Отчет по лабораторной работе 7

Дисциплина: Информационная безопасность

Савченков Дмитрий Андреевич, НПИбд-02-18

Содержание

List of Figures

List of Tables

1 Цель работы

Освоить на практике применение режима однократного гаммирования

2 Выполнение лабораторной работы:

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. Определил вид шифротекста при известном ключе и известном открытом тексте.(рис. 2.1).

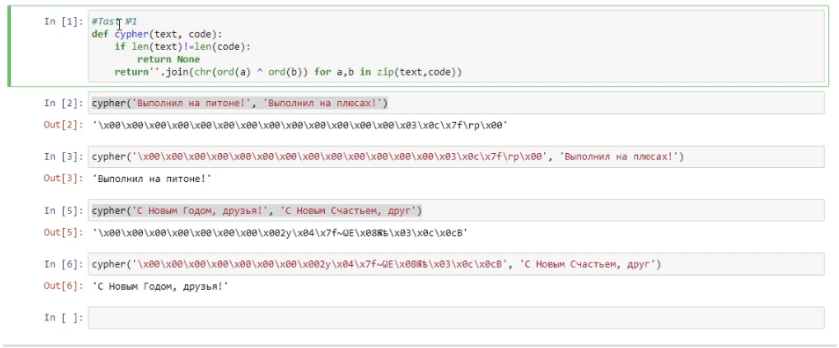

Figure 2.1: Задание №1

2. Определил ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.(рис. 2.2).

Figure 2.2: Задание №2

3 Выводы

Освоил на практике применение режима однократного гаммирования.

Список литературы

1. Кулябов Д. С., Королькова А. В., Геворкян М. Н. Информационная безопасность компьютерных сетей. Лабораторная работа № 5. Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов