Отчет по лабораторной работе №7

Коломиец Мария Владимировна НПИбд-01-18[1]

Информационная Безопасность–2021, 7 декабря, 2021, Москва, Россия

[1]Российский 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.

Процесс выполнения лабораторной работы

Процесс выполнения

1. Написана функция *to_hex*, трансформирующая текст в шестнадцатиричное представление (рис. 1).

```
In [1]: def to_hex (text):
            hexa=[]
            for i in text:
                hexa.append(hex(ord(i))[2:])
            return hexa
```

Рис. 1: Код функции *to_hex*

Процесс выполнения

2. Написана функция *encryption*, которая с помощью однократного гаммирования из сообщения и ключа получает шифротекст (рис. 2).

```
In [2]: def encryption1 (message, key):
            cypher=[]
            cypher_1=[]
            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. 2: Код функции *encryption*

Процесс выполнения

3.Написана функция *gen_key*, генерирующая случайный ключ (рис. 3).

In [3]:
```
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(22))
```

Рис. 3: Код функции *gen_key*

Процесс выполнения

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

```
In [4]: message='Лабораторная работа №7, Коломиец Мария Владимировна'
        #key='01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01'
        key=gen_key(len(message))
        #key = ' '.join(to_hex('КоломиецМарияВладимировна'))

        print('Применение ключа к исходному сообщению.\nСообщение:\t\t\t %s \nКлюч:\t\t\t\t %s' %(message, key))
        key_m=key.split()
        message_hex = to_hex(message)

        cypher_hex, cypher=encryption1(message_hex, key_m)
        cypher=''.join(cypher)
        cypher_hex=' '.join(cypher_hex)
        #print('Зашифрованное сообщение:\t %s' %cypher)
        print('Зашифрованное сообщение:\t %s' %cypher_hex)

        print('\n\nПрименение ключа к зашифрованному сообщению.\nЗашифрованное сообщение:\t %s \nКлюч:\t\t\t\t %s' %(cypher_
        mess_hex, mess=encryption1(cypher_hex.split(), key_m)
        mess=''.join(mess)
        print('Расшифрованное сообщение:\t %s' %mess)

Применение ключа к исходному сообщению.
Сообщение:                      Лабораторная работа №7, Коломиец Мария Владимировна
Ключ:                           ac 4f 3e 15 3d 0f 18 0f e1 23 22 bb ab 1d c9 00 a4 7d 7d cc ab 25 1d 29 67 bd 47 4
6 79 f6 f3 1f 5a 18 c0 4a a4 33 23 22 81 42 f0 90 87 24 b4 bd 39 66 48
Зашифрованное сообщение:        4b7 47f 40f 42b 47d 43f 45a 431 4a1 41e 412 4f4 8b 45d 4f9 431 49a 43f 44d ec 21bd
12 31 09 47d 483 47c 478 445 4ce 4c6 459 7a 404 4f0 40a 49c 47c 03 430 4ba 472 4c4 4a8 4bb 41c 4f4 483 40b 45b 478


Применение ключа к зашифрованному сообщению.
Зашифрованное сообщение:        4b7 47f 40f 42b 47d 43f 45a 431 4a1 41e 412 4f4 8b 45d 4f9 431 49a 43f 44d ec 21bd
12 31 09 47d 483 47c 478 445 4ce 4c6 459 7a 404 4f0 40a 49c 47c 03 430 4ba 472 4c4 4a8 4bb 41c 4f4 483 40b 45b 478
Ключ:                           ac 4f 3e 15 3d 0f 18 0f e1 23 22 bb ab 1d c9 00 a4 7d 7d cc ab 25 1d 29 67 bd 47 4
6 79 f6 f3 1f 5a 18 c0 4a a4 33 23 22 81 42 f0 90 87 24 b4 bd 39 66 48
Расшифрованное сообщение:       Лабораторная работа №7, Коломиец Мария Владимировна
```

Рис. 4: Получение шифротекста

Процесс выполнения

5. 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. 5).

```
In [5]: test='С Новым годом, друзья!'
        new_key_hex, new_key = encryption1(cypher_hex.split(), to_hex(test))

In [6]: test_key=' '.join(new_key_hex)
        test_key=test_key.split()
        print('Подбор ключа.\nЗашифрованное сообщение:\t %s \nТестовый ключ:\t\t\t %s' %(cypher_hex, key))
        mess_hex, mess=encryption1(cypher_hex.split(), test_key)
        mess=''.join(mess)
        print('Возможное сообщение:\t\t %s' %mess)

        Подбор ключа.
        Зашифрованное сообщение:         4b7 47f 40f 42b 47d 43f 45a 431 4a1 41e 412 4f4 8b 45d 4f9 431 49a 43f 44d ec 21bd
        12 31 09 47d 483 47c 478 445 4ce 4c6 459 7a 404 4f0 40a 49c 47c 03 430 4ba 472 4c4 4a8 4bb 41c 4f4 483 40b 45b 478
        Тестовый ключ:                   ac 4f 3e 15 3d 0f 18 0f e1 23 22 bb ab 1d c9 00 a4 7d 7d cc ab 25 1d 29 67 bd 47 4
        6 79 f6 f3 1f 5a 18 c0 4a a4 33 23 22 81 42 f0 90 87 24 b4 bd 39 66 48
        Возможное сообщение:             С Новым годом, друзья!
```

Рис. 5: Один из вариантов прочтения шифротекста

Выводы по проделанной работе

Вывод

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

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?