Отчёт по лабораторной работе №8

Дисциплина: Основы информационной безопасности

Балакирева Дарья Сергеевна, НПМбд-01-19б

Содержание

# 1 Цель работы

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

# 2 Теоретическое 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.

# 3 Выполнение лабораторной работы

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

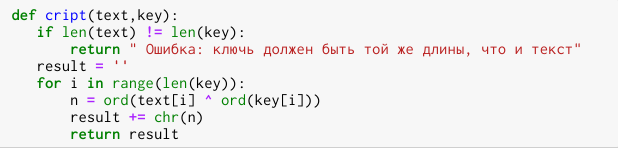


Рис. 1: Функция шифрования

Задаём две равные по длине текстовые строки и создаём случайный символьный ключ такой же длины (рис. 2)

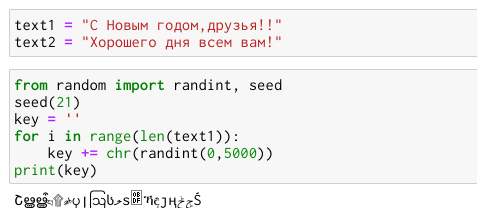


Рис. 2: Исходные данные

Осуществляем шифрование двух текстов по ключу с помощью написанной функции (рис. 3)

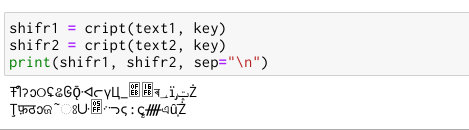


Рис. 3: Шифрование данных

Создаём переменную, которая, прогнав два шифрованных текста через побитовый XOR, поможет злоумышленнику получить один текст, зная другой, без ключа (рис. 4)

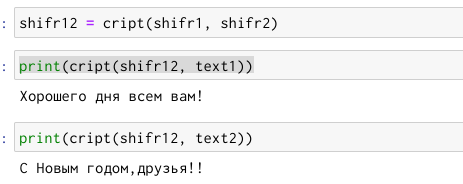


Рис. 4: Получение данных без ключа

Таким же способом можно получить часть данных (рис. 5)



Рис. 5: Получение части данных

# 4 Выводы

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

# Список литературы