Лабораторная работа №7

Основы информационной безопасности

Серёгина Ирина Андреевна

11 мая 2024

Российский университет дружбы народов, Москва, Россия

Цель работы

Освоить на практике применение режима однократного гаммирования.

Задание

Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение должно: 1. Определить вид шифротекста при известном ключе и известном открытом тексте. 2. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

Выполнение лабораторной работы

1. Для начала создаю функцию, которая будет генерировать случайный ключ (рис. 1).

```
def hex_key_gen(text):
    key = ''
    for i in range(len(text)):
        key += random.choice(string.ascii_letters + string.digits)
    return key
```

Figure 1: генерация случайного ключа

2. Затем пишу функцию для шифрования и дешифрования текста (рис. 2).

```
def crypt(text,key):
    new_text = ''
    for i in range(len(text)):
        new_text += chr(ord(text[i]) ^ ord(key[i % len(key)]))
    return new_text
```

Figure 2: шифрование текста

3. После пишу функцию, которая будет находить различные возможные ключи для определенного фрагмента, с помощью которых

шифротекст может быть преобразован в фрагмент (рис. 3).

```
def find_key(text, fragment):
    possible_keys = []
    for i in range(len(text) - len(fragment) + 1):
        possible_key = ""
        for j in range(len(fragment)):
            possible_key += chr(ord(text[i+j]) ^ ord(fragment[j]))
        possible_keys.append(possible_key)
    return possible_keys
```

Figure 3: поиск ключей

4. После этого проверяю работу всех функций, все работает корректно (рис. 4).

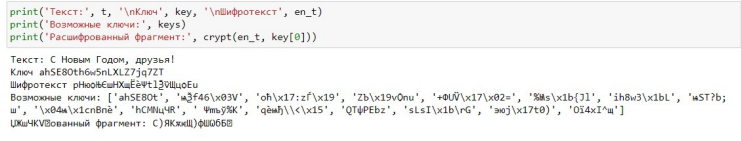

Figure 4: проверка работы кода

Выводы

Я освоила на практике применение режима однократного гаммирования.

Спасибо за внимание!