Отчет по лабораторной работе №7

Астафьева Анна Андреевна НПИбд-01-18¹ Информационная Безопасность—2021, 7 декабря, 2021, Москва, Россия

¹Российский Университет Дружбы Народов

Цели и задачи работы

Цель лабораторной работы

Освоить на практике применение режима однократного гаммирования.

Задание к лабораторной работе

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.

лабораторной работы

Процесс выполнения

1. Написана функция *encryption*, которая с помощью однократного гаммирования из сообщения и ключа получает шифротекст (рис. 1).

```
def encryption (message, key):
    cypher=[]
    cypher_1=[]
    if len(message)>len(key):
        for _ in range(len(message)-len(key)):
            key.append('00')
    for i, j in zip(message, key):
        c = hex(int(i,16)^int(j,16))[2:]
        c = (c, '0'+c)[len(c)==1]
        cypher.append(c)
        cypher_1.append(chr(int(i,16)^int(j,16)))
    return cypher, cypher_1
```

Рис. 1: Код функции encryption

2. Написана функция *gen_key*, генерирующая случайный ключ (рис. 2).

```
from random import randrange

def gen_key (lenght):
    key=[]
    for _ in range(lenght):
        temp=randrange(256)
        temp=hex(temp)[2:]
        key.append((temp, '0'+temp)[len(temp)==1])
    return ' '.join(key)

#print(gen_key(20))
```

Рис. 2: Код функции gen_key

3. Написана функция *to_hex*, трансформирующая текст в шестнадцатиричное представление (рис. 3).

```
def to_hex (text):
    hexa=[]
    for i in text:
        hexa.append(hex(ord(i))[2:])
    return hexa
```

Рис. 3: Код функции *to_hex*

4. Определяю вид шифротекста при известном ключе и известном открытом тексте. Применяю к шифротексту ключ снова, чтобы получить исходное сообщение (рис. 4).

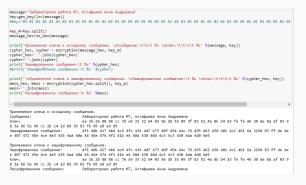


Рис. 4: Получение шифротекста

5. Пробую расшифровать шифротекст с помощью неправильного ключа(рис. 5).

Рис. 5: Применение неправильного ключа

6. Определяю ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста (Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!»)(рис. 6).

```
test='C Hosem rodom, dovaes!'
new key hex, new key-encryption(cypher hex,split(), to hex(test))
test key=' '.join(new key hex)
print('\nПодбор ключа, \nЗацифорванное сообщение:\t %s \nTectoвый ключ:\t\t\t %s' %(cycher hex, test key))
test key=test_key.split()
mess_hex, mess - encryption(cypher_hex.split(), test_key)
mess="'.join(mess)
print('Возможное сообщение:\t\t %s' %mess)
Подбор ключа.
Зашифрованное сообцение:
                               457 453 4c4 4ef 40f 471 435 4f3 428 457 47f 4d3 e8 478 473 439 494 490 44e 24 2108 81 98 d2 42
0 49b 49a 4e7 4bb 446 4c5 414 46f d3 4d1 4d5 45f 45e 9c 469 470 4d3 438 447 4a8 4b4 42f 4bd
Тестовый ключ:
                                76 473 d9 d1 3d 3a 89 4d3 1b 69 4b ed 4d4 454 453 8d d4 d3 79 468 2547 x8 9R d2 428 49x 49x 49x 49x
7 4bb 446 4c5 414 46f d3 4d1 4d5 45f 45e 9c 469 470 4d3 438 447 4a8 4b4 42f 4bd
                          С Новым годом, друзья!
Возможное сообщение:
```

Рис. 6: Один из вариантов прочтения шифротекста

Контрольные вопросы

Контрольные вопросы

- 1. Поясните смысл однократного гаммирования.
- 2. Перечислите недостатки однократного гаммирования.
- 3. Перечислите преимущества однократного гаммирования.
- 4. Почему длина открытого текста должна совпадать с длиной ключа?

Контрольные вопросы

- 5. Какая операция используется в режиме однократного гаммирования, назовите её особенности?
- 6. Как по открытому тексту и ключу получить шифротекст?
- 7. Как по открытому тексту и шифротексту получить ключ?
- 8. В чём заключаются необходимые и достаточные условия абсолютной стойкости шифра?

Выводы по проделанной работе

Вывод

На основе проделанной работы освоила на практике применение режима однократного гаммирования.