Отчёт по лабораторной работе №8

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

Тимур Дмитриевич Калинин

Содержание

# 1 Цель работы

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

# 2 Выполнение лабораторной работы

1. Напишем программу decryptor.c, которая будет выводить два шифротекста по известным текстам и ключу. ([Рис. 1](#fig:001))

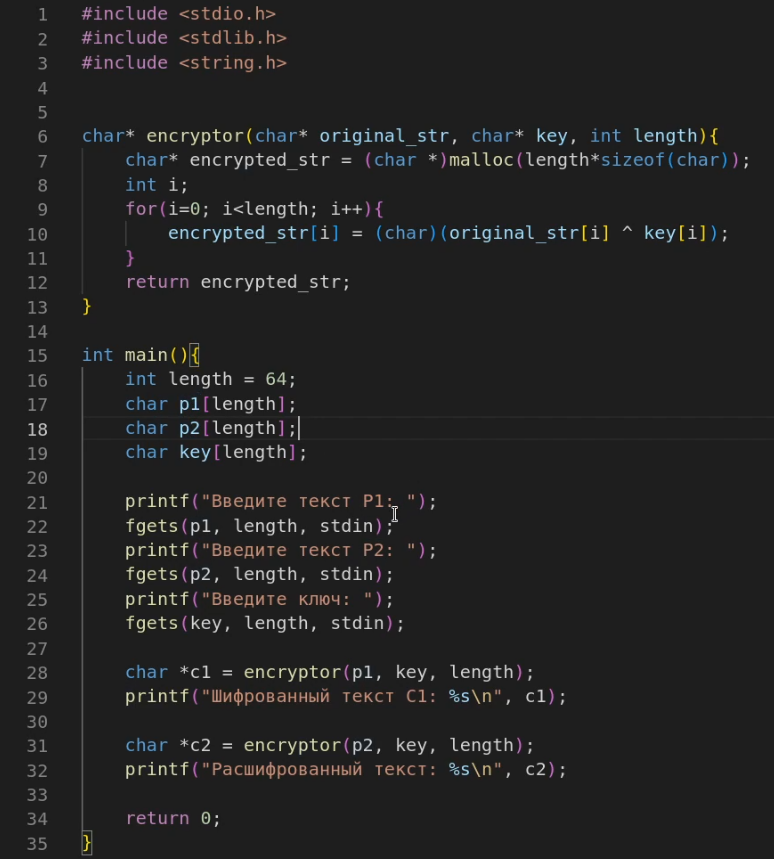


Figure 1: Код decryptor.c

1. Проверим работу программы decryptor ([Рис. 2](#fig:002))

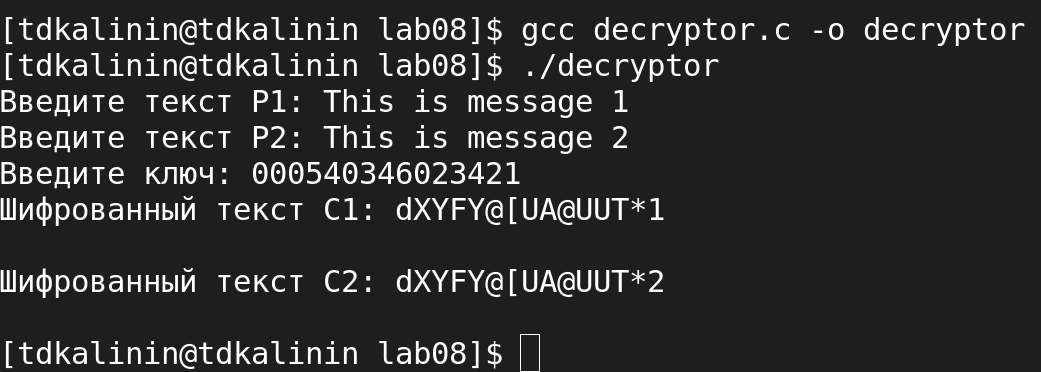


Figure 2: Работа программы decryptor

# 3 Контрольные вопросы

1. Как, зная один из текстов (P1 или P2), определить другой, не зная при этом ключа?

Применить операцию “исключающее или” к первому шифротексту, второму шифротексту и известному тексту.

1. Что будет при повторном использовании ключа при шифровании текста?

Получится исходный текст.

1. Как реализуется режим шифрования однократного гаммирования одним ключом двух открытых текстов?

Один и тот же ключ применяется для двух текстов.

1. Перечислите недостатки шифрования одним ключом двух открытых текстов.

Если злоумышленник узнает некий шаблон текста, то по нему он может попробовать прочитать сообщение.

1. Перечислите преимущества шифрования одним ключом двух открытых текстов.

Не требуется использовать несколько различных ключей.

# 4 Выводы

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

# 5 Библиография

1. Лабораторная работа №8. - 3 с. URL: <https://esystem.rudn.ru/pluginfile.php/1651895/mod_resource/content/2/008-lab_crypto-key.pdf>