Отчет по лабораторной работе № 7

Основы информационной безопасности

Маметкадыров Ынтымак

Российский университет дружбы народов, Москва, Россия

НПМбд-02-20

Цели лабораторной работы

1) Освоить на практике применение режима однократного гаммирования.

Задачи лабораторной работы

1) Написать программу на языке Python, реализующую режим однократного гаммирования.

Ход выполнения лабораторной работы

- In[1]: импорт необходимых библиотек
- In[3]: функция, реализующая сложение по модулю два двух строк
- In[4]: открытый/исходный текст
- In[5]: создание ключа той же длины, что и открытый текст

```
[1]: import random
     from random import seed
     import string

[3]: def cipher(text, key):
         if len(key) != len(text):
             return "Ключ и текст должны быть одной длины"
         cipher_text = ''
         for i in range(len(key)):
             cipher_text_symbol = ord(text[i]) ^ ord(key[i])
             cipher_text += chr(cipher_text_symbol)
         return cipher_text

[4]: text = 'С Новым годом, друзья!'

[5]: key = ''
     seed(10)
     for i in range(len(text)):
         key += random.choice(string.ascii_letters + string.digits)
     key

[5]: 'KcBEKanD0F0rPZkcHFuep8'
```

Рис. 1: Код программы Часть 1

Ход выполнения лабораторной работы

- In[6]: получение шифротекста, при условии, что известны открытый текст и ключ
- In[7]: получение открытого текста, при условии, что известны шифротекст и ключ
- In[8]: получение ключа, при условии, что известны открытый текст и шифротекст

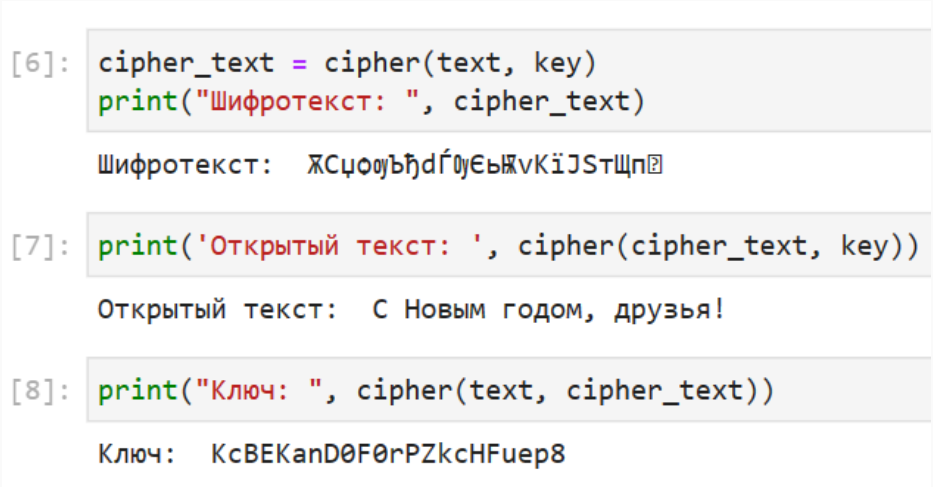

Рис. 2: Код программы Часть 2

Вывод

- В ходе выполнения данной лабораторной работы мы освоили на практике применение режима однократного гаммирования.