Отчёт по лабораторной работе № 7

Информационная безопасность

Надиа Эззакат

Содержание

## Цель работы

Освоить на практике применение режима однократного гаммирования.

## Теоретическое 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. Аналогичным образом можно найти ключ: Ki = Ci XOR Pi. Необходимые и достаточные условия абсолютной стойкости шифра: • длина открытого текста равна длине ключа • ключ должен использоваться однократно • ключ должен быть полностью случаен

## Выполнение лабораторной работы

Код программы(рис. 7.1).

Приложение, реализующее режим однократного гаммирования

• In[1]: импорт необходимых библиотек • In[14]: функция, реализующая сложение по модулю два двух строк • In[15]: открытый/исходный текст • In[16]: создание ключа той же длины, что и открытый текст • In[17]: получение шифротекста с помощию функции, созданной ранее, при условии, что известны открытый текст и ключ • In[18]: получение открытого текста с помощью функции, созданной ранее, при условии, что известны шифротекст и ключ • In[19]: получение ключа с помощью функции, созданной ранее, при условии, что известны открытый текст и шифротекст

## Выводы

В ходе выполнения данной лабораторной работы я освоила на практике применение режима однократного гаммирования.

# Список литературы

Однократное гаммирование [Электронный ресурс]. URL: https://esystem. rudn.ru/pluginfile.php/1651639/mod\_resource/content/2/007-lab\_cryptogamma.pdf.