Лабораторная работа №8

Основы информационной безопасности

Кондрашова А. А.

15 октября 2022 г.

Российский университет дружбы народов, Москва, Россия

НПМбл-01-19

Цели и задачи

- Освоить на практике применение однократного гаммирования при работе различными текстами на одном ключе.

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 same 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 две равные по длине текстовые строки и создаём случайный символьный ключ такой же длины

```
text1 = "С новым годом, друзья!"
text2 = "С днем рождения тебя!!"
```

```
from random import randint, seed
seed(31)
key = ''
for i in range(len(text1)):
    key += chr(randint(0,5000))
print(key)
```

[illegible]

Figure 2: Исходные данные

- Осуществляем шифрование двух текстов по ключу с помощью написанной функции

```
cipher1 = cript(text1, key)
cipher2 = cript(text2, key)
print(cipher1, cipher2, sep="\n")
```

```
xی³ۅفيHLٳحCԳủထ໑ঝ·ɔब˺H
xیئص´˝ètحCF▯ლo·ئजگH
```

Figure 3: Шифрование данных

Выполнение лабораторной работы

- Создаём переменную, которая, прогнав два шифрованных текста через побитовый XOR, поможет злоумышленнику получить один текст, зная другой, без ключа

Выполнение лабораторной работы

- Таким же способом можно получить часть данных

```
In [35]: text2[7:15]
Out[35]: 'рождения'

In [29]: zlo_part = cript(cipher1[7:15], cipher2[7:15])
         print(cript(zlo_part, text2[7:15]))
          годом,
```

Figure 4: Получение части данных

Выводы

Я освоила на практике применение режима однократного гаммирования при работе с несколькими текстами.