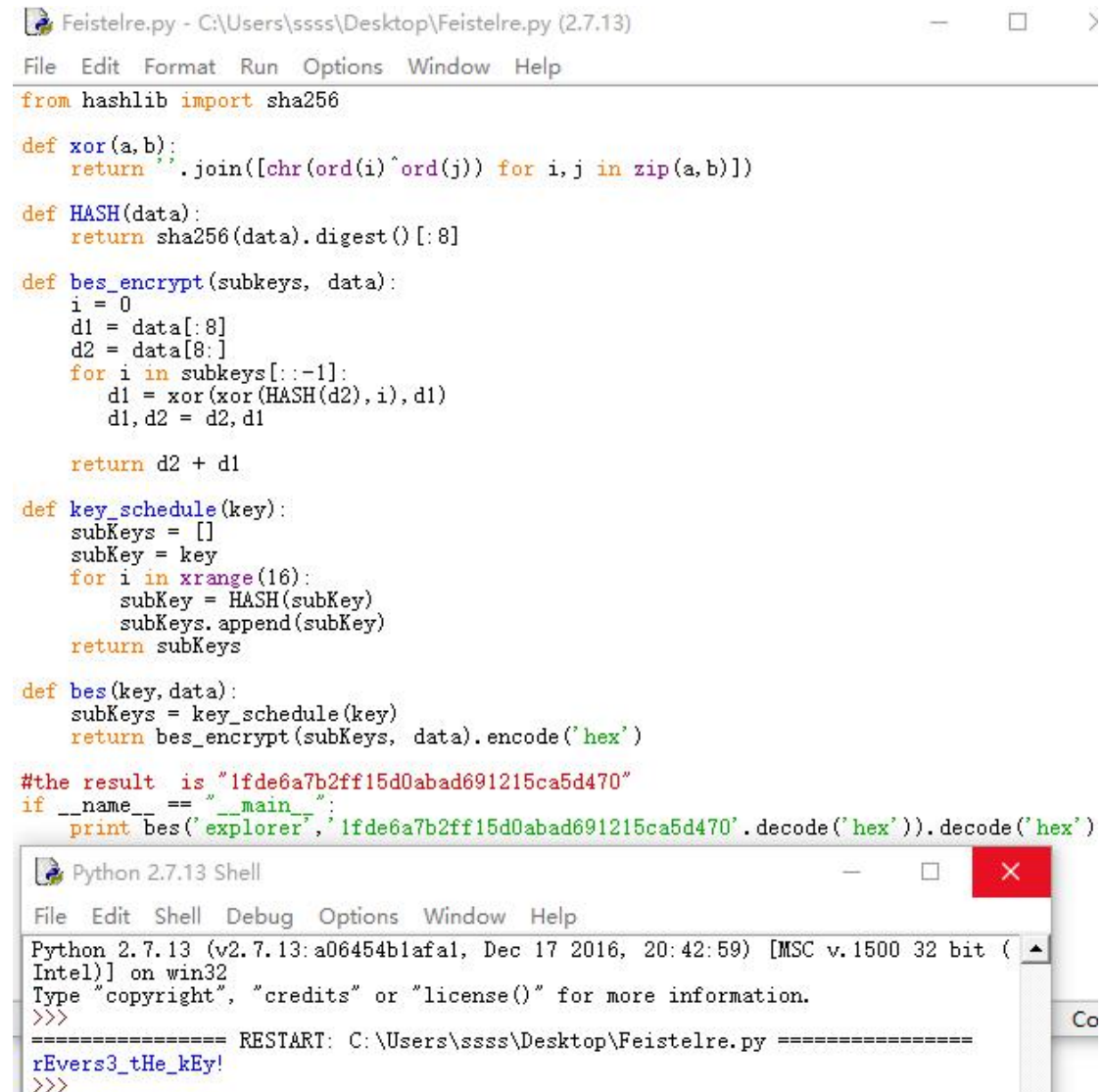


## explorer 的奇怪番外 3

Feistel 解密结构特点是将密文作为输入，以相反次序使用子密钥，既可以完成解密  
于是在源码中的 `for i in subkeys` 后加上 `::-1` 既能满足反次序使用子密钥的条件  
再在最后把密文作为输入再转换成 ASCII 码字符，将结果加上 `hctf{}` 即是 flag



```
Feistelre.py - C:\Users\ssss\Desktop\Feistelre.py (2.7.13)
File Edit Format Run Options Window Help

from hashlib import sha256

def xor(a,b):
    return ''.join([chr(ord(i)^ord(j)) for i,j in zip(a,b)])

def HASH(data):
    return sha256(data).digest()[:8]

def bes_encrypt(subkeys, data):
    i = 0
    d1 = data[:8]
    d2 = data[8:]
    for i in subkeys[::-1]:
        d1 = xor(xor(HASH(d2),i),d1)
        d1,d2 = d2,d1

    return d2 + d1

def key_schedule(key):
    subKeys = []
    subKey = key
    for i in xrange(16):
        subKey = HASH(subKey)
        subKeys.append(subKey)
    return subKeys

def bes(key, data):
    subKeys = key_schedule(key)
    return bes_encrypt(subKeys, data).encode('hex')

#the result is "1fde6a7b2ff15d0abad691215ca5d470"
if __name__ == "__main__":
    print bes('explorer', '1fde6a7b2ff15d0abad691215ca5d470'.decode('hex')).decode('hex')

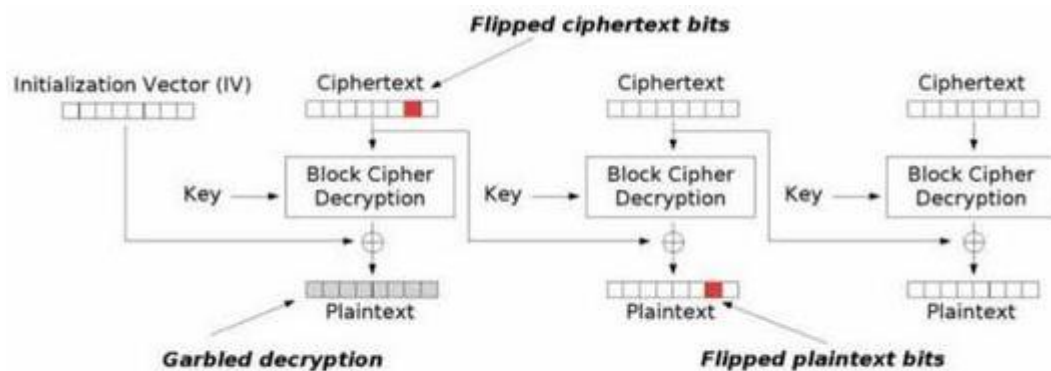
Python 2.7.13 Shell
File Edit Shell Debug Options Window Help
Python 2.7.13 (v2.7.13:a06454b1afaf, Dec 17 2016, 20:42:59) [MSC v.1500 32 bit (Intel)] on win32
Type "copyright", "credits" or "license()" for more information.
>>>
===== RESTART: C:\Users\ssss\Desktop\Feistelre.py =====
rEvers3_tHe_kEy!
>>>
```

## explorer 的奇怪番外 5

这道题我研究了很久，说下自己的理解（可能不对）

