Отчёт по лабораторной работе №8  
Информационная безопасность

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

Выполнил: Мальков Роман Сергеевич,  
НФИбд-02-21, 1032217048

Содержание

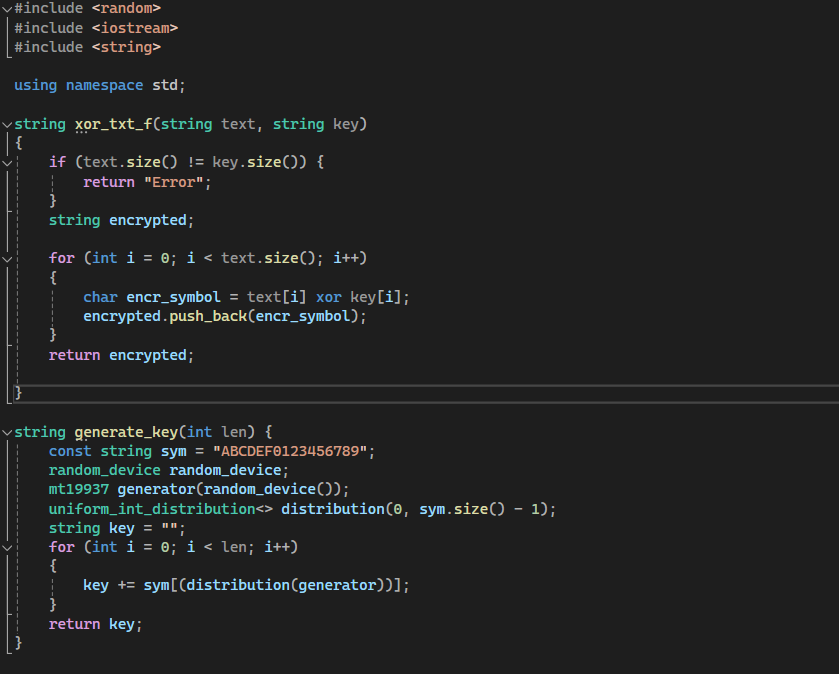
# Цель работы

Освоить на практике применение режима однократного гаммирования разных текстов одним ключом.

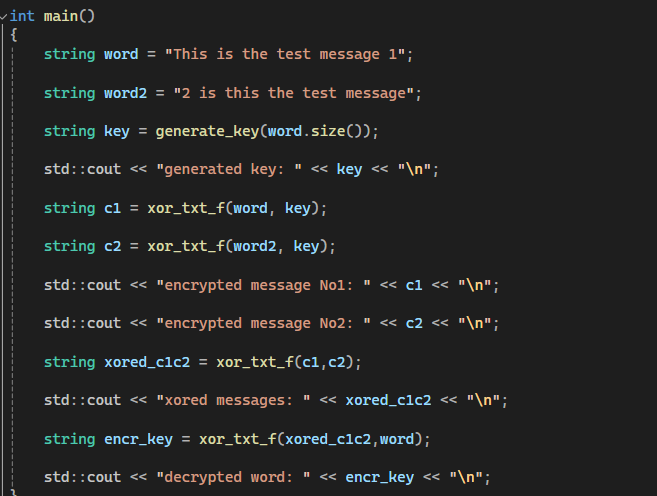
# Выполнение лабораторной работы

Чтобы зашифровать два сообщения одним ключем они должны быть одной и той же длинны. После получения зашифрованных сообщений, положим что у атакующего есть некий шаблон сообщения который совпадает с нашим незашифрованным сообщением. Тогда посредством применения операции однократного гаммирования между двумя зашифрованными сообщениями и одним известным шаблоном, мы можем получить текст второго сообщения.

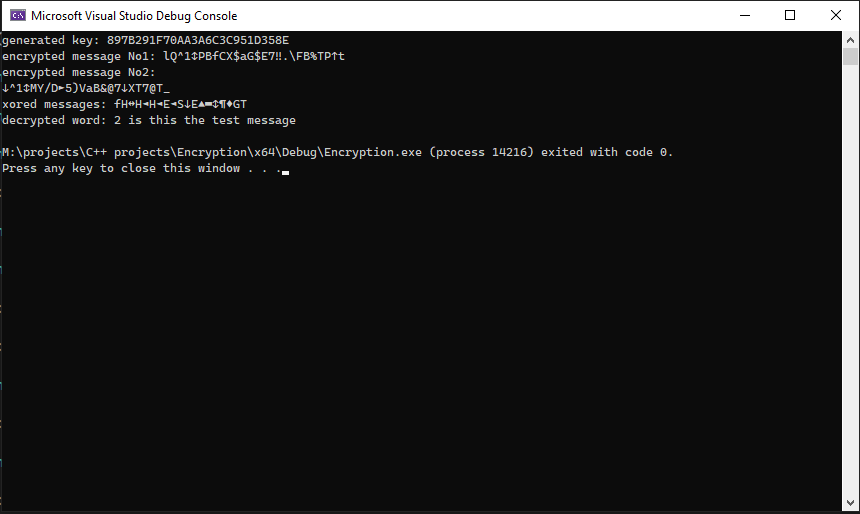
Для решения задачи написан программный код:



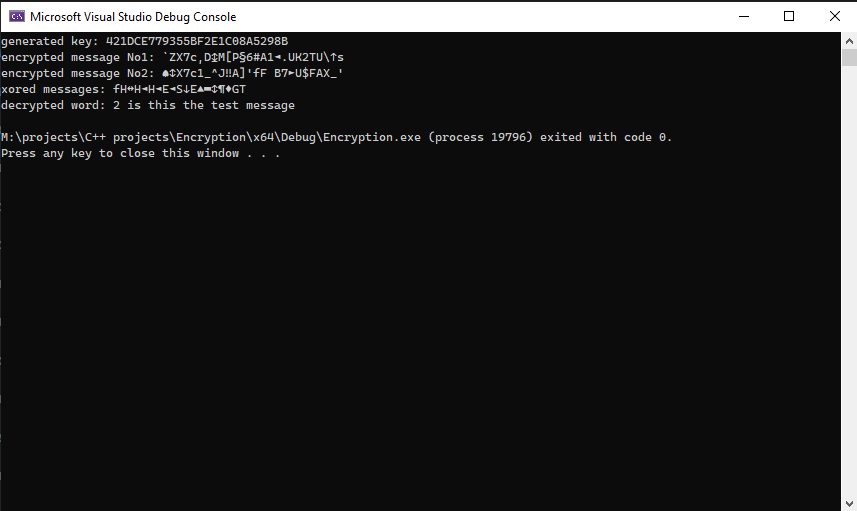
(рис. 1. Программный код приложения, реализующего режим однократного гаммирования)



(рис. 2. Программный код приложения, реализующего режим однократного гаммирования)



(рис. 3. Результат)



(рис. 4. Результат)

# Вывод

В ходе выполнения данной лабораторной работы было освоено на практике применение режима однократного гаммирования к двум сообщениям.

# Список литературы. Библиография

[0] Методические материалы курса