crypto buuctf RSA1

原创

半杯雨水敬过客 于 2021-10-06 17:56:17 发布 108 收藏
文章标签： c++ python

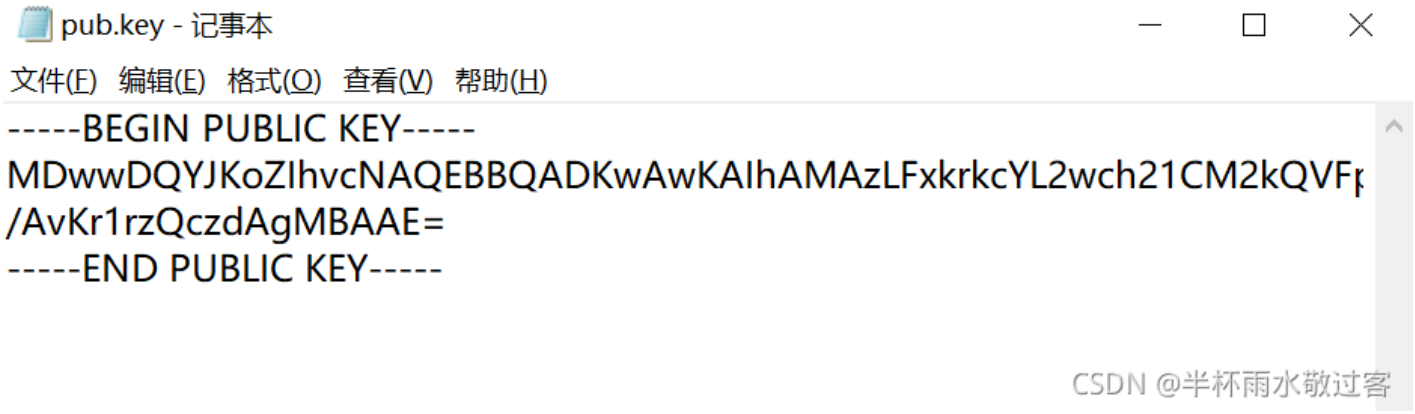
本文链接：https://blog.csdn.net/weixin_44214568/article/details/120627212