CBC 工作方式的特点是第一个块的字节会影响下一个块的字节（对应偏移量）

本题注册后弹出的 token 是由随机生成的 iv 和用户注册的数据加密成的密文组成，所以 iv 作为第一块，借用网上一张图



### Modification attack on CBC



题目必须要账号 admin 和密码 alvndasjncakslbdvlaksdn 登录才能弹出 flag，但是 admin 已经不能注册，所以可以想到改变 admin 中的某个字节，然后再改变弹出的 token 中对应的字节变成能通过管理员验证的 token，这里我把 admin 改成 badmin



```

root@OldDog: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)

+++++
welcome to explorer's strange crypto
+++++
what do you want to do?
1.sign in
2.sing up
enter you choose:2
you name:badmin
you password:alvndasjncakslbdvlaksdn
here is you token: edacc8c7e12abc5346b9184dc2c522f9e99535b84c50a5343ba5edc901738
12d9a4438c1fdc63db9648af5eba3191261
  
```

这里的 ed 就对应我输入的 b，接下来我要修改 ed，先声明几个变量加以说明

Initialization Vector (IV)   
 iv:   
 iv\_: 修改后的 iv  
 c\_[0]: 经过解密后的 Ciphertext

因为  对应影响的是 ，根据亦或关系可得：

$c_{[0]} = iv_{[0]} \oplus 'b'$

$iv_{[0]} = 'a' \oplus c_{[0]} = iv_{[0]} \oplus 'a' \oplus 'b'$

通过 python 计算得到 ed 后修改的值

```

Python 2.7.13 Shell
File Edit Shell Debug Options
Python 2.7.13 (v2.7.13:a06454b1:
Intel) on win32
Type "copyright", "credits" or
>>> chr(0xed ^ ord('a') ^ ord('b'))
'\xee'
  
```

将 ed 修改成 ee 的 token 登录，弹出 flag

```
root@OldDog:~# nc 121.42.25.113 20002
+++++
      welcome to explorer's strange crypto
+++++
what do you want to do?
1.sign in
2.sing up
enter you choose:1
give me you token:eeacc8c7e12abc5346b9184dc2c522f9e99535b84c50a5343ba5edc9017381
2d9a4438c1fdc63db9648af5eba3191261
hctf{cRypT0_ls_1nteRestIng!}
```