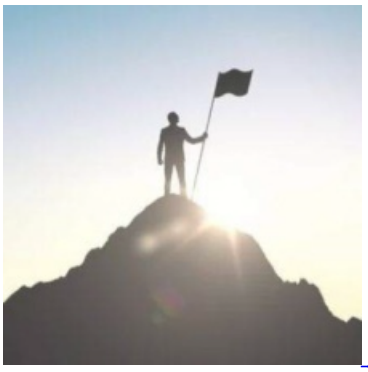
BUUCTF Reverse RSA

原创

A_dmins 于 2019-07-22 21:29:23 发布 962 收藏

分类专栏： CTF题 一天一道CTF BUUCTF

本文链接：https://blog.csdn.net/qq_42967398/article/details/96773826

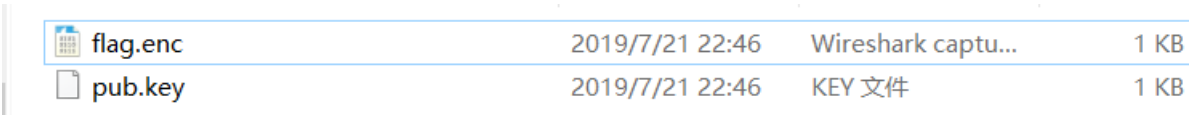


BUUCTF Reverse RSA

一天一道**CTF**，能多不能少

下载文件打开~

发现存在两个文件！！



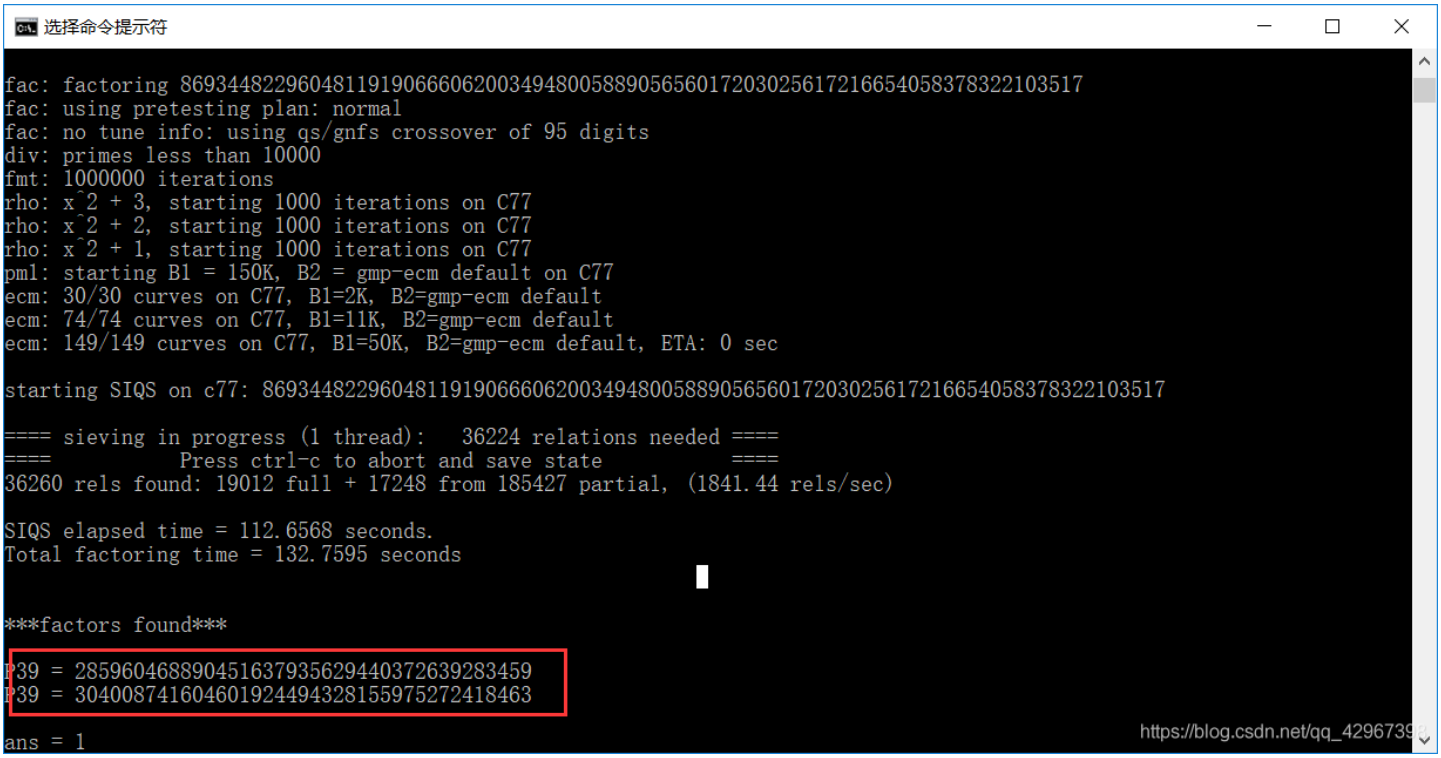
不用说，flag.enc肯定是加密后的，就不用看了，直接看pub.key，内容如下：

```
-----BEGIN PUBLIC KEY-----
MDwwDQYJKoZIhvcNAQEBBQADKwAwKAIhAMAzLFxkrkcYL2wch21CM2kQVFpY9+7+
/AvKr1rzQczdAgMBAAE=
-----END PUBLIC KEY-----
```

RSA的一个公钥？？？貌似是的！
直接利用在线工具分解公钥得到n和e：

密钥类型	RSA
密钥强度	256
PN(e)	65537
PN(n)	869344822960481191906660620034948005889056560172030256172166540583783221035 17
DER格式	303c300d06092a864886f70d0101010500032b003028022100c0332c5c64ae47182f6c1c876d42336910545a58f7eefefc0bcaaf5af341cddd0203010001

ok得到了n，那就可以分解n得到p和q了~~
利用yafu这个工具进行分解，得到p，q：



得到pq就好办了~
直接计算d，然后利用rsa模块生成私钥~
然后就可以直接对文件进行解密了~

```
import hashlib
import gmpy2
import rsa

p = 285960468890451637935629440372639283459
q = 304008741604601924494328155975272418463
e = 65537

n = 869344822960481191906660620034948005889056560172030256172166540583783221035l7

d = gmpy2.invert(e,(q-1)*(p-1))
print(d)

d = 81176168860169991027846870170527607562179635470395365333547868786951080991441

key = rsa.PrivateKey(n,e,d,p,q)
print(key)

with open("output\\flag.enc","rb") as f:
 print(rsa.decrypt(f.read(),key).decode())
```

得到：

```
81176168860169991027846870170527607562179635470395365333547868786951080991441
PrivateKey(869344822960481191906660620034948005889056560172030256172166540583783221035l7, 65537, 81176168860169991027846
870170527607562179635470395365333547868786951080991441, 285960468890451637935629440372639283459, 304008741604601924494328155975272418463)
flag{decrypt_256}
```

flag：`flag{decrypt_256}`

总结：

更深入的了解了RSA算法的奥秘~

同时也学会了yafu工具的使用，私钥生成函数的使用

利用rsa模块和gmpy2模块对RSA进行解密~

过程虽有坎坷，但还是能够跨越过去的！！！