Отчет по лабораторной работе №7

Элементы криптографии. Однократное гаммирование

Низамова Альфия Айдаровна

Содержание

# 1 Цель работы

Освоить на практике применение режима однократного гаммирования

# 2 Выполнение

Задание:  
Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!».  
Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования.  
Приложение должно: 1. Определить вид шифротекста при известном ключе и известном открытом тексте. 2. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

Импортируем необходимые библиотеки (рис.1)



Рис. 1

Мы написали функцию *func( )*, определяющую вид шифротекста при известном ключе и известном открытом тексте (рис.2)



Рис. 2

Мы написали функцию *findk( )*, определяющую ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста (рис.3)

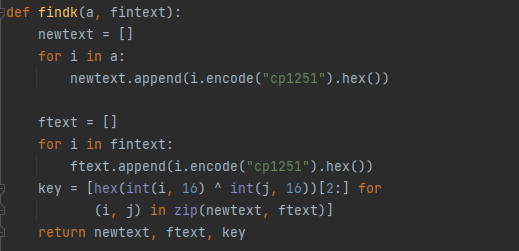
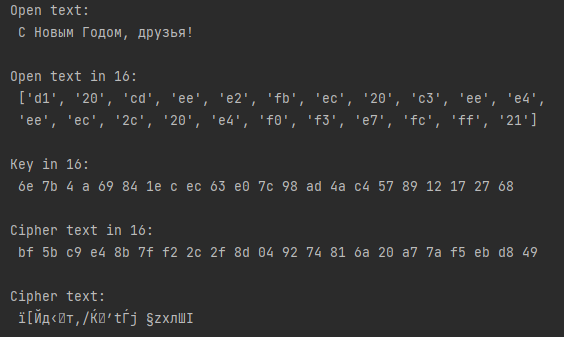
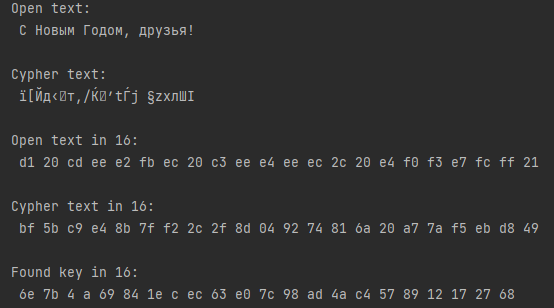


Рис. 3

Вывод программы (рис.4-5)

# 3 Вывод

Мы освоили на практике применение режима однократного гаммирования