Информационная безопасность. Отчет по лабораторной работе №8

Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Терентьев Егор Дмитриевич 1032192875

Содержание

# 1 Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

# 2 Выполнение лабораторной работы

Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе.

Для этого у меня есть функция позволяющая зашифровывать данные с помощью сообщения и ключа fig. 1.

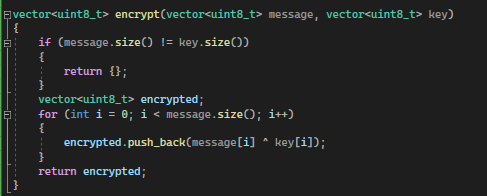


Figure 1: encrypt\_fuction

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

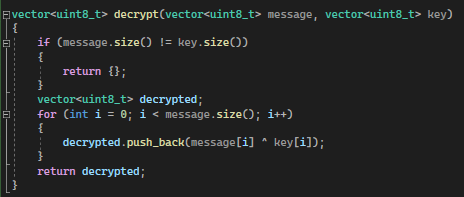


Figure 2: decrypt\_func

Затем создал функцию получения ключа fig. 3.

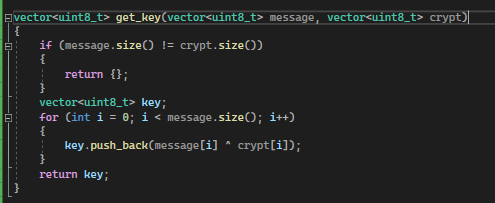


Figure 3: get\_key

Создал функцию получения расшифрованного сообщения без ключа fig. 4

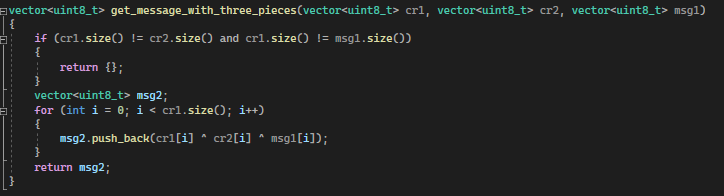


Figure 4: decrypt\_without\_key

Остальное в программе отвечает за вывод полученных результатов fig. 5

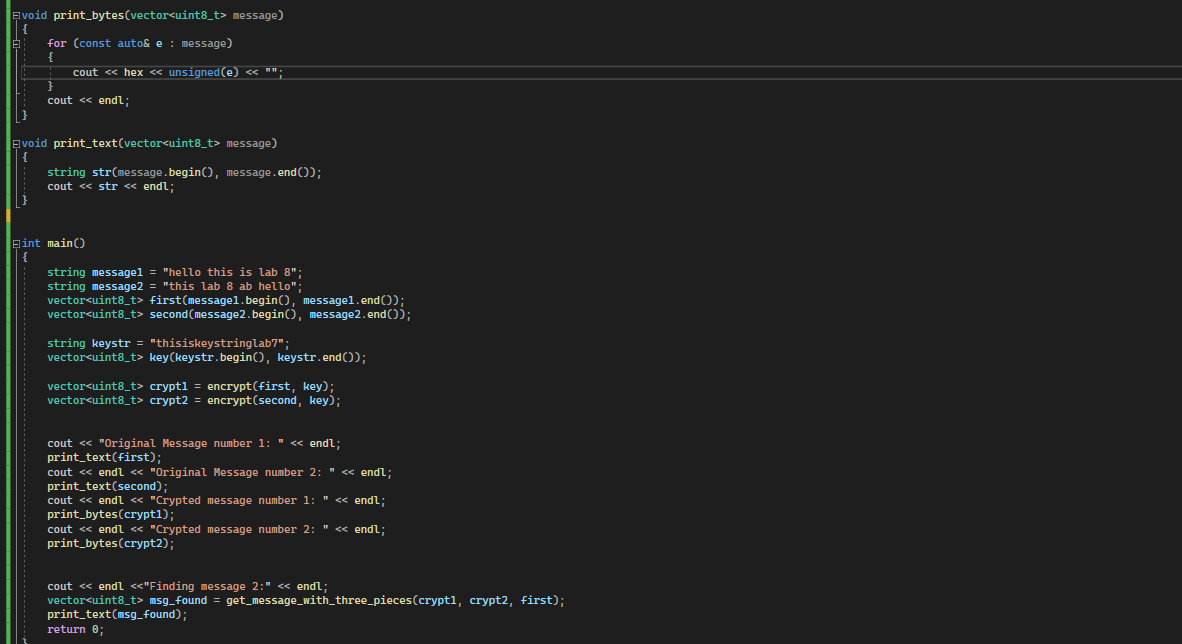


Figure 5: output\_prog

Получаю вывод программы, где мы видим, что мы смогли расшифровать сообщение без знаний ключа fig. 6

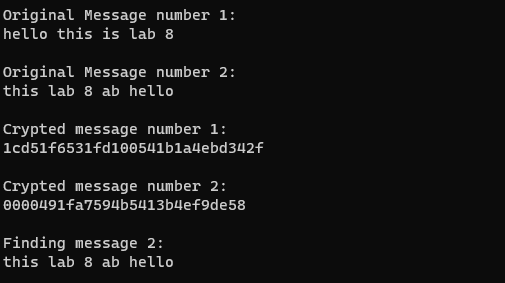


Figure 6: console\_output

# 3 Выводы

В результате выполнения работы я освоил на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

# 4 Список литературы

1. Методические материалы курса