Информационная безопасность

Л.8. Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Греков Максим Сергеевич

2021

Содержание

# Цель работы

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

# Теория

## Однократное гаммирование одним ключом

Режим шифрования однократного гаммирования одним ключом двухвидов открытого текста реализуется в соответствии со схемой (рис. 1)

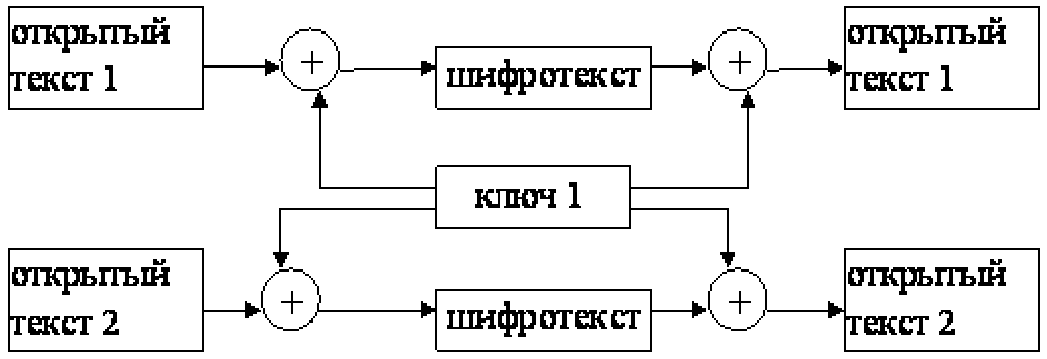


Figure 1: Общая схема шифрования двух различных текстов одним ключом

## Шифротексты телеграмм

Шифротексты обеих телеграмм можно получить по формулам режима однократного гаммирования:

Открытый текст можно найти в соответствии с (рис. 1), зная шифротекст двух телеграмм, зашифрованных одним ключом.

## Следствие свойства операции XOR

Для это оба равенства складываются по модулю 2. Тогда получаем:

Предположим, что одна из телеграмм является шаблоном — т.е. имеет текст фиксированный формат, в который вписываются значения полей.

## Получение второго открытого текста по первому

Допустим, что злоумышленнику этот формат известен. Тогда он получает достаточно много пар (известен вид обеих шифровок).

Тогда зная *P1*, имеем:

Таким образом, злоумышленник получает возможность определить те символы сообщения *P2*, которые находятся на позициях известного шаблона сообщения *P1*.

В соответствии с логикой сообщения *P2*, злоумышленник имеет реальный шанс узнать ещё некоторое количество символов сообщения *P2*.

Затем вновь используется описанное свойство с подстановкой вместо *P1* полученных на предыдущем шаге новых символов сообщения *P2*. И так далее.

Действуя подобным образом, злоумышленник даже если не прочитает оба сообщения, то значительно уменьшит пространство их поиска.

# Ход работы

## Исходные данные

Рассмотрим две телеграммы Центра:

* *P1* = НаВашисходящийот1204
* *P2* = ВСеверныйфилиалБанка

Ключ Центра длиной 20 байт:

*K* = 05 0C 17 7F 0E 4E 37 D2 94 10 09 2E 22 57 FF C8 0B B2 70 54

## Код исходных данных

Установим данные значения в соответствующие поля (рис. 2), используя программный код, реализованный в ходе предыдущий лабораторной, и получим шифротексты.

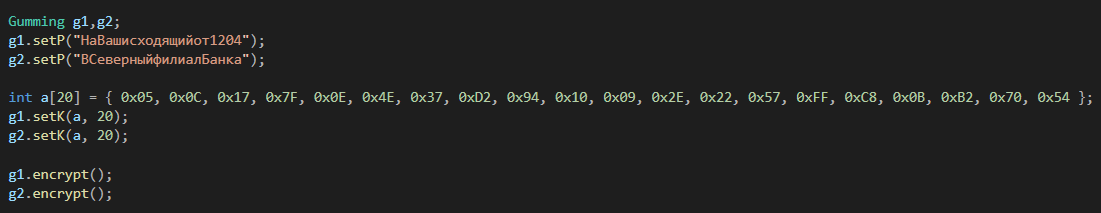


Figure 2: Исходные данные

## Функция tripl()

Реализуем функцию (рис. 3), принимающую три строки, и возвращающую их совместное наложение операцией *XOR*, согласно описанному раннее свойству.

