РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №8

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

дисциплина: Информационная безопасность

Студент: Койфман Кирилл Дмитриевич

Группа: НПИбд-01-21

Введение.

Цель работы.

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

Задачи.

1. Разобрать теоретическую часть и указание к работе, описанные в файле.
2. Разработать приложение, позволяющее шифровать и дешифровать тексты $P\_1$ и $P\_2$ в режиме однократного гаммирования. Приложение должно определить вид шифротекстов $C\_1$ и $C\_2$ обоих текстов $P\_1$ и $P\_2$ при известном ключе.

# Ход работы

1 задание

Разберём теоретическую часть лабораторной работы:

Исходные данные.

Две телеграммы Центра:

$P\_1$ = "НаВашисходящийот1204"

$P\_2$ = "ВСеверныйфилиалБанка" Ключ Центра длиной 20 байт:

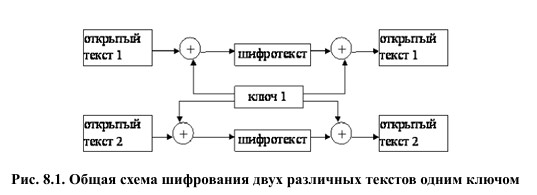
$K$ = 05 0C 17 7F 0E 4E 37 D2 94 10 09 2E 22 57 FF C8 OB B2 70 54

Режим шифрования однократного гаммирования одним ключом двух видов открытого текста реализуется в соответствии со схемой, приведён ной на рис. 8.1.

Шифротексты обеих телеграмм можно получить по формулам режима однократного гаммирования:

$$ (8.1) C\_1 = P\_1 \oplus K, \ C\_2 = P\_2 \oplus K. $$

Открытый текст можно найти в соответствии с (8.1), зная шифротекст двухтелеграмм, зашифрованныходнимключом:



Для этого оба равенства складываются по модулю 2. Тогда с учётом свойства операции XOR

$$ (8.2) 1\oplus1=0, 1\oplus0=1 $$ получаем:

$$ C\_1\oplus C\_2 = P\_1\oplus K\oplus P\_2\oplus K = P\_1\oplus P\_2 $$

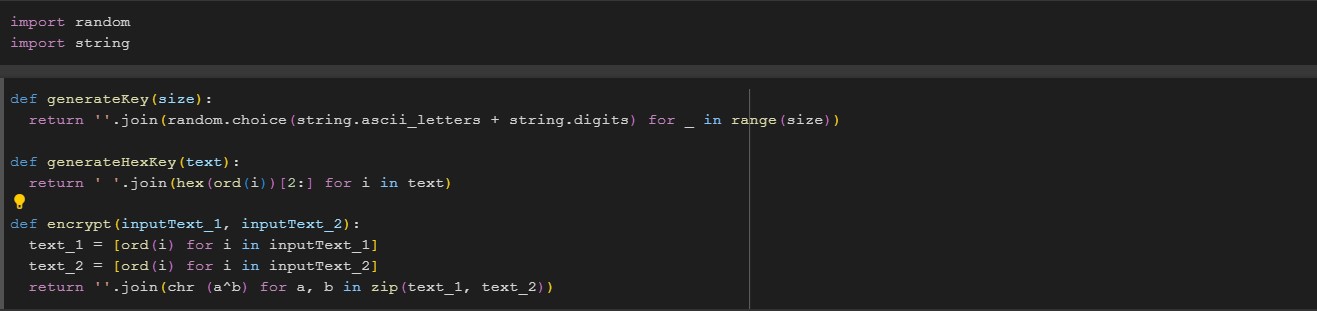
Предположим, что одна из телеграмм является шаблоном — т.е. имеет текст фиксированный формат, в который вписываются значения полей. Допустим, что злоумышленнику этот формат известен. Тогда он получает достаточно много пар $C\_1\oplus C\_2$ (известен вид обеих шифровок). Тогда зная $P\_1$ и учитывая (8.2), имеем:

$$ C\_1\oplus C\_2\oplus P\_1 = P\_1\oplus P\_2\oplus P\_1 = P\_2 $$

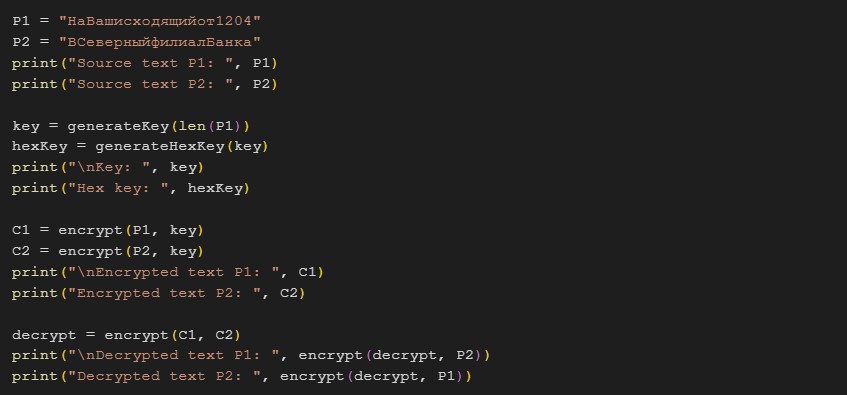
Таким образом, злоумышленник получает возможность определить те символы сообщения $P\_2$, которые находятся на позициях известного шаблона сообщения $P\_1$. В соответствии с логикой сообщения $P\_2$, злоумышленник имеет реальный шанс узнать ещё некоторое количество символов сообщения $P\_2$. Затем вновь используется (8.3) с подстановкой вместо $P\_1$ полученных на предыдущем шаге новых символов сообщения $P\_2$. И так далее. Действуя подобным образом, злоумышленник даже если не прочитает оба сообщения, то значительно уменьшит пространство их поиска.

2 задание

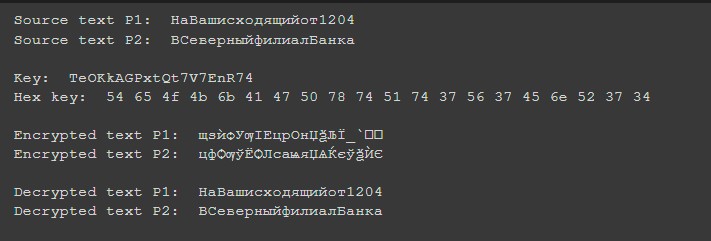
Далее реализуем программу, позволяющую шифровать и дешифровать тексты $P\_1$ и $P\_2$ в режиме однократного гаммирования, на языке Python и протестируем её (рис. 1 - рис.3):



*РИС.1(код программы: подключение необходимых модулей и объявление основных функций для генерации ключей и шифрования, дешифрования текста)*



*РИС.2*



*РИС.3(результаты программы)*

# Заключение

В ходе проделанной лабораторной работы мной были усвоены навыки применениея режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.