Лабораторная работа №8

Информационная безопасность

Банникова Екатерина Алексеевна

Содержание

# 1 Цель работы

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

# 2 Теоретическое введение

# 3 Выполнение лабораторной работы

Создаем функцию, которая осуществляет однократное гаммирование посредством побитового XOR

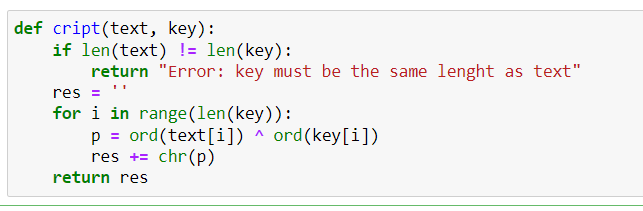


Рис. 1: Функция шифрования

Задаем две равные по длине текстовые строки и создаем случайный символьный ключ такой же длины

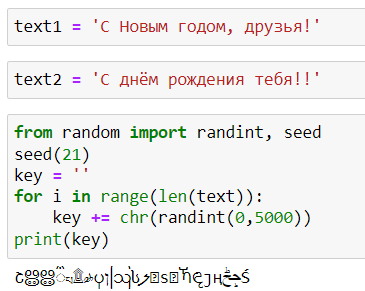


Рис. 2: Исходные данные

Осуществляем шифрование двух текстов по ключу с помощью написанной функции

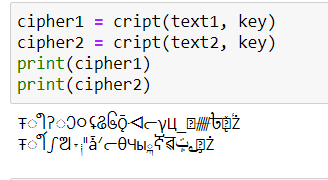


Рис. 3: Шифрование данных

Создаем переменную, которая, прогнав два шифрованных текста через побитый XOR, поможет злоумышлинику получить один текс, зная другой, без ключа

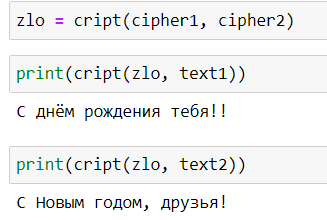


Рис. 4: Получение данных без ключа

Таким же способом можно получить часть данных

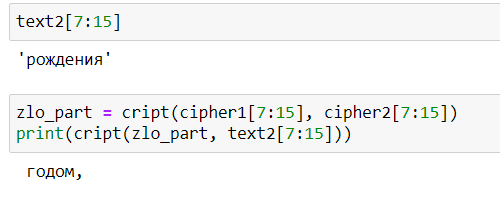


Рис. 5: Получение части данных

# 4 Выводы

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