Лабораторная работа №7

Информационная безопасность

Банникова Екатерина Алексеевна

Содержание

1	Цель работы	5
2	Теоретическое введение	6
3	Выполнение лабораторной работы	7
4	Выводы	ç

Список иллюстраций

3.1	Функция шифрования	7
3.2	Исходные данные	7
3.3	Результат работы программы	8

Список таблиц

1 Цель работы

Освоить основы шифрования через однократное гаммирование

2 Теоретическое введение

3 Выполнение лабораторной работы

Лабораторная выполнена на языке Python 3 в среде Jupiter Notebook. Создаем функцию, которая осуществляет однократное гаммирование посредством побитового XOR

```
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
```

Рис. 3.1: Функция шифрования

Задаем текстовую строку и создаем случайный символьный ключ такой длины

```
text = 'C Новым годом, друзья!'

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

tlestv__'Tean
```

Рис. 3.2: 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. Все эти действия осуществляются через одну и ту же функцию

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

Print(cipher)

Print(cript(cipher, key))

С Новым годом, друзья!

print(cript(text, cipher))

Theasy are a cript(text, cipher)
```

Рис. 3.3: Результат работы программы

4 Выводы

Я освоила на практике применение режима однократного гаммирования.