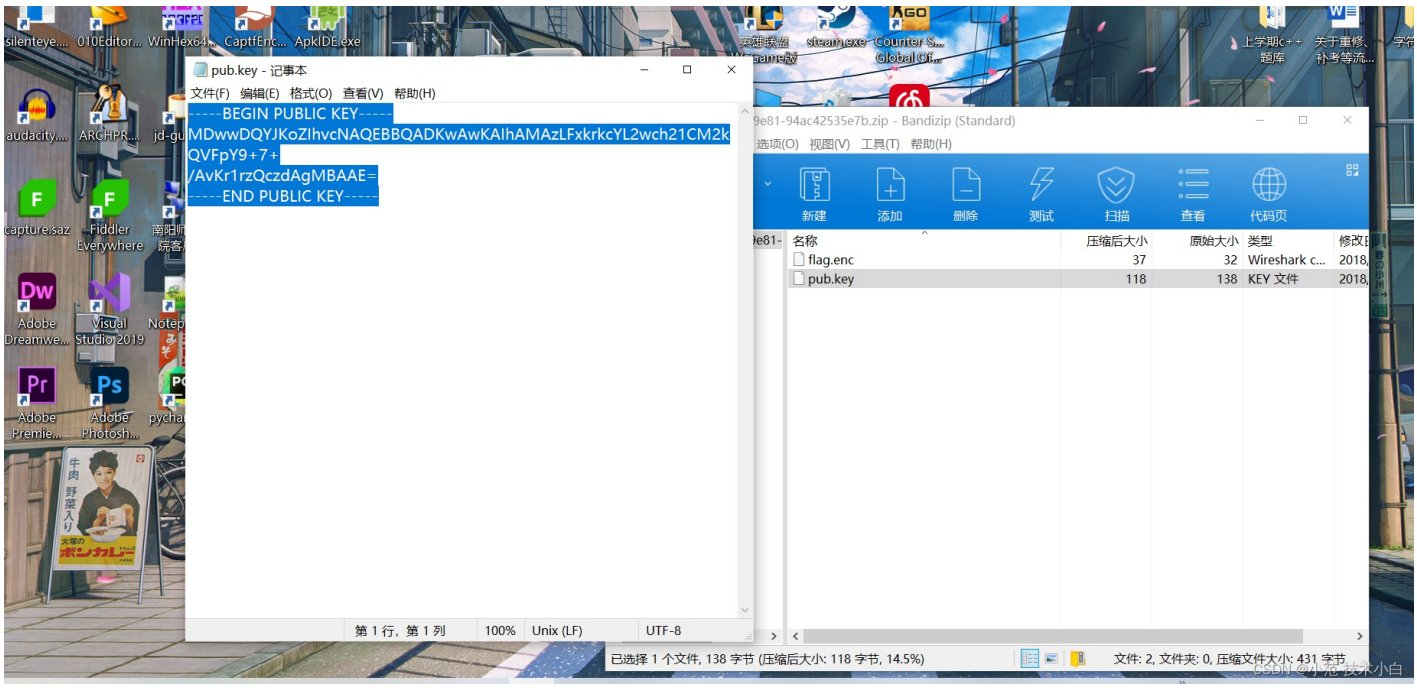
BUUCTF RSA

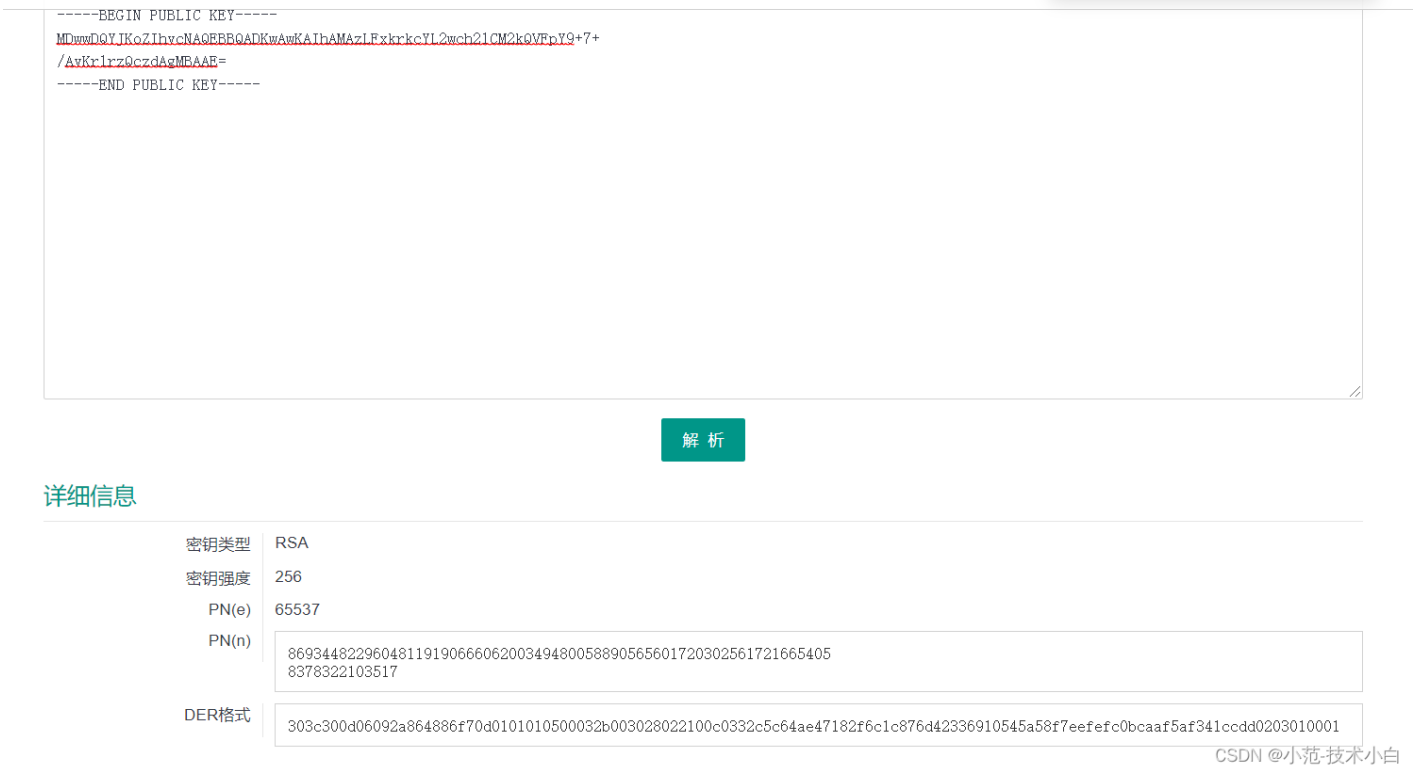
原创

小范-技术小白 于 2022-01-12 13:54:01 发布 21 收藏
分类专栏： CTF 文章标签： 服务器 运维

打开压缩文件后

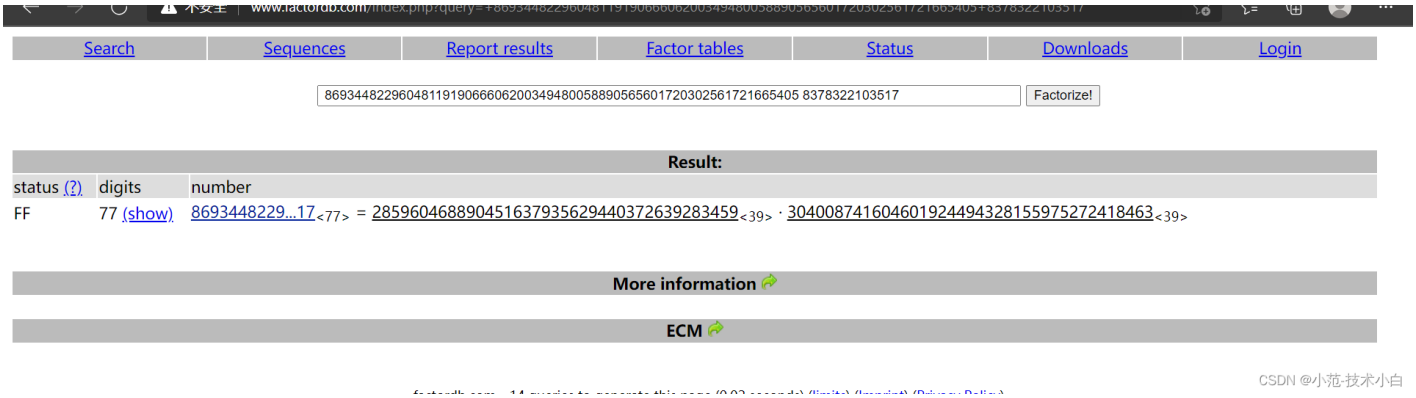


然后进行公钥解析



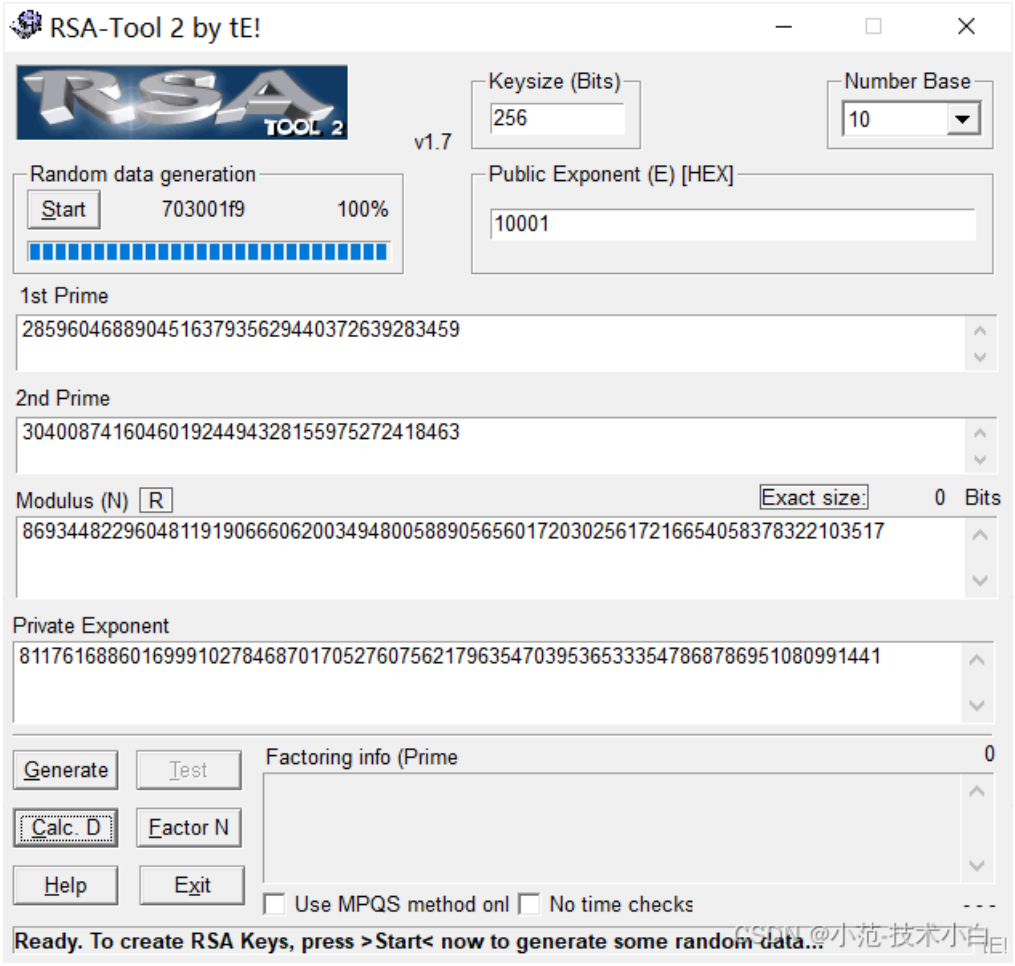
CSDN @小范-技术小白

分解质因数n



CSDN @小范-技术小白

然后由工具得d



最后拿出我珍藏已久的脚本

```
import rsa

e= 65537
n= 869344822960481191906660620034948005889056560172030256172166540583783221035 17
p= 285960468890451637935629440372639283459
q= 304008741604601924494328155975272418463
d= 811761688601699102784687017052760756217963547039536533354786878695108099144 1

key = rsa.PrivateKey(n,e,d,p,q)          #在pkcs标准中,pkcs#1规定,私钥包含(n,e,d,p,q)

with open("H:\\flag.text","rb") as f:  #以二进制读模式，读取密文
    f = f.read()
    print(rsa.decrypt(f,key))            # f:公钥加密结果   key:私钥
```

得flag