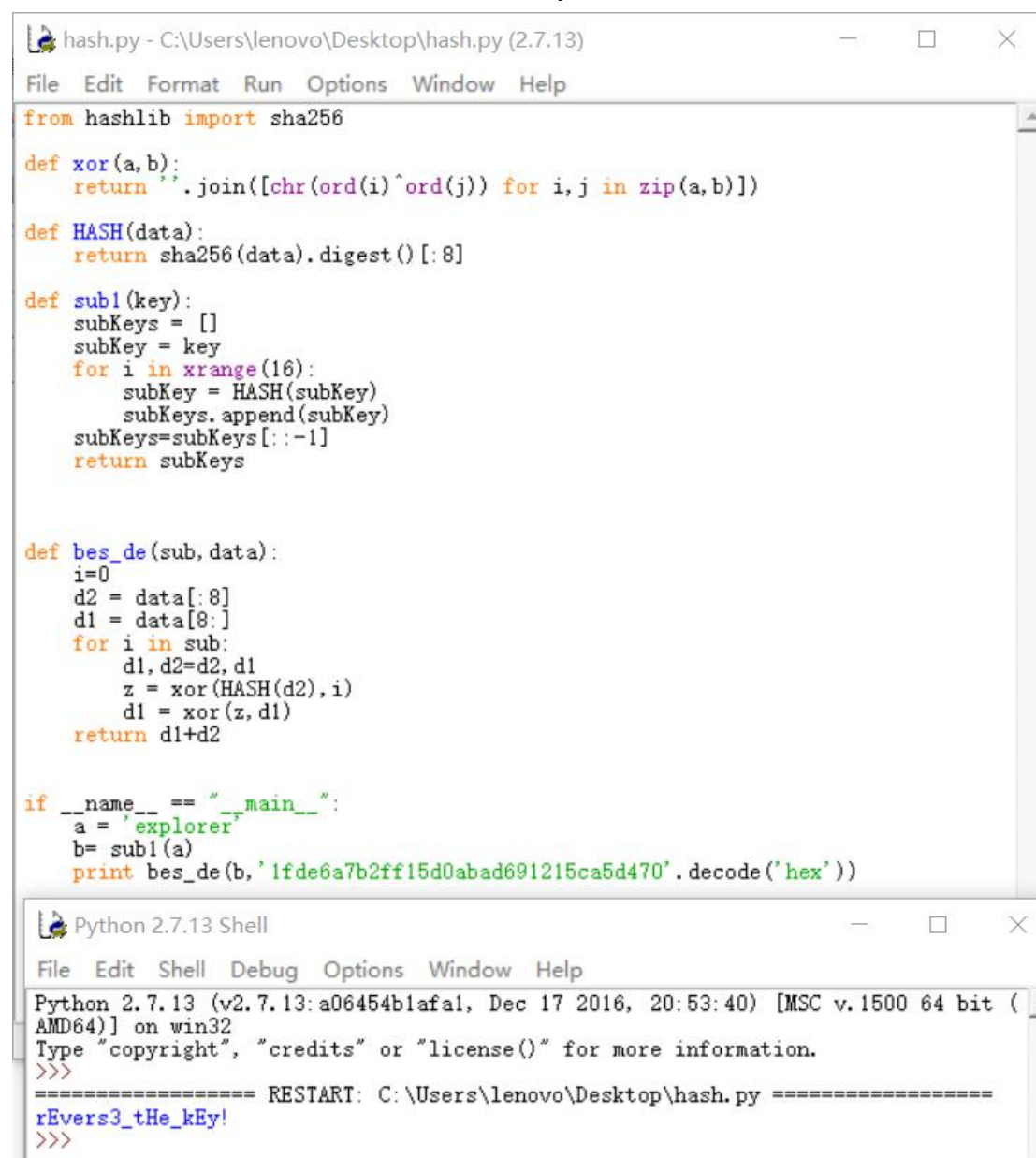


Week3

说实话，这周题好难，而且还没有时间做，好不爽 2333

explorer 的奇怪番外 3

因为有加密代码，看懂后反过来就好，写了点 Python 脚本



The image shows a screenshot of a Python script named 'hash.py' and its execution output in a shell window.

hash.py script:

```
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 sub1(key):
    subKeys = []
    subKey = key
    for i in xrange(16):
        subKey = HASH(subKey)
        subKeys.append(subKey)
    subKeys=subKeys[:-1]
    return subKeys

def bes_de(sub, data):
    i=0
    d2 = data[:8]
    d1 = data[8:]
    for i in sub:
        d1,d2=d2,d1
        z = xor(HASH(d2),i)
        d1 = xor(z,d1)
    return d1+d2

if __name__ == "__main__":
    a = 'explorer'
    b= sub1(a)
    print bes_de(b,'1fde6a7b2ff15d0abad691215ca5d470'.decode('hex'))
```

Python 2.7.13 Shell output:

```
Python 2.7.13 (v2.7.13:a06454blafal, Dec 17 2016, 20:53:40) [MSC v.1500 64 bit (AMD64)] on win32
Type "copyright", "credits" or "license()" for more information.
>>>
===== RESTART: C:\Users\lenovo\Desktop\hash.py =====
rEvers3_tHe_kEy!
>>>
```

Cbc 反转字节攻击

附上一个学习博客：

<http://zke1ev3n.me/2015/12/15/CBC%E5%AD%97%E8%8A%82%E5%8F%8D%E8%BD%AC%E6%94%BB%E5%87%BB/>

同样在看懂加密代码基础上进行攻击，原本不知道为什么改第一位，第一次改的密文，后来发现密文解密不受控制，只有解密后同第一组异或才可以控制，所以我先用 sdmin 申请 token，然后将 token 第一位跟 's' 异或再跟 'a' 异或，得到的 iv 再跟原密文解密出的字符异或后就可以成为我们想要的 'admin'

攻击：IV[0]=IV[0]^ORD('S')^ORD('A')

```
cbc2.py - C:\Users\lenovo\Desktop\cbc2.py (2.7.13)
File Edit Format Run Options Window Help
a = '127ebbae31f5340c5dcebd081f5f7f5f0897e6681e710efbfc32f409a70cb8149e5d9070fb0
b = a.decode('hex')
c = list(b)
c[0]=chr(ord(c[0])^ord('s')^ord('a'))
c = ''.join(c)
print c.encode('hex')
```

```
Python 2.7.13 Shell
File Edit Shell Debug Options Window Help
Python 2.7.13 (v2.7.13:a06454b1afaf, Dec 17 2016, 20:53:40) [MSC v.1500 64 bit (
AMD64)] on win32
Type "copyright", "credits" or "license()" for more information.
>>>
===== RESTART: C:\Users\lenovo\Desktop\hash.py =====
rEvers3_tHe_kEy!
>>>
===== RESTART: C:\Users\lenovo\Desktop\cbc2.py =====
007ebbae31f5340c5dcebd081f5f7f5f0897e6681e710efbfc32f409a70cb8149e5d9070fb0f026c
ae77264f57734d79
>>>
```

上交 token, 得到 flag

```
zhuyixuan@ubuntu: ~
zhuyixuan@ubuntu:~$ 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:007ebbae31f5340c5dcebd081f5f7f5f0897e6681e710efbfc32f409a70cb8149e5d9070fb0f026cae77264f57734d79
hctf{cRypT0_ls_1nteRestIng!}
zhuyixuan@ubuntu:~$
```