

Лабораторная работа №7

Основы информационной безопасности

Кондрашова А. А.

15 октября 2022 г.

Российский университет дружбы народов, Москва, Россия

НПМбл-01-19

Освоить основы шифрования через однократное гаммирование.

- Создаём функцию, которая осуществляет однократное гаммирование посредством побитового XOR

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

Figure 1: Функция шифрования

- Задаём текстовую строку и создаём случайный символьный ключ такой же длины

```
: text = "С новым годом друзья!"
```

Figure 2: Исходные данные

```
from random import randint, seed
seed(31)
key = ''
for i in range(len(text)):
    key += chr(randint(0,5000))
print(key)
```

dϣθζΤΨIHC јѵϗđĵŷđHHm3gđ

Figure 3: Задание ключа

Я освоила основы шифрования через однократное гаммирование