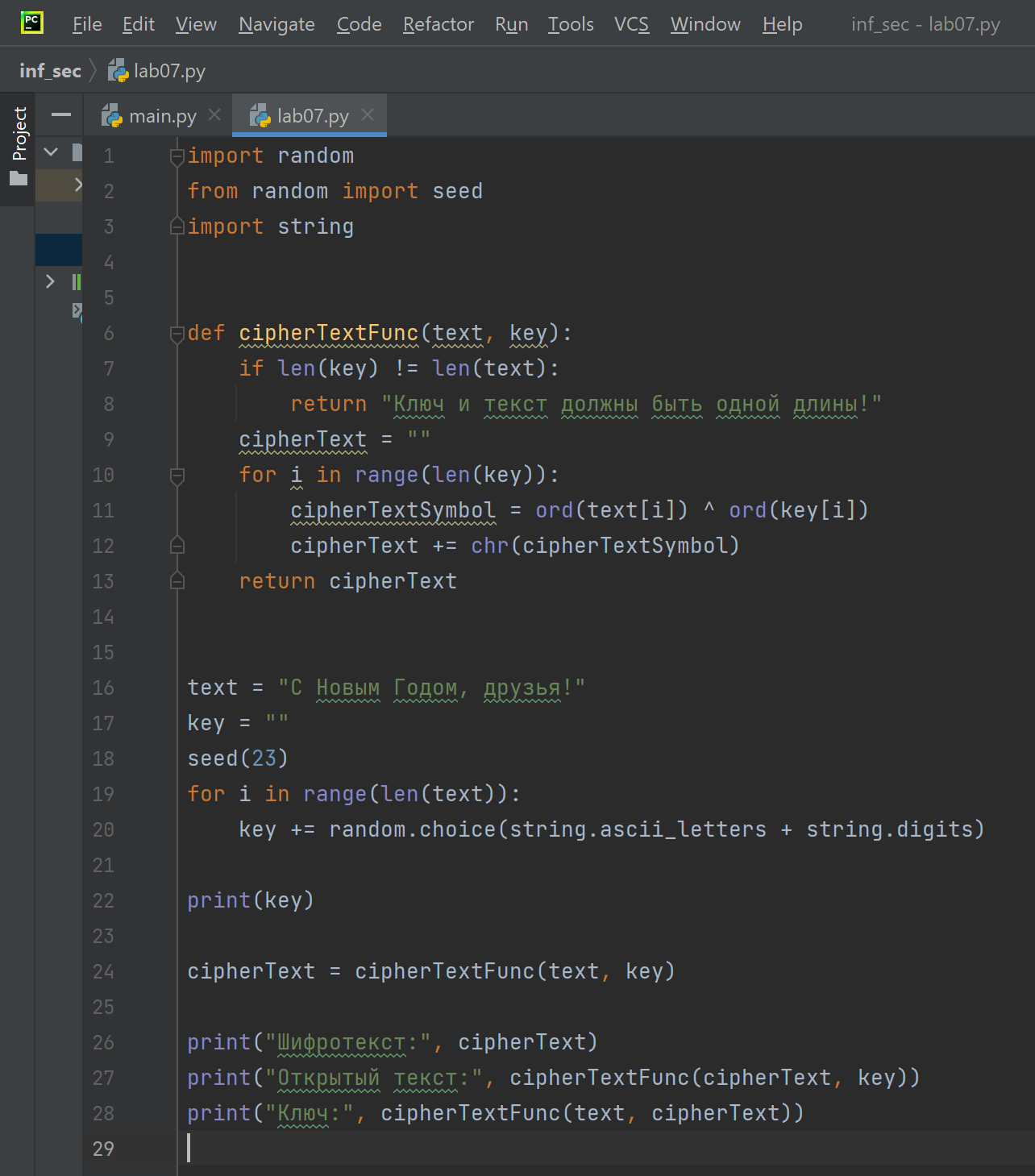
• длина открытого текста равна длине ключа

• ключ должен использоваться однократно

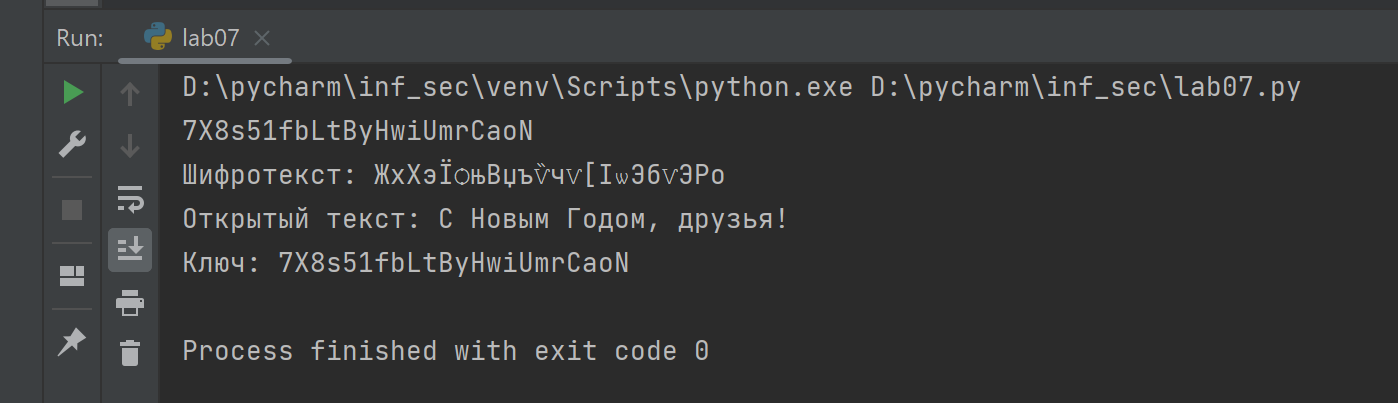
• ключ должен быть полностью случаен

# Выполнение лабораторной работы

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



Приложение, реализующее режим однократного гаммирования



Вывод программы

1. Пояснения к программе:

• Lines 1-3: импорт необходимых библиотек

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

• Line 16: открытый/исходный текст

• Lines 17-22: создание ключа той же длины, что и открытый текст

• Lines 24-26: получение шифротекста с помощию функции, созданной ранее, при условии, что известны открытый текст и ключ

• Line 27: получение открытого текста с помощью функции, созданной ранее, при условии, что известны шифротекст и ключ

• Line 28: получение ключа с помощью функции, созданной ранее, при условии, что известны открытый текст и шифротекст

# Выводы

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

# 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)