Отчёт по лабораторной работе №7

Георгес Гедеон

19 Октября 2024

# Отчет по лабораторной работе №7

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].

Код программы.



Рисунок 1

## Выводы

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