Отчёт по лабораторной работе №8

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

Низамова Альфия Айдаровна

Содержание

# 1 Цель работы

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

# 2 Выполнение

Задание:  
Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

Для написания программы использовала язык Python.  
Для начала импортировала необходимые библиотеки и задала две исходные строки равной длины(рис.1)

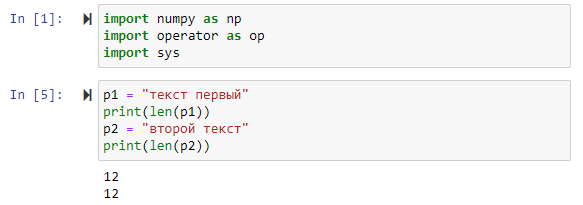


Рис. 1

Написала функцию, которая определяет вид шифротекстов обеих строк при известном ключе(рис.2)



Рис. 2

Вывод первой функции(рис.3)

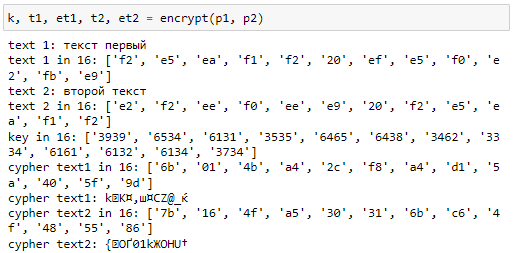


Рис. 3

Написала функцию, которая при известных двух шифротекстах и одном открытом тексте находит вид второго открытого текста без ключа (рис.4)

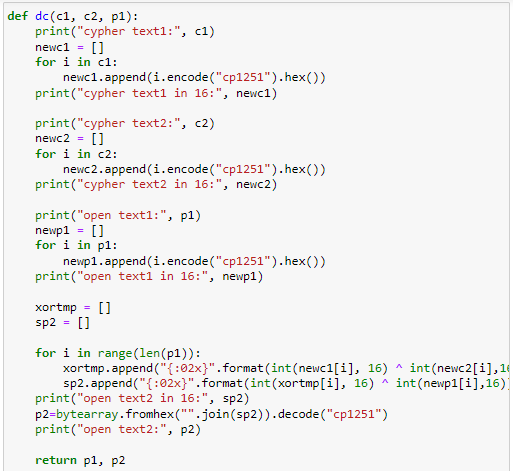


Рис. 4

Вывод второй функции(рис.5)

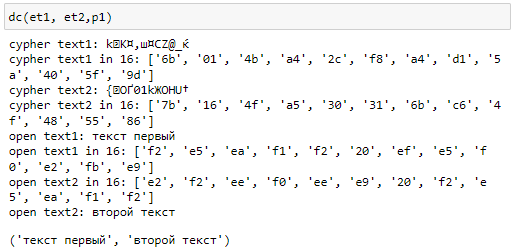


Рис. 5

# 3 Вывод

В ходе лабораторной работы мне удалось освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.