Лабораторная работа №7

Основы информационной безопасности

Балакирева Дарья Сергеевна

19 октября 2022

Российский университет дружбы народов, Москва, Россия

НПМбд-01-19б

Элементы криптографии.

Однократное гаммирование

Цель лабораторной работы

- Получить практические навыки по работе с однократным гаммированием

Задачи лабораторной работы

- Написать функцию шифровки и дешифровки данных в режиме однократного гаммирования
- Определить вид шифротекста при известном ключе и открытом тексте
- Определить ключ, преобразующий шифротекст в один из вариантов прочтения открытого текста

Ход лабораторной работы

Гаммирование представляет собой наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных. Иными словами, наложение гаммы — это сложение её элементов с элементами открытого (закрытого) текста по некоторому фиксированному модулю, значение которого представляет собой известную часть алгоритма шифрования.

Функция шифрования

Создаём функцию, которая осуществляет однократное гаммирование посредством побитового XOR

```
def cript(text,key):
    if len(text) != len(key):
        return " Ошибка: ключь должен быть той же длины, что и текст"
    result = ''
    for i in range(len(key)):
        n = ord(text[i] ^ ord(key[i]))
        result += chr(n)
        return result
```

Figure 1: Функция

Исходные данные

Задаём текстовую строку и создаём случайный символьный ключ такой же 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)
```

Figure 2: Исходные данные

Результат работы программы

- 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.

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

[illegible]

```
print(cript(shifr, key))
```

```
С Новым годом,друзья!
```

```
print(cript(text, shifr))
```

[illegible]

Выводы

- Освоено на практике применение режима однократного гаммирования