Лабораторная работа №8

Основы информационной безопасности

Кондрашова Анастасия Андреевна

Содержание

# 1 Теоретческое введение

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.

В соответствии с теорией криптоанализа, если в методе шифрования используется однократная вероятностная гамма (однократное гаммирование) той же длины, что и подлежащий сокрытию текст, то текст нельзя раскрыть. Даже при раскрытии части последовательности гаммы нельзя получить информацию о всём скрываемом тексте. Наложение гаммы по сути представляет собой выполнение операции сложения по модулю 2 (XOR) (обозначаемая знаком ⊕) между элементами гаммы и элементами подлежащего сокрытию текста.

# 2 Цель работы

Освоить на практике применение однократного гаммирования при работе с различными текстами на одном ключе.

# 3 Выполнение лабораторной работы

Лабораторная работа выполнена на языке Python 3 в среде Jupiter Notebook.

1. Cоздаём функцию, которая осуществляет однократное гаммирование посредством побитового XOR

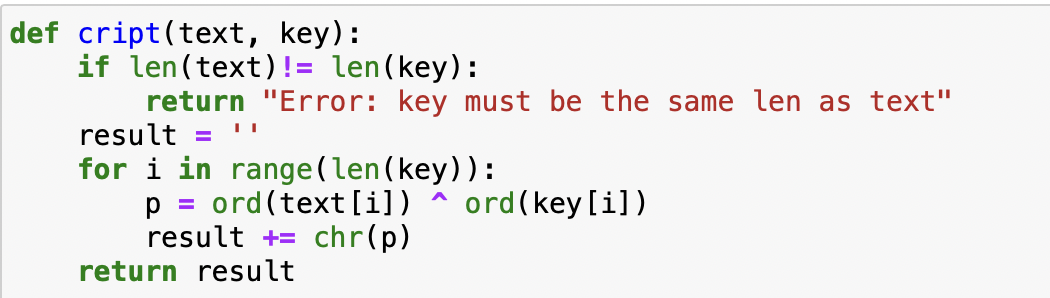


Рис. 1: Функция шифрования

1. Задаём две равные по длине текстовые строки и создаём случайный символьный ключ такой же длины

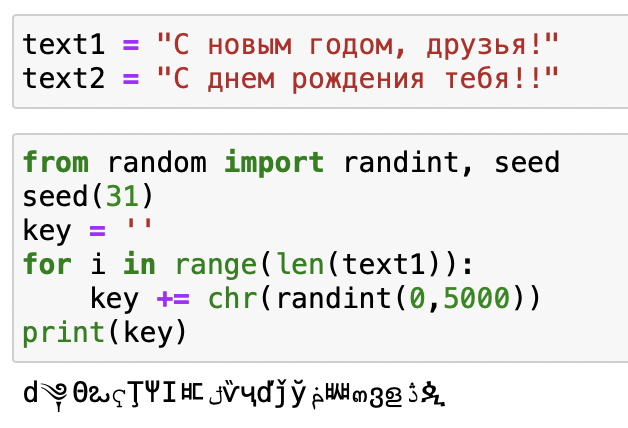


Рис. 2: Исходные данные

1. Осуществляем шифрование двух текстов по ключу с помощью написанной функции

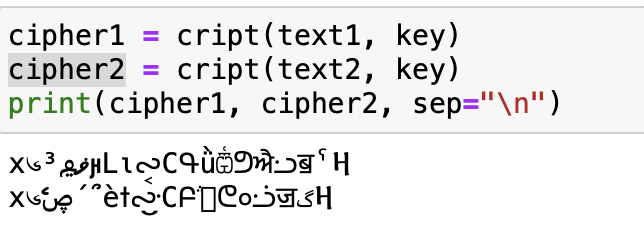


Рис. 3: Шифрование данных

1. Создаём переменную, которая, прогнав два шифрованных текста через побитовый XOR, поможет злоумышленнику получить один текст, зная другой, без ключа

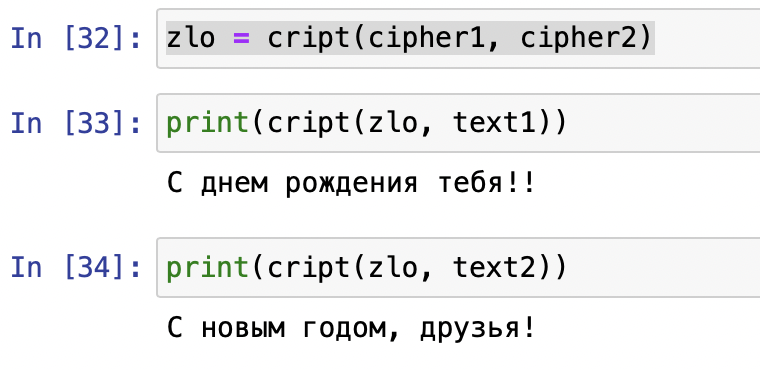


Рис. 4: Получение данных без ключа

1. Таким же способом можно получить часть данных

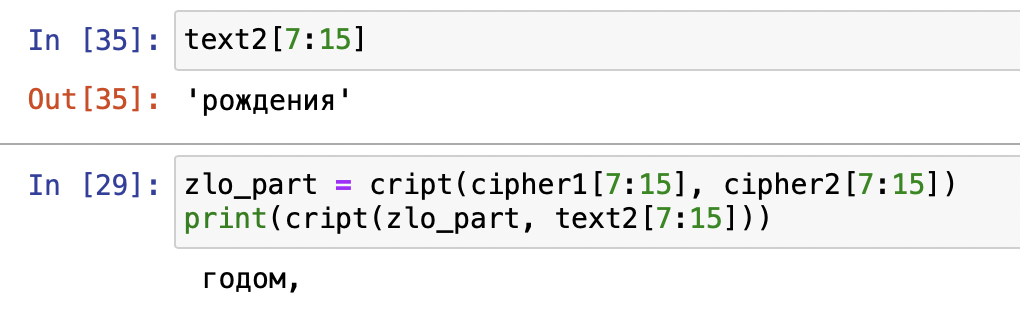


Рис. 5: Получение части данных

# 4 Выводы

Я освоила на практике применение режима однократного гаммирования при работе с несколькими текстами.