Отчет по лабораторной работе №8

Основы информационной безопасности

Маметкадыров Ынтымак

Российский университет дружбы народов имени Патриса Лумумбы, Москва, Россия

НПМбд-02-20

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[15]: открытые/исходные тексты (одинаковой длины)
- In[6]: создание ключа той же длины, что и открытые тексты

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

[2]:
```
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
```

[15]:
```
text_1 = 'С Новым годом, друзья!'
text_2 = 'Поздравляем с 8 марта!'
```

[6]:
```
key = ''
seed(10)
for i in range(len(text_1)):
    key += random.choice(string.ascii_letters + string.digits)
key
```

[6]:
```
'KcBEKanD0F0rPZkcHFuep8'
```

Ход выполнения лабораторной работы

- In[8]: получение шифротекстов при условии, что известны открытые тексты и ключ
- In[9]: получение открытых текстов при условии, что известны шифротексты и ключ

```
[8]:
cipher_text_1 = cipher(text_1, key)
cipher_text_2 = cipher(text_2, key)
print("Шифротекст 1: ", cipher_text_1)
print("Шифротекст 2: ", cipher_text_2)

Шифротекст 1:  ѪСџѻђЂћdЃЏЄьѬvKїJSтЩп□
Шифротекст 2:  єйvψЋёЌѾѾѳЌRБzSCVѶeЧp□

[9]:
print('Открытый текст 1: ', cipher(cipher_text_1, key))
print('Открытый текст 2: ', cipher(cipher_text_2, key))

Открытый текст 1:  С Новым годом, друзья!
Открытый текст 2:  Поздравляем с 8 марта!
```

Рис. 2: Код программы Часть 2

Ход выполнения лабораторной работы

- In[11]: сложение по модулю два двух шифротекстов
- In[12]: получение открытых текстов при условии, что известны оба шифротекста и один из открытых текстов
- In[16]: получение части первого открытого текста (срез)
- In[17]: получение части второго текста при условии, что известны оба шифротекста и часть первого открытого текста

[11]:

```
cipher_text_xor = cipher(cipher_text_1, cipher_text_2)
print("Шифротекст 1 XOR Шифротекст 2: ", cipher_text_xor)
```

```
Шифротекст 1 XOR Шифротекст 2:  >O*
r{ЫЛ|O}ЫД|swЫЫ
```

[12]:

```
print('Перый открытый текст: ', cipher(cipher_text_xor, text_2))
print('Второй открытый текст: ', cipher(cipher_text_xor, text_1))
```

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

[16]:

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

```
Часть первого открытого текста:  овы
```

[17]:

```
cipher_text_xor_ = cipher(cipher_text_1[3:6], cipher_text_2[3:6])
print('Часть второго откыртого текста: ', cipher(cipher_text_xor_, text_1_))
```

```
Часть второго откыртого текста:  дра
```

Вывод

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