Лабораторная работа №8

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

Легиньких Г.А.

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Легиньких Галина Андреевна
- НФИбд-02-21
- Российский университет дружбы народов
- 1032216447@pfur.ru
- https://github.com/galeginkikh

Выполнение

Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

Выполнение лабораторной работы

1. Написала функцию для генерации рандомного ключа(состоит из случайно последовательности символов).

```python
import random

def generate_key(word):
    key = ""
    for _ in range(len(word)):
        key += random.choice("0123456789abcdef") # Шестнадцатеричная систкма
    return key
```

Рис. 1: Ключ

2. Добавила функцию для шифрования и дешифрования.

```
def en_de_crypt(text, key):
    new_text = ""
    for i in range(len(text)):
        new_text += chr(ord(text[i])^ord(key[i%len(key)]))
    return new_text
```

Рис. 2: Шифрование и дешифрование

3. Задала два предложения одной длины.

```
text_1 = 'Машина быстро проехала мимо парка'
text_2 = 'Кошка тихо спала на мягком диване'
```

Рис. 3: Предложения

4. Использовала один ключ для шифрования и дешифрования обоих предложений.

```
key = generate_key(text_1)
en_text_1 = en_de_crypt(text_1, key)
de_text_1 = en_de_crypt(en_text_1, key)
en_text_2 = en_de_crypt(text_2, key)
de_text_2 = en_de_crypt(en_text_2, key)

print("Ключ -", key)
print("Текст 1","\nЗашифрованный текст -", en_text_1, "\nДешифрованный текст -", de_text_1)
print("Текст 2","\nЗашифрованный текст -", en_text_2, "\nДешифрованный текст -", de_text_2)
```

Рис. 4: Запуск функций

5. После запуска получилось вот это.

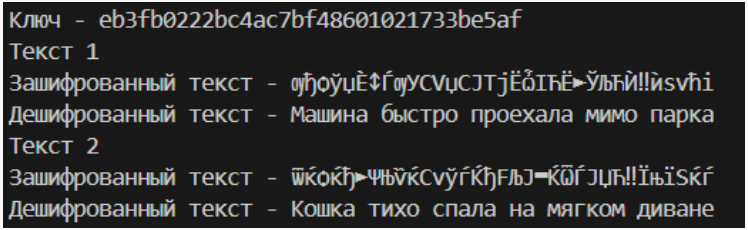

Рис. 5: Вывод

Вывод

Вывод

Освоила на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.