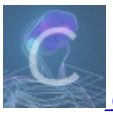
XCTF攻防世界 Normal_RSA

原创

CleanMe 于 2020-12-06 22:07:15 发布 2084 收藏 9

分类专栏： ctf crypto 文章标签： 加密解密



XCTF攻防世界 Normal_RSA

实验环境: windows 10

实验所需工具：
python工具:
yafu (可以在https://github.com/DarkenCode/yafu上下载)

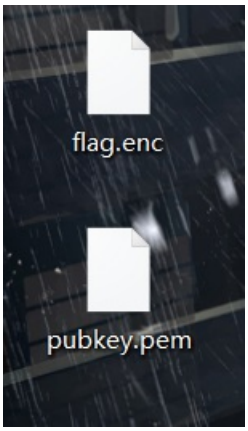
gmpy2 (直接pip install gmpy2即可)

rsa加密的相关知识可以看这两篇文章

http://www.ruanyifeng.com/blog/2013/06/rsa_algorithm_part_one.html

http://www.ruanyifeng.com/blog/2013/07/rsa_algorithm_part_two.html

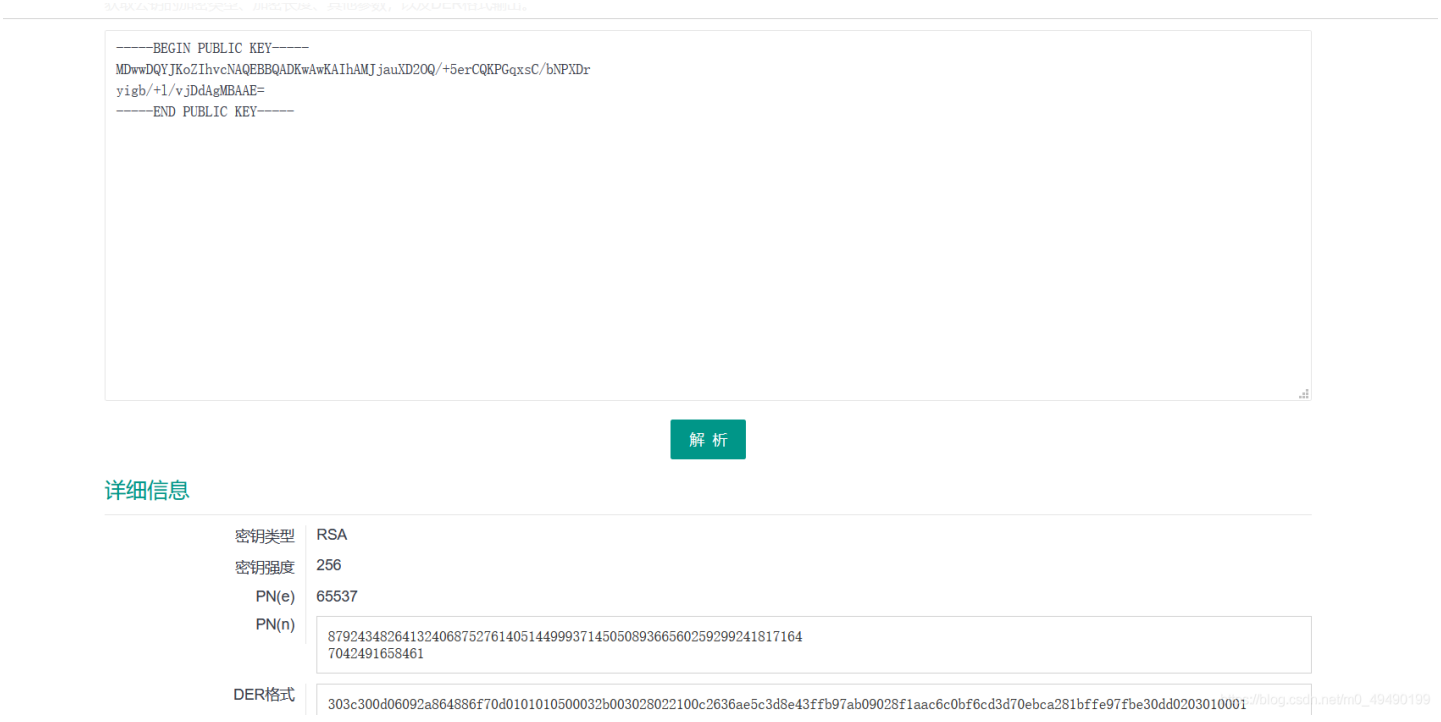
看题



题目给了这两个文件

