Презентация для лабораторной работы №8

Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Боровикова К. В.

23 сентября 2023

Российский университет дружбы народов, Москва, Россия

Лабораторная работа №8

Вводная часть

Объект и предмет исследования

- Язык Python
- Шифрование различных исходных текстов одним ключом

Цели и задачи

- Написать программу для шифровки и дешифровки текстов
- Произвести работу по шифровке и дешифровке текстов

Ход выполнения работы

Пишем код на Python

```
[38] import random
     from random import seed
     import string
```

```
[40] def infosec(text, key):
       if len(key) != len(text):
         return 'Error! The text and the key must have the same length!'
       e_text = ''
       for i in range(len(key)):
         e_text_symb = ord(text[i]) ^ ord(key[i])
         e_text += chr(e_text_symb)

       return e_text
```

Loading...

```
text_1 = input('Enter the first text: ')
text_2 = input('Enter the second text: ')
```

```
Enter the first text: Мяу
Enter the second text: Мур
```

```
[41] key = ''
     seed(45)
     for i in range(len(text_1)):
       key += random.choice(string.ascii_letters + string.digits)

     print(key)
```

```
rAF
```

```
[42] encoded_text_1 = infosec(text_1, key)
     encoded_text_2 = infosec(text_2, key)

     print(f'The first encoded text: {encoded_text_1}, '
           f'The second encoded text: {encoded_text_2}')
```

Пишем код на Python

```
[42] encoded_text_1 = infosec(text_1, key)
     encoded_text_2 = infosec(text_2, key)

     print(f'The first encoded text: {encoded_text_1}, '
           f'The second encoded text: {encoded_text_2}')
```

```
The first encoded text: ЗЎЅ, The second encoded text: ЗЪI
```

```
[43] print(f'The first decoded text: {infosec(encoded_text_1, key)}, '
           f'The second decoded text: {infosec(encoded_text_2, key)}')
```

```
The first decoded text: May, The second decoded text: Myp
```

```
e_text_xor = infosec(encoded_text_1, encoded_text_2)
print(f'The first xor encoded text: {e_text_xor}')
```

```
The first xor encoded text: ⍰⍈
```

```
[45] print(f'The first decoded text: {infosec(e_text_xor, text_2)}, '
           f'The second decoded text: {infosec(e_text_xor, text_1)}')
```

```
The first decoded text: May, The second decoded text: Myp
```

```
text_1_slice = text_1[1:3]
print(f'The known slice of the first text: {text_1_slice}')
```

```
The known slice of the first text: ay
```

```
[47] e_text_xor_slice = infosec(encoded_text_1[1:3], encoded_text_2[1:3])
     print(f'Part of the second decoded text: {infosec(e_text_xor_slice, text_1_slice)}')
```

```
Part of the second decoded text: yp
```

```
[ ]
```

Результаты

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