Информационная безопасность. Отчет по лабораторной работе №7

Элементы криптографии. Однократное гаммирование

Серенко Данил Сергеевич

Содержание

# Цель работы

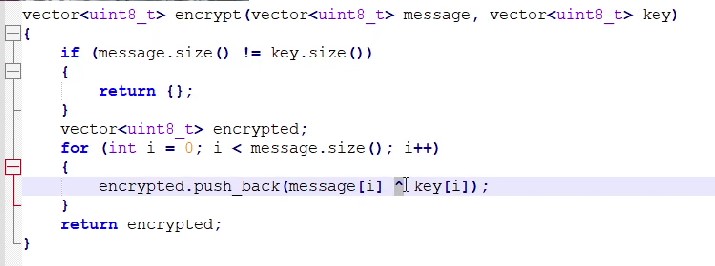
Освоить на практике применение режима однократного гаммирования.

# Выполнение лабораторной работы

Требуется разработать приложение позволяющие шифровать и дешифровать данные в режиме однократного гаммирования. Приложение должно:

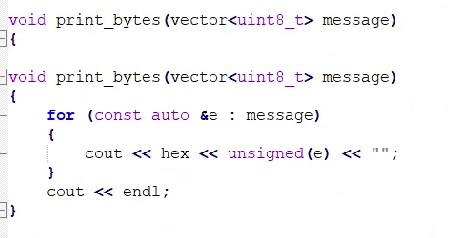
1. Определить вид шифротекста при известном ключе и известном открытом тексте.
2. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

Для этого у меня есть функция позволяющая зашифровывать, расшифровывать данные с помощью сообщения и ключа. А также позволяющая получить ключ.



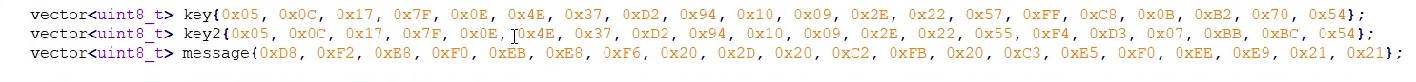
encrypt\_fuction

Функция для вывода результатов



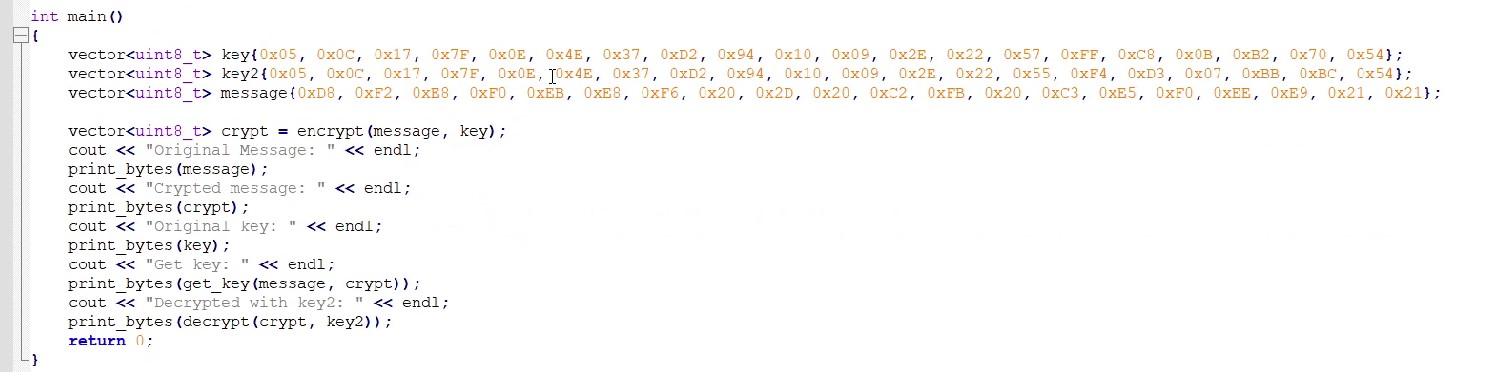
output\_prog

Биты сообщения и ключей.



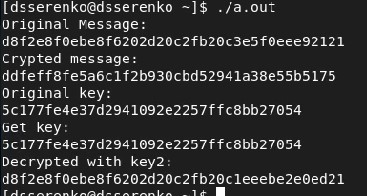
bytes

Главная функция



Main

Затем я запускаю программу и сравниваю полученные результаты с тем, что должен был получить в методичке. Видно, что все ключи и закодированные и раскодированные сообщения сошлись



console\_output

# Выводы

В результате выполнения работы я освоил на практике применение режима однократного гаммирования.

# Список литературы

1. Методические материалы курса