Лабораторная №7

Основы информационной безопасности

Банникова Екатерина Алексеевна

Российский университет дружбы народов, Москва, Россия

НПМбд-01-19

Элементы криптографии.

Однократное гаммирование

Цель лабораторной работы

- Получить практические навыки по работе с однократным гаммированием

Задачи лабораторной работы

1. Написать функцию шифровки и дешифровки данных в режиме однократного гаммирования
2. Определить вид шифротекста при известном ключе и октрытом тексте
3. Определить ключ, преобразующий шифротекст в один из вариантов прочтения открытого текста

Выполнение

Создаем функцию, которая осуществляет однократное гаммирование посредством побитового XOR

```python
def cript(text, key):
    if len(text) != len(key):
        return "Error: key must be the same lenght as text"
    res = ''
    for i in range(len(key)):
        p = ord(text[i]) ^ ord(key[i])
        res += chr(p)
    return res
```

Figure 1: Функция шифрования

Задаем текстовую строку и создаем случайный символьный ключ такой длины

```
text = 'С Новым годом, друзья!'
```

```
from random import randint, seed
seed(42)
key = ''
for i in range(len(text)):
    key += chr(randint(0,5000))
print(key)
```

```
ťÌ?ﻬ∑v̈‗—'Ħ?Ąô˛ﮨ́◌́ǀ٩Ùㅎㄴ.╕‖
```

Figure 2: Исходные данные

Запускаем функцию. В первом случае получаем зашифрованный текст. Используя тот же ключ, осуществляем дешифровку текста. Зная оригинальный текст и его шифровку, может получить ключ.

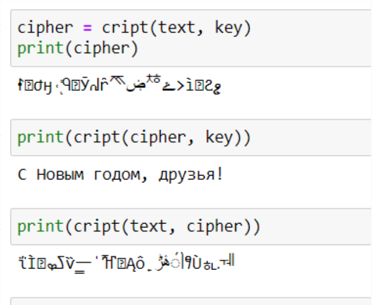

Figure 3: Результат работы программы

Выводы

Освоено на практике применение режима однократного гаммирования.