flag.enc 是经过rsa加密后的密文, **pubkey.pem** 是rsa的公钥文件

可以用记事本打开pubkey.pem文件，把文件内容放到rsa解密网站上分析



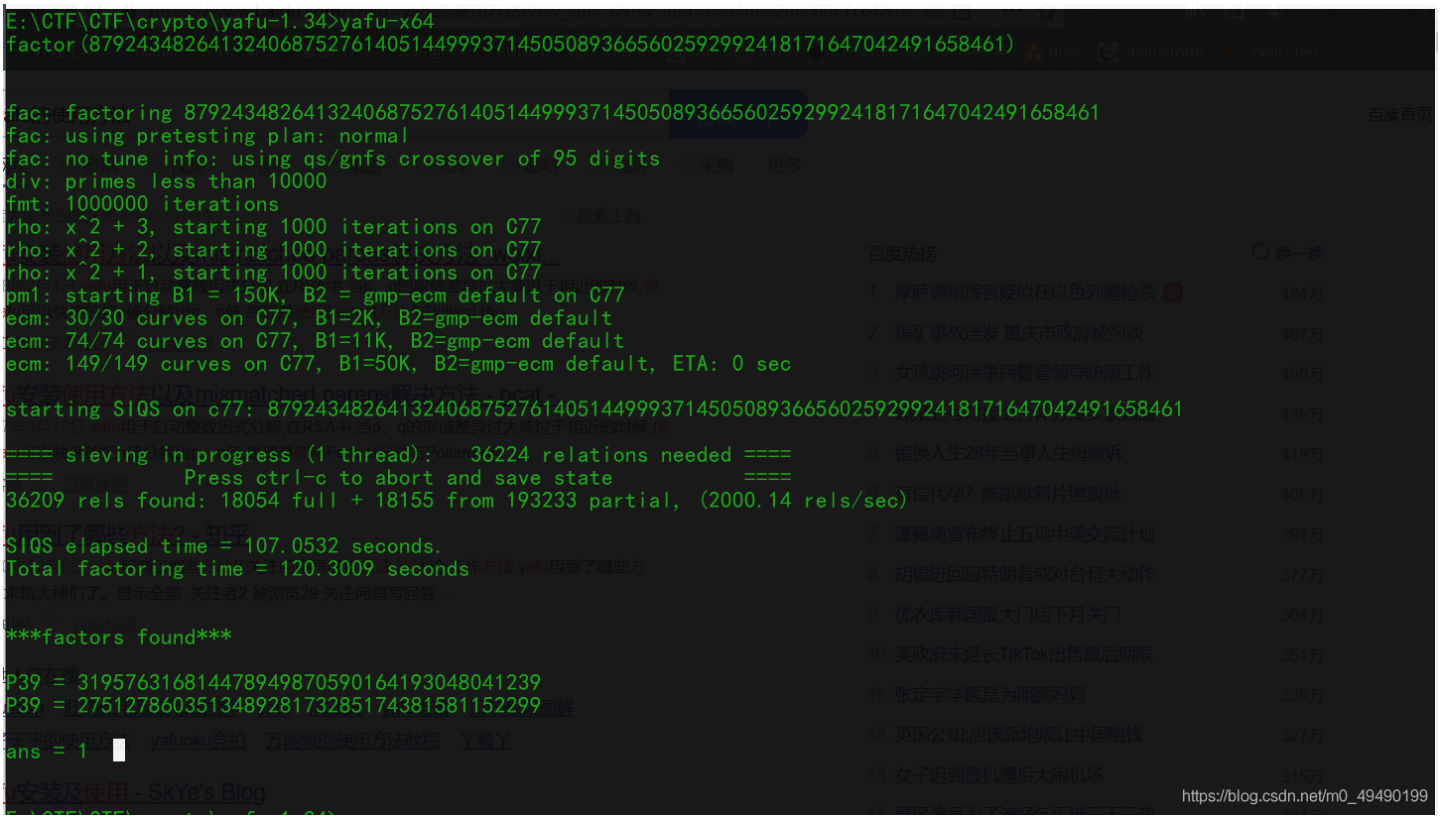
由此可知

```
n = 879243482641324068752761405144999371450508936656025929924181716470424916584617
e = 65537
```

使用yafu对n进行质因数分解，到yafu安装的文件目录输入yafu-x64使用

输入`factor(879243482641324068752761405144999371450508936656025929924181716470424916584 61)`

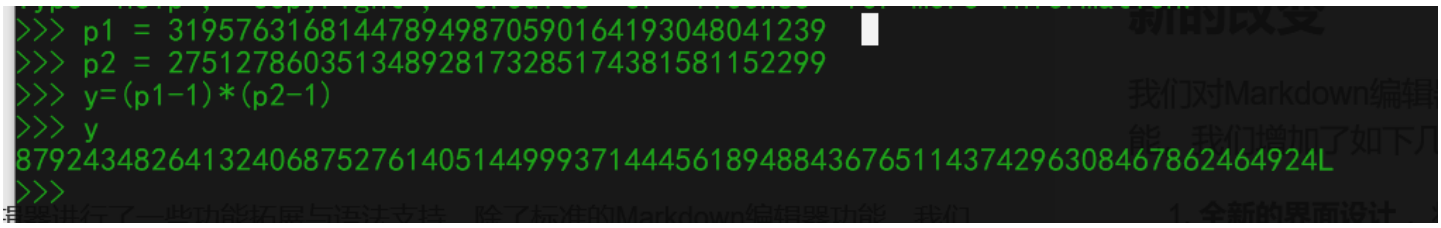
即可分解出质因数



其中的两个p39为分解出来的两个质因数

```
p1 = 319576316814478949870590164193048041239
p2 = 275127860351348928173285174381581152299
```

