Лабораторная работа №8

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 на примере кодирования различных исходных текстов одним ключом.

Задачи лабораторной работы

1) Написать программу на языке Python, реализующую режим однократного гаммирования для двух текстов, кодируемых одним ключом.

Ход выполнения лабораторной работы

- In[1]: импорт необходимых библиотек
- In[2]: функция, реализующая сложение по модулю два двух строк
- In[3]: открытые/исходные тексты (одинаковой длины)
- In[5]: создание ключа той же длины, что и открытые тексты

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

In [2]:
```
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 [3]:
```
text_1 = "С Новым годом, друзья!"
text_2 = "Поздравляем с 8 марта!"
```

In [5]:
```
key = ''
seed(23)
for i in range(len(text_1)):
    key += random.choice(string.ascii_letters + string.digits)
print(key)
```

```
7X8s51fbLtByHwiUmrCaoN
```

Figure 1: Рис.1: Код программы Часть 1

- In[7]: получение шифротекстов при условии, что известны открытые тексты и ключ
- In[8]: получение открытых текстов при условии, что известны шифротексты и ключ

```
In [7]: cipher_text_1 = cipher_text_function(text_1, key)
        cipher_text_2 = cipher_text_function(text_2, key)
        print('Первый шифротекст:', cipher_text_1)
        print('Второй шифротекст:', cipher_text_2)

        Первый шифротекст: ЖxXэЇѲњBѿъѶчV[IwЭбVЭPo
        Второй шифротекст: ШѦЏчvЁєљЃcѾYЉWQuётЃYџo

In [8]: print('Первый открытый текст:', cipher_text_function(cipher_text_1, key))
        print('Второй открытый текст:', cipher_text_function(cipher_text_2, key))

        Первый открытый текст: С Новым годом, друзья!
        Второй открытый текст: Поздравляем с 8 марта!
```

Figure 2: Рис.2: Код программы Часть 2

Ход выполнения лабораторной работы

- In[9]: сложение по модулю два двух шифротекстов
- In[10]: получение открытых текстов при условии, что известны оба шифротекста и один из открытых текстов
- In[12]: получение части первого открытого текста (срез)
- In[14]: получение части второго текста при условии, что известны оба шифротекста и часть первого открытого текста

```
In [9]: cipher_text_xor = cipher_text_function(cipher_text_1, cipher_text_2)
        print('Первый шифротекст XOR Второй шифротекст:', cipher_text_xor)

        Первый шифротекст XOR Второй шифротекст: >O*
        r{ЫЛ|O}ЫД|sw▯▯

In [10]: print('Первый открытый текст:', cipher_text_function(cipher_text_xor, text_2))
         print('Второй открытый текст:', cipher_text_function(cipher_text_xor, text_1))

         Первый открытый текст: С Новым годом, друзья!
         Второй открытый текст: Поздравляем с 8 марта!

In [12]: text_1_ = text_1[3:6]
         print('Часть первого открытого текста:', text_1_)

         Часть первого открытого текста: овы

In [14]: cipher_text_xor_ = cipher_text_function(cipher_text_1[3:6], cipher_text_2[3:6])
         print('Часть второго открытого текста:', cipher_text_function(cipher_text_xor_, text_1_))

         Часть второго открытого текста: дра
```

Вывод

- В ходе выполнения данной лабораторной работы я освоила на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.