Отчёт по лабораторной работе 7

Радимов Игорь

Цель работы

Освоить на практике применение режима однократного гаммирования.

Задание

Лабораторная работа подразумевает использование языков программирования для создания программы для щифрования и дещифрования в режиме однократного гаммирования.

Выполнение лабораторной работы

Выполнение лабораторной работы

1. Импортируем библиотеки random,string. Зададим строковую переменную text.

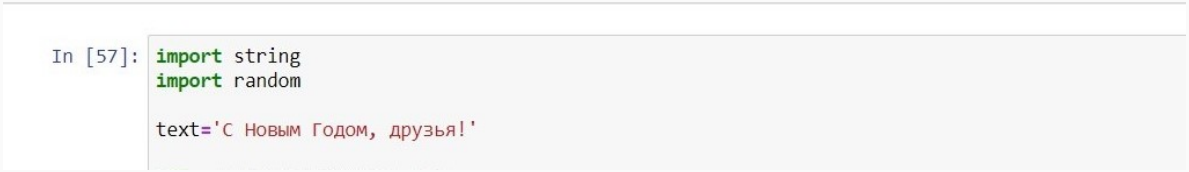

Figure 1: рис.1. Импорт библиотек.

2. Зададим генератор ключа и напечатаем ключ по этой строке.

```
def generator(length,abc):
    return ''.join(random.choice(abc) for i in range(length))
abc=string.ascii_letters.join(string.digits)
key=generator(len(text),abc)
```

Figure 2: рис.2. Генератор ключа.

3. Зададим функцию для гаммирования, обнаружения ключа и дешифрования.

```
In [58]: def gamm(string,key):
             return ''.join(chr(n^m) for n,m in zip ([ord(i) for i in string ],[ord(i) for i in key]))

In [59]: txt1=gamm(text,key)   #закодированная строка
```

Figure 3: рис.3. Функция gamm.

4. Получим закодированную строку и её шестнадцатеричный вид. Попробуем подобрать ключ и увидим, что он неверный. Используем настоящий ключ и декодированную строку.

```
In [59]: txt1=gamm(text,key)   #закодированная строка

In [60]: key2=generator(len(txt1),abc)
         txt2=gamm(txt1,key2)
         txt2 #расшифрованная строка

Out[60]: "Ш8вжвwЩ\x18ЩвЌЇЊ\x1b'гwњкмь\x00"

In [61]: true_key=gamm(text,txt1)  #настоящий ключ

In [62]: gamm(txt1,true_key) #декодированная строка

Out[62]: 'С Новым Годом, друзья!'
```

Figure 4: рис.4.

Спасибо за внимание