crypto.53 explorer的奇怪番外3

根据Feistel结构 只需要把k子密钥逆序作解密即可
修改得到相应py脚本

```
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_decrypt(subkeys, data):
    i = 0
    d1 = data[:8]
    d2 = data[8:]
    for i in subkeys:
       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)
    subKeys.reverse()
    return subKeys

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

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

hex转字符串 得到flag: rEvers3_tHe_kEy!

crypto.56 进击的 Crypto [0]

hint 流密码 s神助攻的b站链接av1269426
稍微理解点RC4
+参考hctf2015的WEB.server is done

F12看到Flag注释 128B
提交相同大小的M 得到C; 作M xor C 得到本次K;
令K xor Flag注释 得到flag明文

```
'UpZv))iw|?U?]RaA-@bR-X^)P#l@z3_z^Km,<B?UApSj|N9QgaIYEzw{9h!)Up4nT|d$!jsh{I&Gw/D
Ob3KK8*Jwq$}U/[_Fu,1%Ihcta{Rive5t_C1pher_4_6s_ez}'
```

还是出现了点小错误 ‘a’和’6’ 分别是 ‘f’和’1’
至于原因 应该是直接复制注释时有空字符 (有时复制出来还不是128B)

快结束才拿到flag也是慌= =

crypto.63 explorer的奇怪番外5

直接name输入admin就炸 改成advim passwd不变 得到toekn
写出相应脚本 目的把第3个字节 由 ‘v’ 改成 ‘m’

```
ciphertext =
'd0fac31498bd8dcd73e9cd66297f40331491548678ad6aa44408362c14999e1677e5c72d3460c9
5cdfb3920f498c559f'.decode('hex')
ciphertext = list(ciphertext)
ciphertext[2] = chr(ord(ciphertext[2]) ^ ord('v') ^ ord('m'))
ciphertext = ''.join(ciphertext)
ciphertext = ciphertext.encode('hex')

print ciphertext
```

得到admin的token 输入获得flag

```
vvv@vvv-virtual-machine:~$ nc -v 121.42.25.113 20002
Connection to 121.42.25.113 20002 port [tcp/*] succeeded!

++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
        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:d0fad81498bd8dcd73e9cd66297f40331491548678ad6aa44408362c14999e
1677e5c72d3460c95cdfb3920f498c559f
hctf{cRypT0_ls_1nteRestlng!}
vvv@vvv-virtual-machine:~$
```