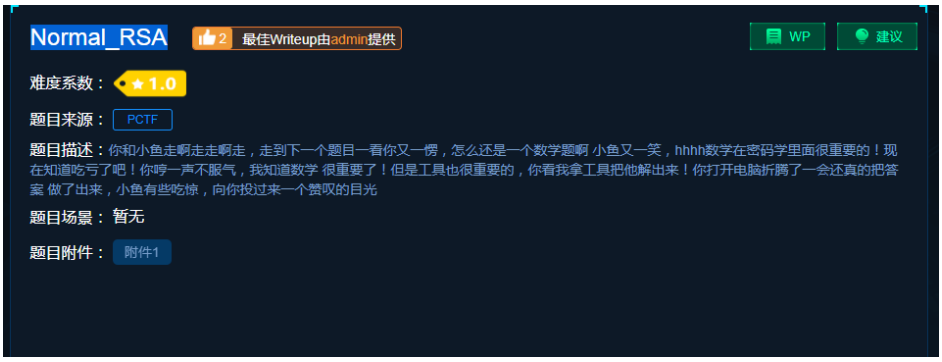
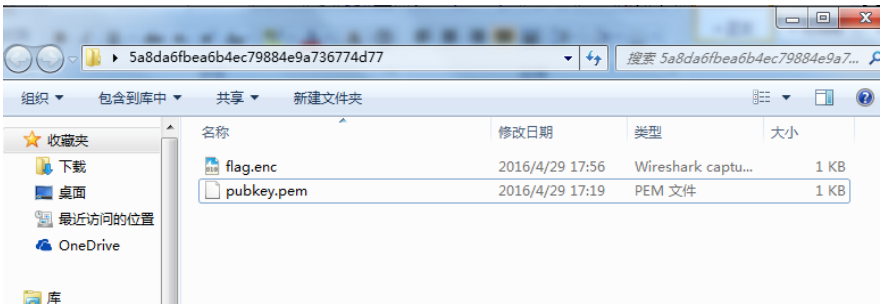
1、打开题目



下载附件看到两个文件



2、OpenSSL 使用 **PEM 文件格式存储证书和密钥**。PEM 实质上是 Base64 编码的二进制内容，再加上开始和结束行，如证书文件的

-----BEGIN CERTIFICATE-----

和

-----END CERTIFICATE-----

在这些标记外面可以有额外的信息，如编码内容的文字表示。文件是 ASCII 的，可以用任何文本编辑程序打开它们。

3、解题思路是：①使用 openssl 解密.pem 中参数 --> ②参数十六进制转换为十进制 --> ③利用 factor 对大整数进行分解，得到 p 和 q --> ④用 rsatool 生成私钥文件: private.pem --> ⑤用 private.pem 解密 flag.enc

接下来解题了

①使用 openssl 解密.pem 中参数。

Openssl 是 linux 自带的一个加密库，可以直接使用。

指令：openssl rsa -pubin -text -modulus -in warmup -in pubkey.pem

```
root@kali:~/Desktop#
root@kali:~/Desktop#
root@kali:~/Desktop# openssl rsa -pubin -text -modulus -in warmup -in pubkey.pem
Public-Key: (256 bit)
Modulus:
    00:c2:63:6a:e5:c3:d8:e4:3f:fb:97:ab:09:02:8f:
    1a:ac:6c:0b:f6:cd:3d:70:eb:ca:28:1b:ff:e9:7f:
    be:30:dd
Exponent: 65537 (0x10001)
Modulus=C2636AE5C3D8E43FFB97AB09028F1AAC6C0BF6CD3D70EBCA281BFFE97FBE30DD
writing RSA key
-----BEGIN PUBLIC KEY-----
MDwwDQYJKoZIhvcNAQEBBQADKwAwKAIhAMJjauXD20Q/+5erCQKPGqxsC/bNPXDr
yigb/+l/vjDdAgMBAAE=
-----END PUBLIC KEY-----
root@kali:~/Desktop#
```

②参数十六进制转换为十进制

Python 支持直接将 16 进制转换为 10 进制
Linux 下进入 python 命令行
0x C2636AE5C3D8E43FFB97AB09028F1AAC6C0BF6CD3D70EBCA281BFFE97FBE30DD

```
root@kali:~/Desktop# python
Python 2.7.11 (default, Jan 11 2016, 21:04:40)
[GCC 5.3.1 20160101] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> 0xC2636AE5C3D8E43FFB97AB09028F1AAC6C0BF6CD3D70EBCA281BFFE97FBE30DD
87924348264132406875276140514499937145050893665602592992418171647042491658461L
>>>
```

③利用 factor 对大整数进行分解，得到 p 和 q

在线大整数分解网站：http://www.factordb.com/

Search | Sequences | Report results | Factor tables | Status | Downloads | Login

8792434826413240687527614051449993714505089366560259299241817164704249165846 1 Factorize! (?)

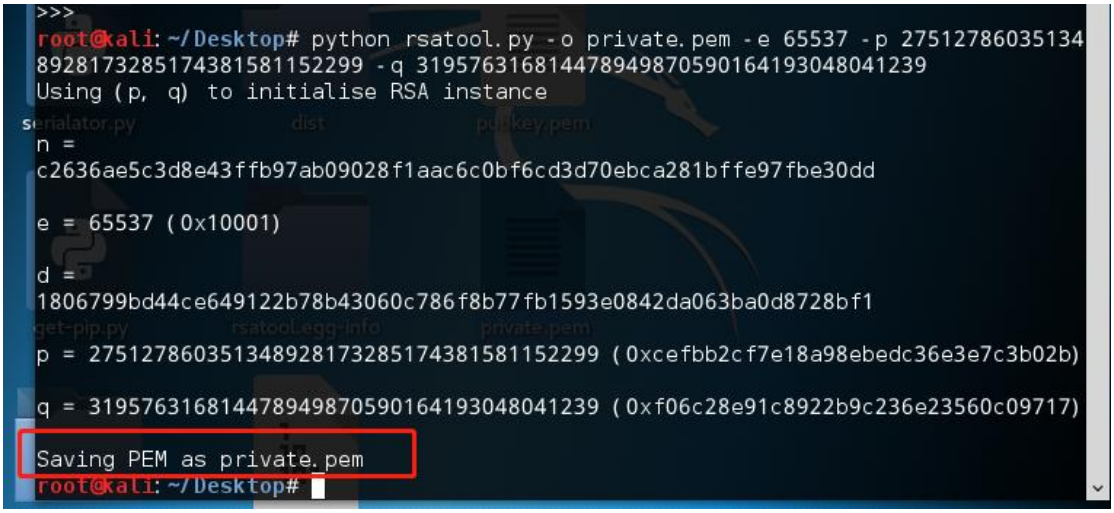
Result:

status (?)	digits	number
FF	77 (show)	8792434826...61<77> = 2751278603513489281732851743815811522 99<39> · 3195763168144789498705901641930480412 39<39>

More information

分解得到 p= 275127860351348928173285174381581152299
q= 319576316814478949870590164193048041239

④用 rsatool 生成私钥文件: private.pem
python rsatool.py -o private.pem -e 65537 -p XXX -q XXX



⑤用 private.pem 解密 flag.enc

openssl rsautl -decrypt -in flag.enc -inkey private.pem