Лабораторная работа №7

Информационная безопасность

Леонтьева К. А., НПМбд-01-19

18 октября 2022

Российский университет дружбы народов

Москва, Россия

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[21]: импорт необходимых библиотек
- In[22]: функция, реализующая сложение по модулю два двух строк
- In[23]: открытый/исходный текст
- In[24]: создание ключа той же длины, что и открытый текст

In [21]:
```
import random
from random import seed
import string
```

In [22]:
```
def cipher_text_function(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
```

In [23]:
```
text = "С Новым годом, друзья!"
```

In [24]:
```
key = ''
seed(23)
for i in range(len(text)):
    key += random.choice(string.ascii_letters + string.digits)
print(key)
```

```
7X8s51fbLtByHwiUmrCaoN
```

Figure 1: Рис.1: Код программы Часть 1

Ход выполнения лабораторной работы

- In[25]: получение шифротекста, при условии, что известны открытый текст и ключ
- In[26]: получение открытого текста, при условии, что известны шифротекст и ключ
- In[27]: получение ключа, при условии, что известны открытый текст и шифротекст

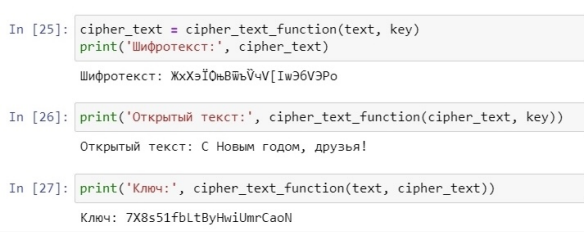

Figure 2: Рис.2: Код программы Часть 2

Вывод

- В ходе выполнения данной лабораторной работы я освоила на практике применение режима однократного гаммирования.