Лабораторная работа №7

Информационная безопасность

Леонтьева Ксения Андреевна | НПМбд-01-19

Содержание

# 1 Цель работы

Освоить на практике применение режима однократного гаммирования.

# 2 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

Более подробно см. в [1].

# 3 Выполнение лабораторной работы

Код программы (рис. 1).



Рис. 1: Приложение, реализующее режим однократного гаммирования

* In[21]: импорт необходимых библиотек
* In[22]: функция, реализующая сложение по модулю два двух строк
* In[23]: открытый/исходный текст
* In[24]: создание ключа той же длины, что и открытый текст
* In[25]: получение шифротекста с помощию функции, созданной ранее, при условии, что известны открытый текст и ключ
* In[26]: получение открытого текста с помощью функции, созданной ранее, при условии, что известны шифротекст и ключ
* In[27]: получение ключа с помощью функции, созданной ранее, при условии, что известны открытый текст и шифротекст

# 4 Выводы

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

# Список литературы

1. Однократное гаммирование [Электронный ресурс]. URL: <https://esystem.rudn.ru/pluginfile.php/1651639/mod_resource/content/2/007-lab_crypto-gamma.pdf>.