Лабораторная работа №7

Информационная безопасность

Маметкадыров Ынтымак | НПМбд-02-20

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 [@Gamma:bash].

# Выполнение лабораторной работы

Код программы (рис. [-@fig:001]).



Приложение, реализующее режим однократного гаммирования

* In[1]: импорт необходимых библиотек
* In[3]: функция, реализующая сложение по модулю два двух строк
* In[4]: открытый/исходный текст
* In[5]: создание ключа той же длины, что и открытый текст
* In[6]: получение шифротекста с помощию функции, созданной ранее, при условии, что известны открытый текст и ключ
* In[7]: получение открытого текста с помощью функции, созданной ранее, при условии, что известны шифротекст и ключ
* In[8]: получение ключа с помощью функции, созданной ранее, при условии, что известны открытый текст и шифротекст

# Выводы

В ходе выполнения данной лабораторной работы мы освоили на практике применение режима однократного гаммирования.

# Список литературы