отчёта по лабораторной работе 7

Элементы криптографии. Однократное гаммирование

Неустроева Ирина Николаевна

Содержание

Список иллюстраций

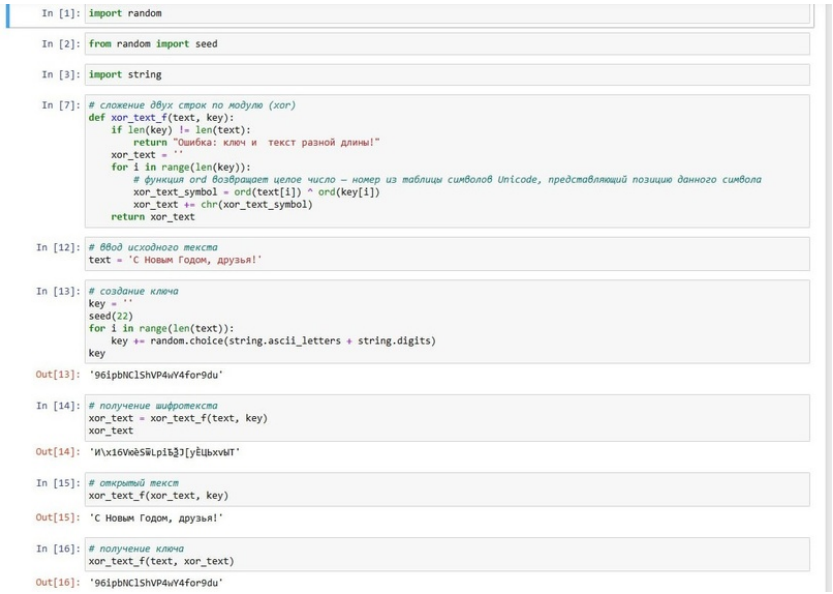
Список таблиц

1 Цель работы

Освоить напрактике применение режима однократного гаммирования.

2 Выполнение лабораторной работы

В подтверждение выполнения задания прилагаю скриншот кода программы, написанной на языке Python.



```
In [1]: import random

In [2]: from random import seed

In [3]: import string

In [7]: # сложение двух строк по модулю (xor)
        def xor_text_f(text, key):
            if len(key) != len(text):
                return "Ошибка: ключ и  текст разной длины!"
            xor_text = ''
            for i in range(len(key)):
                # функция ord возвращает целое число — номер из таблицы символов Unicode, представляющий позицию данного символа
                xor_text_symbol = ord(text[i]) ^ ord(key[i])
                xor_text += chr(xor_text_symbol)
            return xor_text

In [12]: # ввод исходного текста
         text = 'С Новым Годом, друзья!'

In [13]: # создание ключа
         key = ''
         seed(22)
         for i in range(len(text)):
             key += random.choice(string.ascii_letters + string.digits)
         key

Out[13]: '96ipbNClShVP4wY4for9du'

In [14]: # получение шифротекста
         xor_text = xor_text_f(text, key)
         xor_text

Out[14]: 'И\x16VюЬ§Ѓ Lpi‰J[yЁЦЬхvЫТ'

In [15]: # открытый текст
         xor_text_f(xor_text, key)

Out[15]: 'С Новым Годом, друзья!'

In [16]: # получение ключа
         xor_text_f(text, xor_text)

Out[16]: '96ipbNClShVP4wY4for9du'
```

Рис. 2.1: Программный код

Ключевым элементом этой программы является функция xortextf, которая принимает две строки для сложения. Эти строки должны иметь одинаковую длину, и программа проверяет это условие. Если длины строк различаются, выводится сообщение об ошибке. В случае успешной проверки мы поочередно применяем операцию сложения по модулю к символам строк, в результате чего получаем сумму двух строк.

3 Выводы

В процессе выполнения лабораторной работы я овладела навыками шифрования и дешифрования сообщений с использованием однократного гаммирования и познакомилась с этим методом в криптографии.