BUUCTF(rsarsa)

原创

Bigotry77 于 2021-07-28 18:28:38 发布 379 收藏 1
分类专栏： ctf 文章标签： 密码学 python

看到题目之后应该能想到这跟RSA算法相关，于是乎，习惯性用python写代码来解密

代码如下：

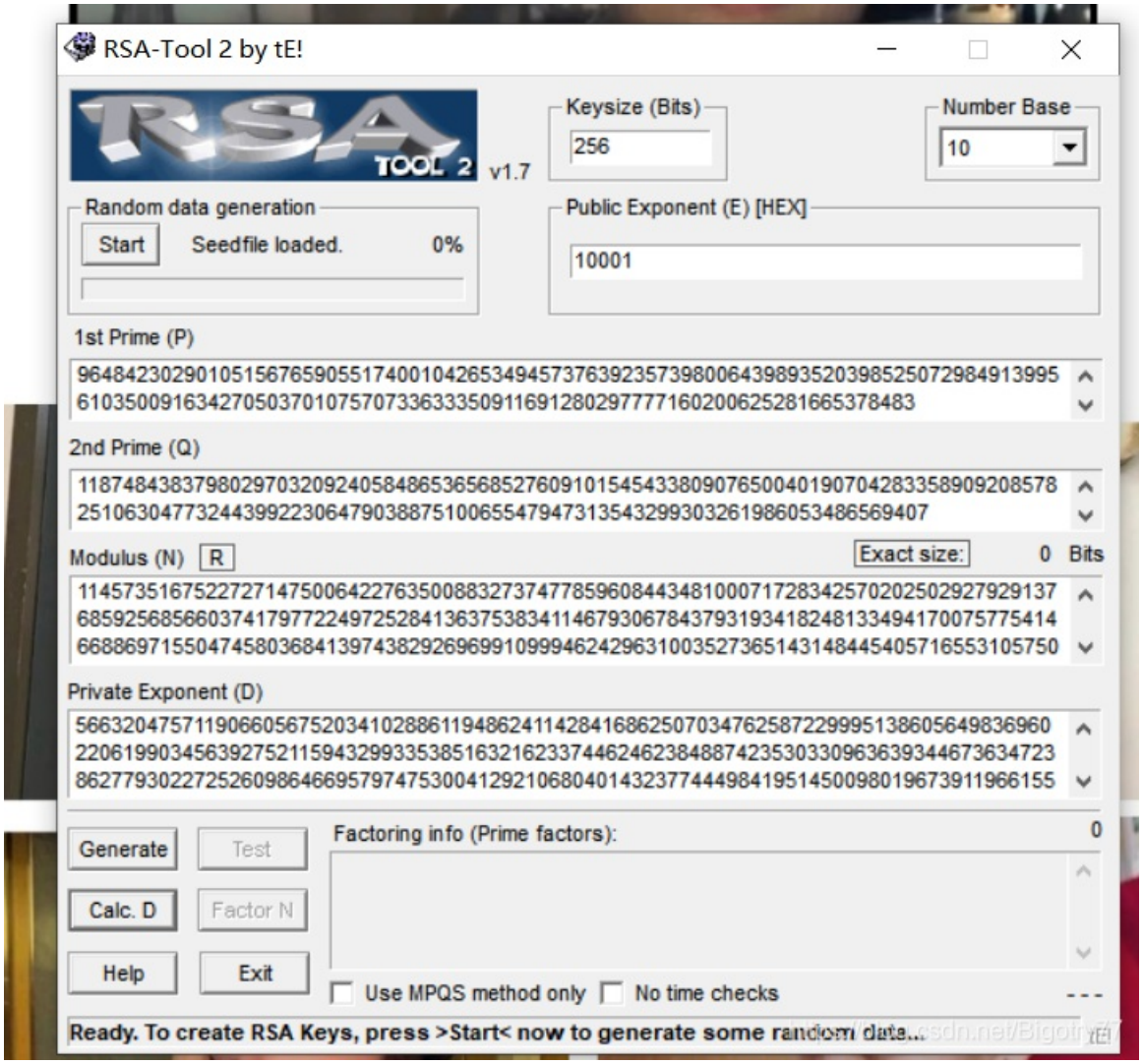
```
import gmpy2
e = 65537
p = 964842302901051567659055174001042653494573763923573980064398935203985250729849139956103500916342705037
q = 118748438379802970320924058486536568527609101545433809076500401907042833589092085782510630477324439922
n = p*q
#密文
C = 832082989951746041747735902982036393605400248712561268928896613457424033149298619391004926660564731664

d =gmpy2.invert(e,(p-1)*(q-1))
print(d)
#求明文
M = pow(C,d,n)     #快速求幂取模运算
print(M)
```

然后运行之后上面一行是d的值，下面一行就是flag了。

还有一种是：

先用工具解出d，如图：



然后解出来d以后就可以用代码得到flag，代码如下：

```
e = 65537
p = 964842302901051567659055174001042653494573763923573980064398935203985250729849139956103500916342705037
q = 118748438379802970320924058486536568527609101545433809076500401907042833589092085782510630477324439922
n = p*q
#密文
C = 832082989951746041747735902982036393605400248712561268928896613457424033149298619391004926666056473166

d = 566320475711906605675203410288611948624114284168625070347625872299951386056498369602206199034563927521

#求明文
M = pow(C,d,n)     #快速求幂取模运算
print(M)
```

其实两个方法本质差不多，就是一个直接一点用代码全部搞定，第二个麻烦一点，需要先用工具然后再用代码。