BUUCTF Reverse rsa WriteUp

原创

PlumpBoy 于 2021-09-11 16:15:05 发布 44 收藏

分类专栏： BUUCTF 逆向题解 文章标签： php 系统安全 安全

本文链接：https://blog.csdn.net/weixin_45723661/article/details/120228104

rsa-WP

打开文件，发现有有两个文件，拖入HxD发现一个是公钥一个是密文，那么本题的目标就是求解私钥进行解密。

先将公钥放入在线工具：http://ctf.ssleye.com/pub_asys.html

息

密钥类型	RSA
密钥强度	256
PN(e)	65537
PN(n)	869344822960481191906660620034948005889056560172030256172166540583783221035178378322103517
DER格式	303c300d06092a864886f70d0101010500032b003028022100c0332c5c64ae47182f6c1c876d42336910545a58f7eefefc0bcaaf5af341ccdd0203010001

解析得到

```
e=65537
n=869344822960481191906660620034948005889056560172030256172166540583783221035178378322103517
```

然后打开RSA-Tool2，将n填入n处，点击Factor N即可分解，但是大数分解特别慢，建议使用在线工具：http://factordb.com/index.php

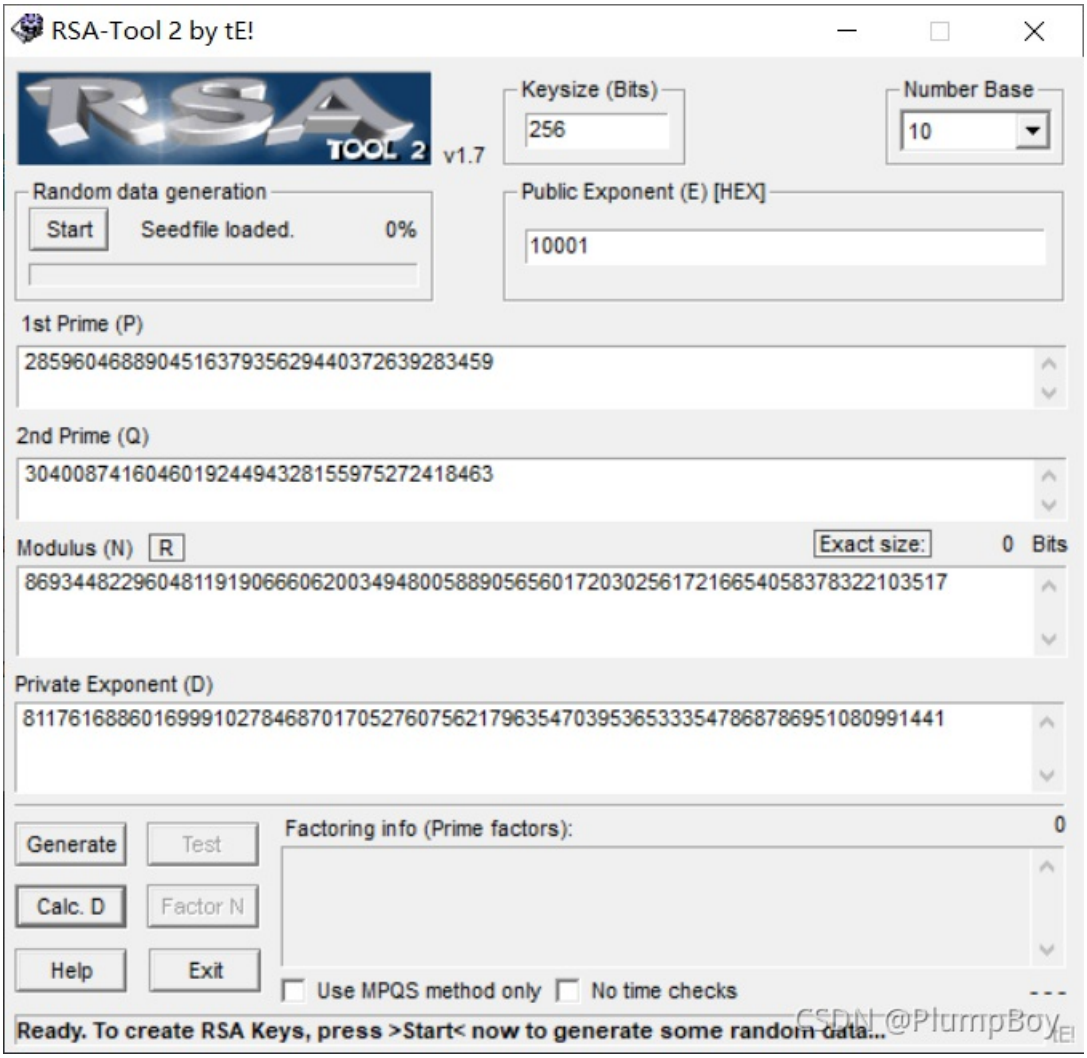
869344822960481191906660620034948005889056560172030256172166540583783221035178378322103517 Factorize!

Result:

tatus (?)	digits	number
F	77 (show)	8693448229...17<77> = 285960468890451637935629440372639283459<39> · 304008741604601924494328155975272418463<39>


```
p=285960468890451637935629440372639283459
q=304008741604601924494328155975272418463
```

此时打开RSA-Tool2，选择10进制，填入p，q，e（注意e是需要转换为16进制）。点击Calc.D得到d的值



此时我们已经得到了e，n，p，q，d的值，可以进行解密了。

脚本如下

```
import rsa

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

key = rsa.PrivateKey(n,e,d,q,p)
with open(r'C:\Users\27475\Desktop\output\flag.enc','rb')as data:
    data = data.read()
    print(rsa.decrypt(data,key))
```

最终得到`flag{decrypt_256}`