Лабораторная работа №7

Дисциплина: Основы информационной безопасности

Георгес Гедеон

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

Более подробно см. в [1].

# Выполнение лабораторной работы

1)Код программы(Рисунок 3.1).



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

# Выводы

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