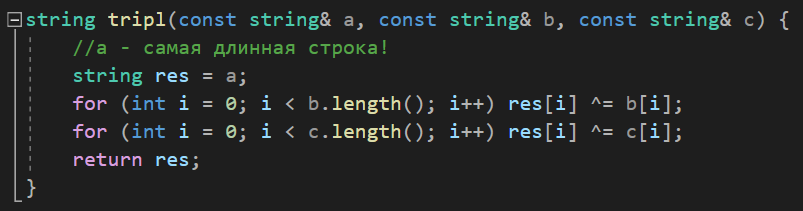


Figure 3: Функция tripl()

## Последовательные вызовы tripl()

Предположим, что злоумышленник знает начало первого сообщения *“НаВаш”*.

Пользуясь *tripl()* (рис. 4) пробуем расшифровать имеющиеся сообщения последовательной подстановкой в функцию открытых участков то первого, то второго сообщения, постепенно подбирая (рис. 5) продолжения уже имеющихся участков, тем самым увеличивая длину расшифрованных последовательностей.

Таким образом удалось полность расшифровать оба сообщения.

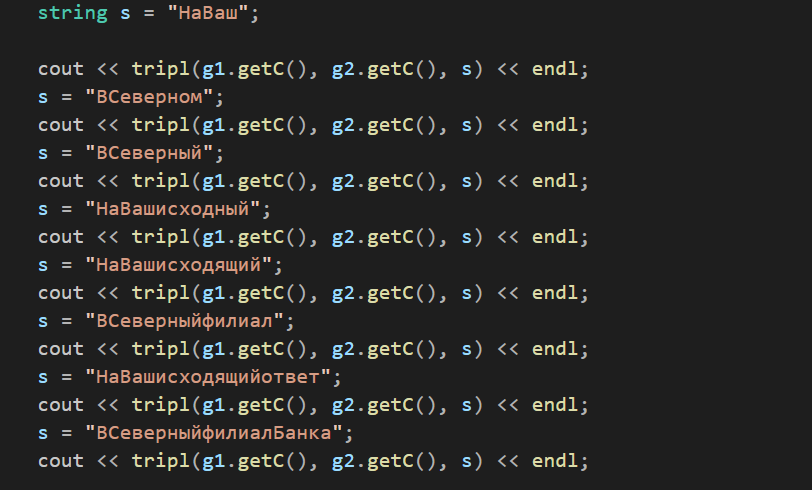


Figure 4: Последовательные вызовы функции *tripl()* с новыми данными

## Последовательные открытия участков

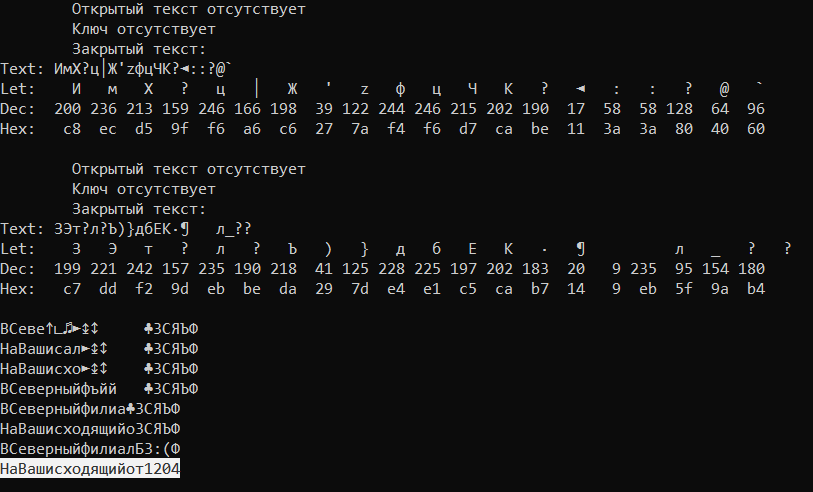


Figure 5: Последовательные открытия участков с новыми данными

# Вывод

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