Лабораторная работа №8

Основы информационной безопасности

Колчева Юлия Вячеславовна

Содержание

# 1 Цель работы

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

# 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.

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.

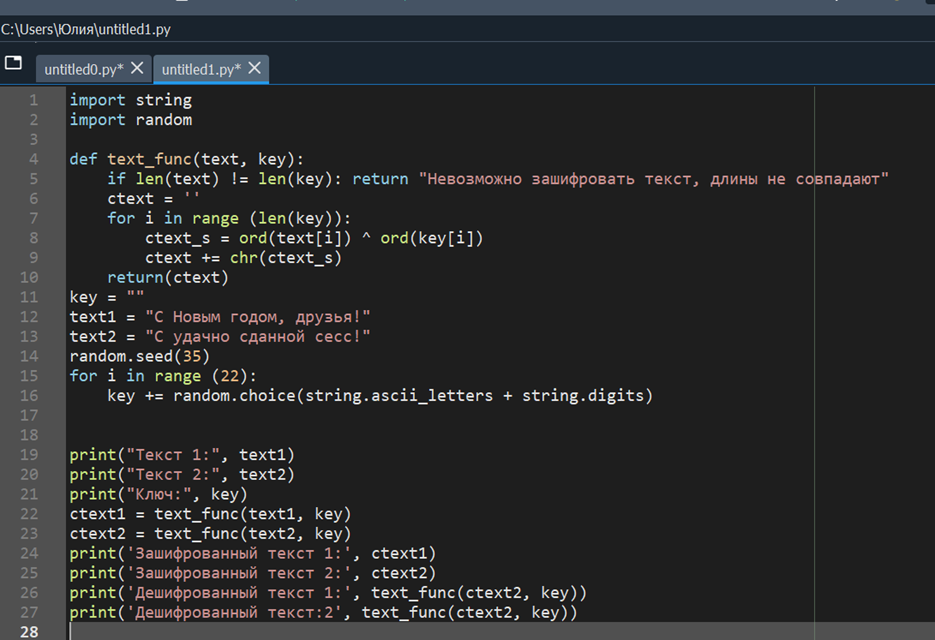
Если нам известны оба шифротекста и один открытый текст, то мы можем найти другой открытый текст, это следует из следующих формул:

C1 xor C2 = P1 xor K xor P2 xor K = P1 xor P2,

C1 xor C2 xor P1 = P1 xor P2 xor P1 = P2.

# 3 Выполнение лабораторной работы

Код программы для выполнения задания.(рис. [??])



Код программы

1-2 строки: импорт необходимых библиотек

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

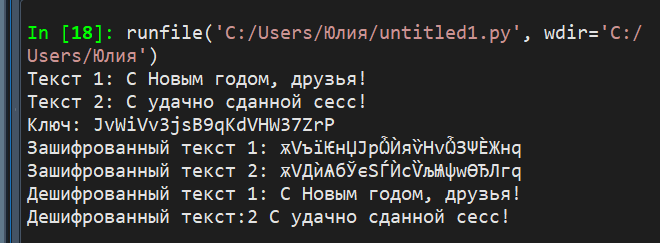
12-13: открытые/исходные тексты

15-16: создание ключа той же длины, что и открытый текст

22-23: получение шифротекстов с помощью функции, созданной ранее, при условии, что известны открытые тексты и ключ

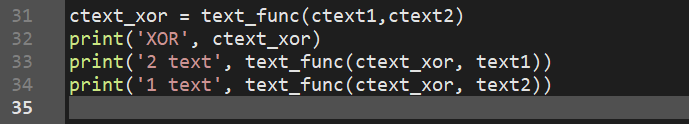
26-27: получение открытых текстов с помощью функции, созданной ранее, при условии, что известны шифротексты и ключ

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



Результат работы

Теперь попробуем реализовать “взлом” текстов при помощи операции XOR и без использования ключа. (рис. [??])

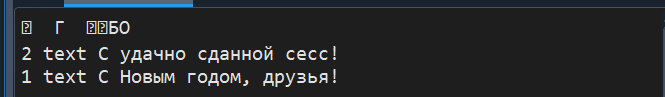


“Взлом” текстов

31: сложение по модулю два двух шифротекстов с помощию функции, созданной ранее.

33-34: получение открытых текстов с помощью функции, созданной ранее, при условии, что известны оба шифротекста и один из открытых текстов.

Как видно на скриншоте, при помощи текста 1 мы можем получить текст 2 и наоборот. (рис. [??])



“Взлом” текстов

# 4 Выводы

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

# 5 Список литературы

Лабораторная работа №8

Однократное гаммирование [Электронный ресурс]. URL: https://esystem. rudn.ru/pluginfile.php/1651641/mod\_resource/content/2/008-lab\_cryptokey.pdf.