Информационная безопасность. Отчет по лабораторной работе №7

Элементы криптографии. Однократное гаммирование

Терентьев Егор Дмитриевич 1032192875

Содержание

# 1 Цель работы

Освоить на практике применение режима однократного гаммирования.

# 2 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 данные с помощью сообщения и ключа fig. 1.

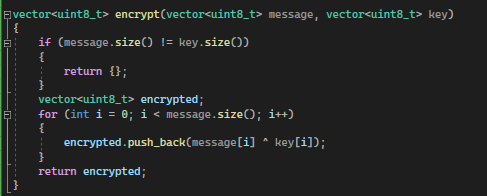


Figure 1: encrypt\_fuction

Далее я создал функцию для того, чтобы расщифровывать сообщения с помощью сообщения и ключа fig. 2.

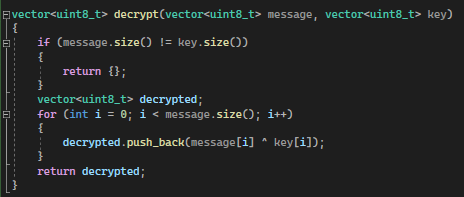


Figure 2: decrypt\_func

Затем создал функцию получения ключа fig. 3.

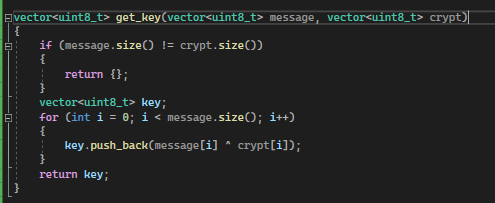


Figure 3: get\_key

Остальное в программе отвечает за вывод полученных результатов fig. 4

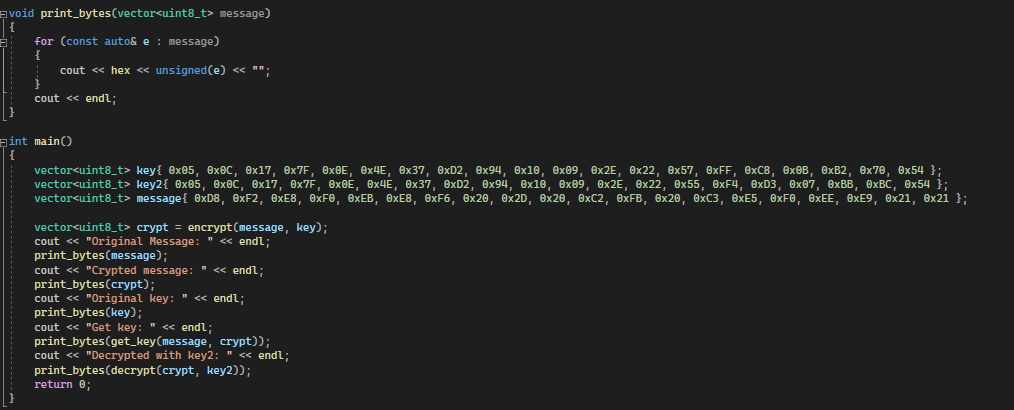


Figure 4: output\_prog

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 fig. 5

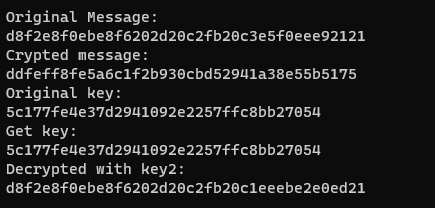


Figure 5: console\_output

# 3 Выводы

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

# 4 Список литературы

1. Методические материалы курса