

BUUCTF-Crypto-RSA

原创

几番89 于 2021-04-19 08:17:34 发布 620 收藏 7

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/qq_45970858/article/details/115854635

版权

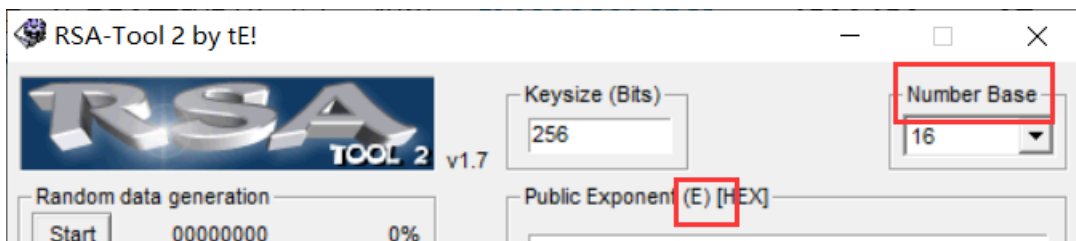
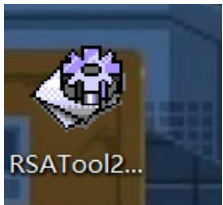
BUUCTF-Crypto-RSA

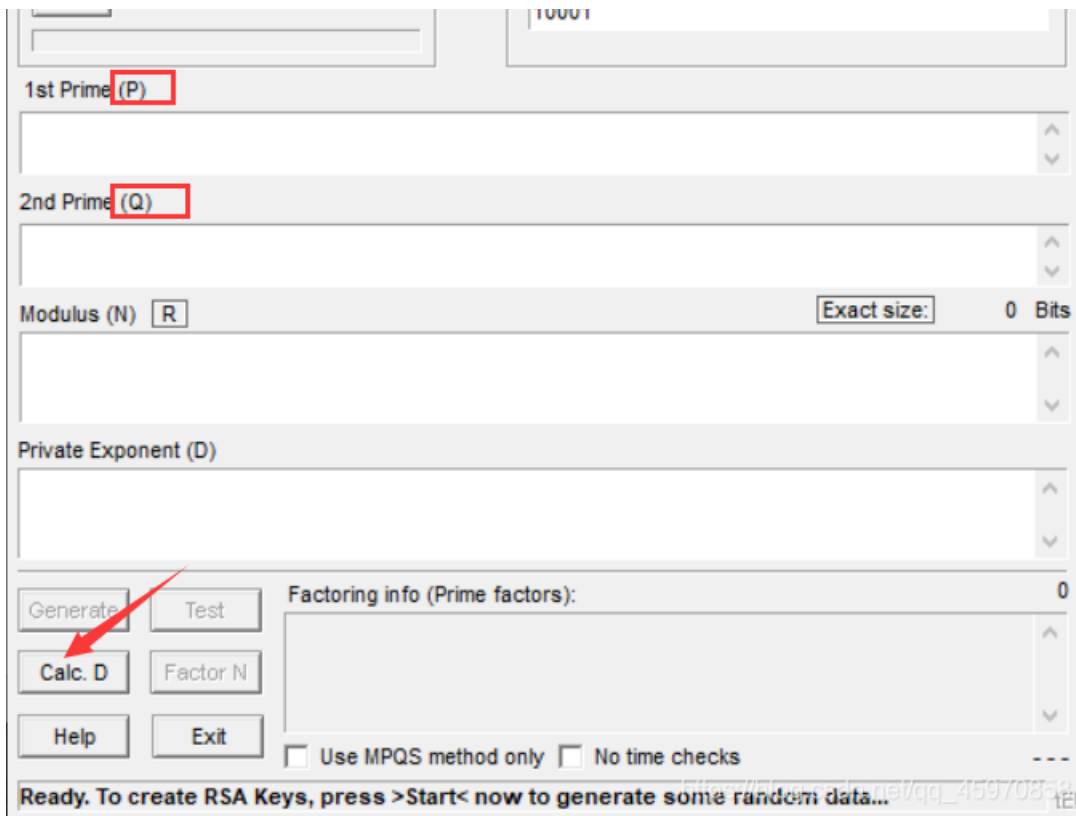


在一次RSA密钥对生成中，假设 $p=473398607161$ ， $q=4511491$ ， $e=17$

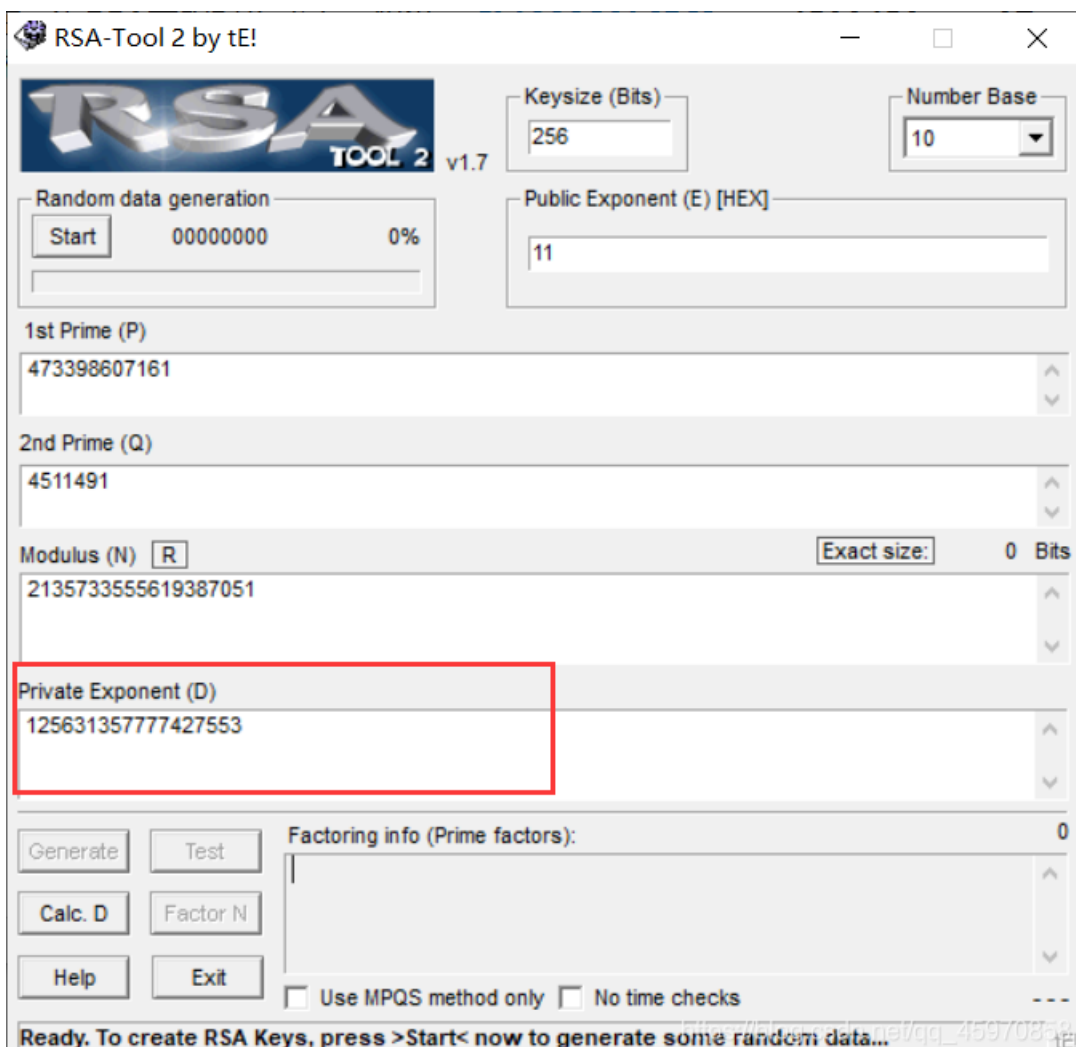
求解出 d 作为flag提交

此时可以利用工具 RSA-Tool2 by tE





先将e,p,q输入进去，再点击Calc.D,获得d（给出p,q,e的话直接填入，再点击Calc.D,获得d）
（注：给出的是n和e的话，输入n和e，点击Factor N(分解)，得到p,q,再重复上一步步就能得到d了）
Public Exponent这里要使用16进制的数，如果公钥e=17的话，就应该填入十六进制的11



RSA

1

注意：得到的 flag 请将 noxCTF 替换为 flag，格式为 flag{} 提交。

 70a2f2f0-d...

flag{125631357777427553}

Submit

https://blog.csdn.net/qq_45970858

RSA ✓

2570 Solves
1 Points