Лабораторная работа №7

Основы информационной безопасности

Колчева Юлия Вячеславовна

Содержание

# 1 Цель работы

Освоить на практике применение режима однократного гаммирования.

# 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:

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:

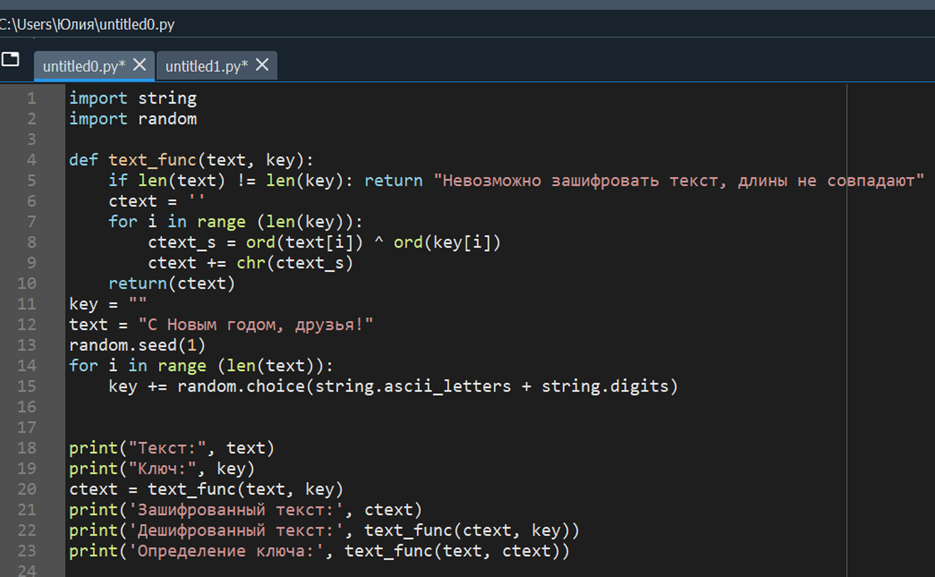
• длина открытого текста равна длине ключа

• ключ должен использоваться однократно

• ключ должен быть полностью случаен

# 3 Выполнение лабораторной работы

В ходе выполнения данной лабораторной работы я освоила на практике применение режима однократного гаммирования.(рис. [??])



Код программы

1-2 строки: импорт необходимых библиотек

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

12: строка открытый/исходный текст

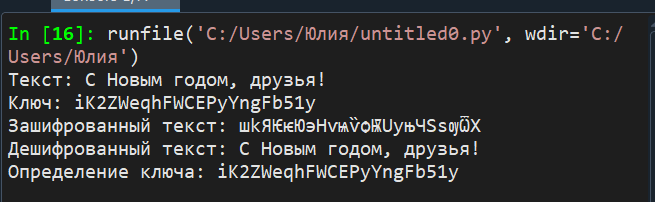
14-15: создание ключа той же длины, что и открытый текст

20: получение шифротекста с помощию функции, созданной ранее, при условии, что известны открытый текст и ключ

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

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

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



Результат работы

# 4 Выводы

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

# 5 Список литературы

Лабораторная работа №7

Однократное гаммирование [Электронный ресурс]. URL: https://esystem. rudn.ru/pluginfile.php/1651639/mod\_resource/content/2/007-lab\_cryptogamma.pdf.