Лабораторная работа №7

Информационная безопасность

Банникова Екатерина Алексеевна

Содержание

# 1 Цель работы

Освоить основы шифрования через однократное гаммирование

# 2 Теоретическое введение

# 3 Выполнение лабораторной работы

Лабораторная выполнена на языке Python 3 в среде Jupiter Notebook. Создаем функцию, которая осуществляет однократное гаммирование посредством побитового XOR

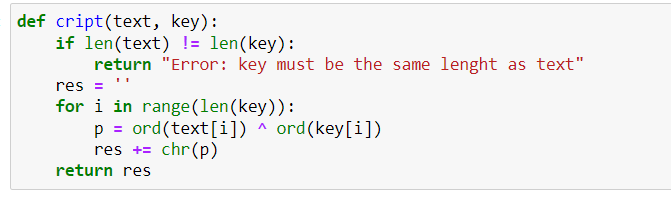


Рис. 1: Функция шифрования

Задаем текстовую строку и создаем случайный символьный ключ такой длины

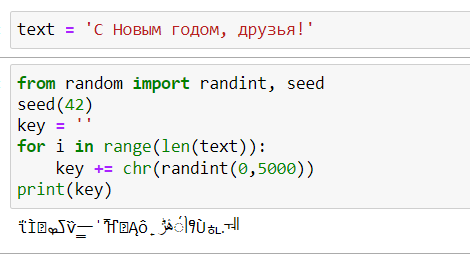


Рис. 2: Исходные данные

Запускаем функцию. В первом случае получаем зашифрованный текст. Используя тот же ключ, осуществляем дешифровку текста. Зная оригинальный текст и его шифровку, может получить ключ. Все эти действия осуществляются через одну и ту же функцию

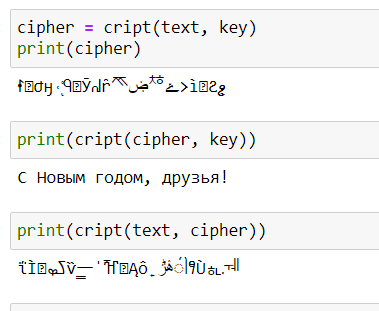


Рис. 3: Результат работы программы

# 4 Выводы

Я освоила на практике применение режима однократного гаммирования.