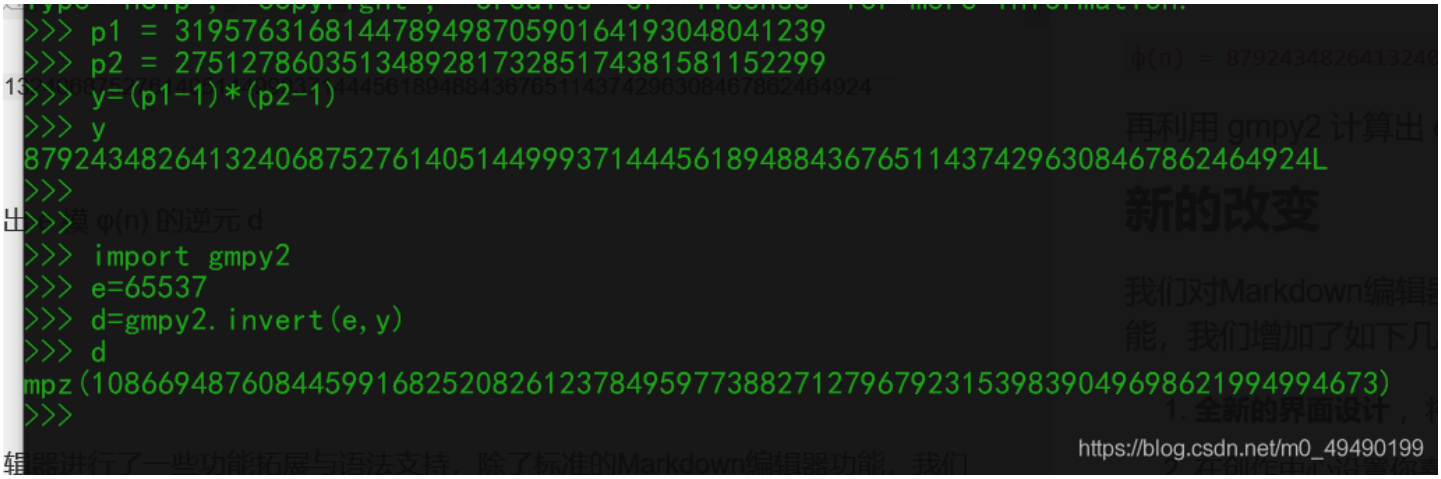
然后在计算n的欧拉函数`ϕ(n) = (p1-1)*(p2-1)`



`ϕ(n) = 879243482641324068752761405144999371444561894884367651143742963084678624649 24`

再利用 **gmpy2** 计算出 e 模 φ(n) 的逆元 **d**

gmpy2.invert()方法中第一个参数为 e ，第二个参数为 φ(n)，通过此方法计算可以得到 d



得到`d = 1086694876084459916825208261237849597738827127967923153983904969862199 4994673`

到这里，我们已经知道了

```
n = 879243482641324068752761405144999371450508936656025929924181716470424916584 61
e = 65537
d = 1086694876084459916825208261237849597738827127967923153983904969862199 4994673
```

看到好多文章中都用了 **rsatool** 这个工具 ，但是我安装总是会报错，也不知道是什么原因，现在都没安装好。。。

但是看了一下rsatool的作用是已知 **n,e,d** 和**密文文件** 可以进行解密得到从而得到**明文**

既然用不了rsatool，那就根据RSA加解密的原理来计算

设m为明文，c为密文，则RSA的加解密算法为

$$c= \quad m \quad \bmod n$$

密文**c**在flag.enc文件中，打开文件看到是这样的

```
m>·ß#îáÓ‡<0x10>¾ºx ‡Ž<0x0e>œe½=<0x08>ImÚd’A™<0x11><0x0c>y
```

但根据公式， c 需要为数字，那么就用16进制编码重新打开文件，得到了密文的16进制形式

```
6d3e b7df 23ee e1d3 8710 beba 78a0 878e
0e9c 65bd 3d08 496d da64 9241 9911 0c79
```

```
c = 0x6d3eb7df23eee1d38710beba78a0878e0e9c65bd3d08496dda64924199110c79
```

根据

$$m= \qquad c \quad \bmod n$$

现在已经得到了明文 **m** 的**16进制**形式
那么就可以把16进制转换为字符串，即可得到明文
但是又出现了一个问题，我放到在线网站上转换为字符串的时候，转换不出字符串

后来发现这串16进制的字符个数为奇数个，正常的话16进制的字符应该是由两个 **0~f** 的数组成，也就是这串16进制的字符数的个数一定是偶数

可以看到这一串字符串的长度为 64-2-1=61 是奇数(减2是因为最前面的0x，减1是因为最后面的L(表示长整型))
于是就把第一个字符删去，再转换为字符串

其中可见字符串即为**flag**