解压，一个是enc格式的文件，一个是Key格式的文件，

enc格式：enc是用Encore 软件制作的文件，用Adobe Encore 打开。是一个制作dvd的软件产生的格式。

key格式：key文件一般是用来注册或破解的文件，可以用记事本打开。

用记事本打开pub.key：

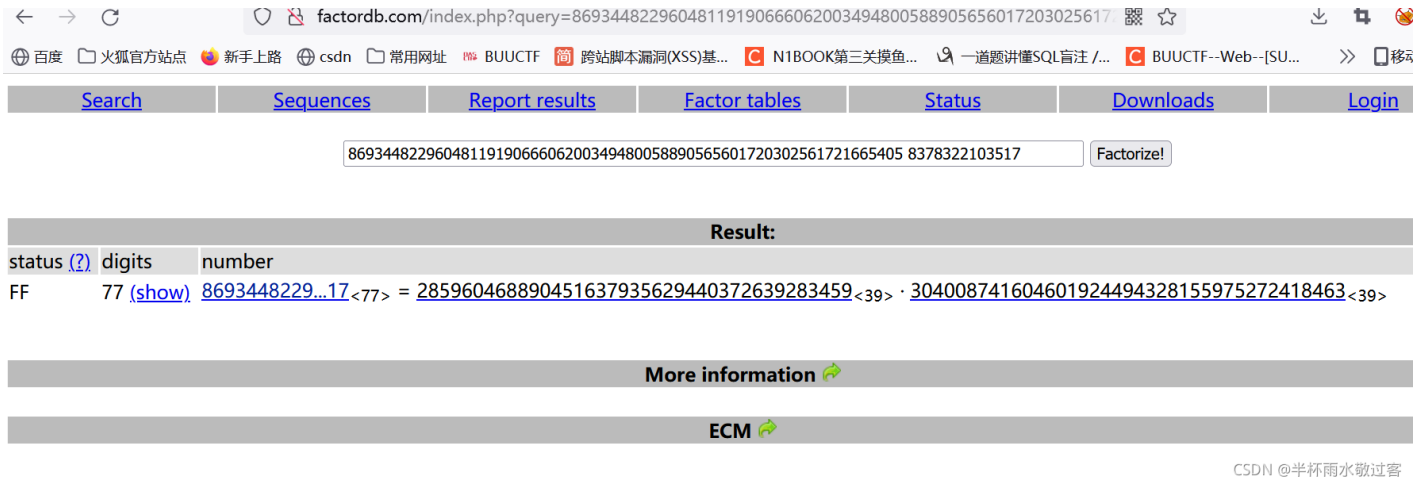


公钥文件，需要进行公钥解析SSL在线工具-公钥解析

计算出了e和n；

再需要解d；

对n进行分解：factordb.com

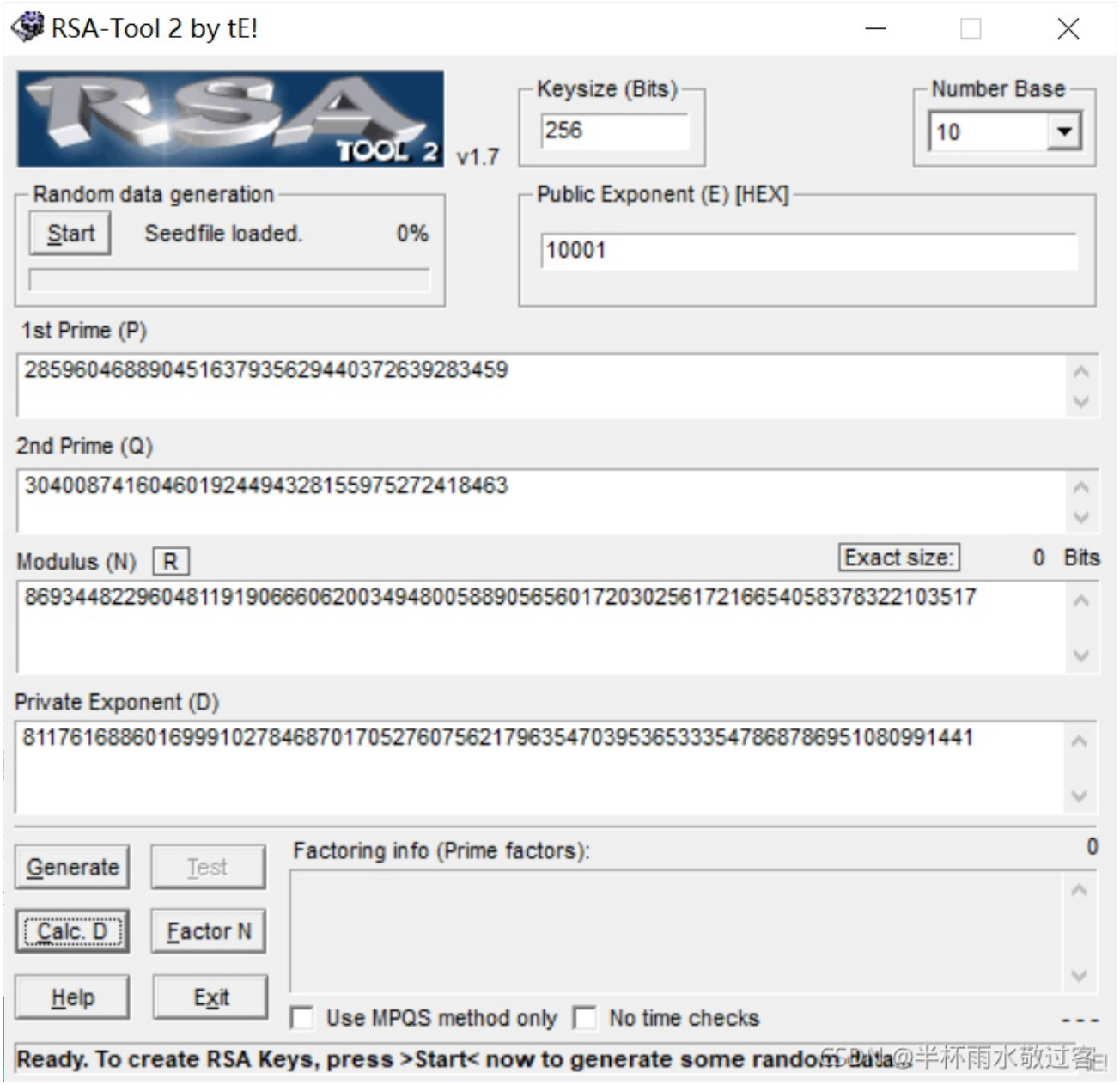


计算出p和q

p=285960468890451637935629440372639283459

q=304008741604601924494328155975272418463

求d:



再通过简单的脚本即可计算出：

脚本：

```
import rsa

e = 65537
n = 869344822960481191906660620034948005889056560172030256172166540583783221035 17
p = 285960468890451637935629440372639283459
q = 304008741604601924494328155975272418463
d = 811761688601699910278468701705276075621796354703953653335478687869510809914 41

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

with open("C:\\Users\\86155\\Desktop\\0eaf8d6c-3fe5-4549-9e81-94ac42535e7b\\flag.enc","rb+") as f:
     f = f.read()
     print(rsa.decrypt(f,key))
```

运行flag{decrypt_256}