Отчёт по лабораторной работе №8

Дисциплина: Информационная безопасность

Выполнил: Танрибергенов Эльдар

Содержание

Список иллюстраций

# 1 Цель работы

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

# 2 Задания

* Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста.

# 3 Указания к работе

Исходные данные. Две телеграммы Центра: P1 = НаВашисходящийот1204 P2 = ВСеверныйфилиалБанка

# 4 Выполнение работы

Программа написана на языке программирования С++

Функции с предыдущей лр не были изменены, поэтому их снимки я приводить не стану. В главной функции лишь добавил переменные для второй строки и провёл следующую последовательность действий: гаммировал два шифротекста, а затем полученный результат гаммировал с каждым шестнадцатеричным кодом. В итоге получил исходные сообщения без ключа.

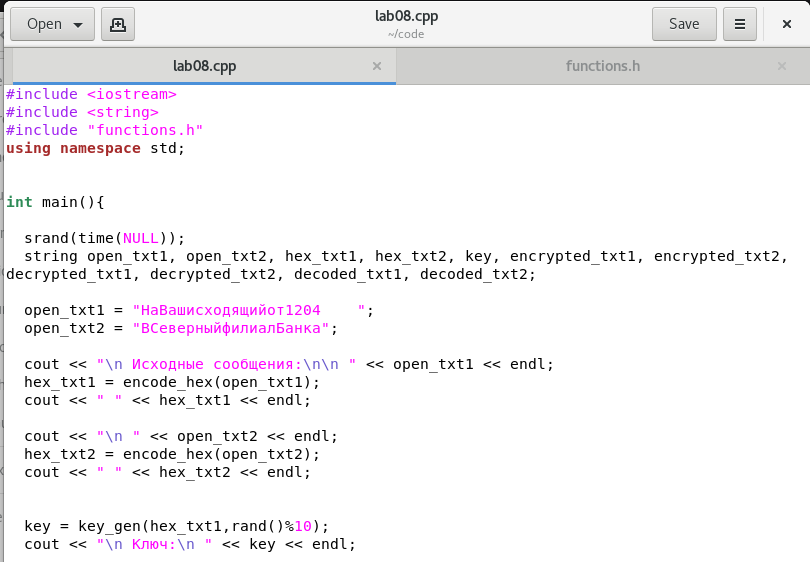


Рис. 1: Программа шифрования двух сообщений одним ключом

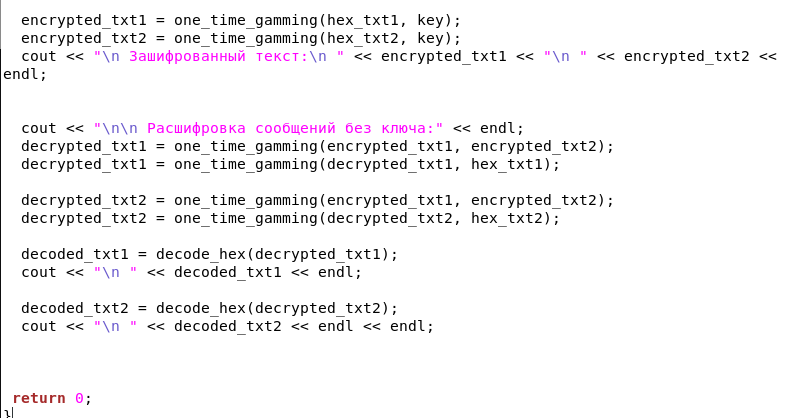


Рис. 2: Программа шифрования двух сообщений одним ключом

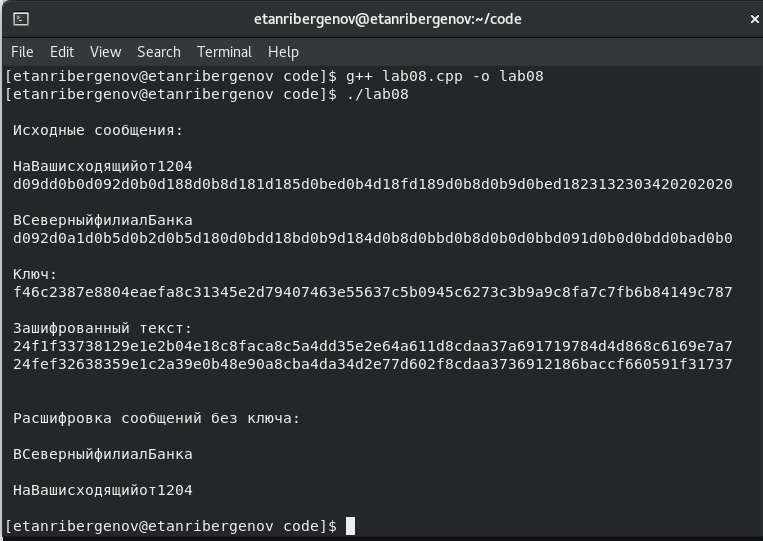


Рис. 3: Результат

# 5 Выводы

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

# 6 Ответы на контрольные вопросы

1. Гаммировать два шифротекста, а затем полученный результат гаммировать с известным текстом.
2. Дешифрование.
3. В функцию гаммирования передаются разные значения сообщений, а ключ единый.
4. Если они подчиняются некоторому шаблону, и злоумышленник знает об этом шаблоне, то может получить оба исходных текстов.
5. В однократном гаммировании используется операция сложения по модулю 2 (XOR).
6. Простота, скорость, универсальность.