## Лабораторная работа №7

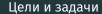
Основы информационной безопасности

Кондрашова А. А.

15 октября 2022 г.

Российский университет дружбы народов, Москва, Россия

НПМбл-01-19



Освоить основы шифрования через однократное гаммирование.

## Выполнение лабораторной работы

• 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

## Выполнение лабораторной работы

• 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)
d % 0&cTYIHL jvydjy i ### 1825
```

Figure 3: Задание ключа

## Выполнение лабораторной работы

- Запускаем функцию. В первом случае получаем зашифрованный текст. Далее, используя тот же самый ключ, осущвляем дешифровку текста. Так же, зная оригинальный текст и его шифорку, можем получить ключ.
- Все эти действия осуществляются через одну и ту же функцию.

```
cipher = cript(text,key)
print(cipher)
xw³ههالدب
```

Figure 4: Результат работы программы - зашифрованный текст

```
(print(cript(cipher, key)))
С новым годом друзья!
```

Figure 5: Результат работы программы - дешифровка текста



Я освоила основы шифрования через однократное гаммирование