

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](#)

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/weixin_44214568/article/details/120627212

版权

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:

```
pub.key - 记事本
文件(E) 编辑(E) 格式(O) 查看(V) 帮助(H)
-----BEGIN PUBLIC KEY-----
MDwwDQYJKoZIhvcNAQEBBQADKwAwKAIhAMAzLFxkrkcYL2wch21CM2kQVFf
/AvKr1rzQczdAgMBAAE=
-----END PUBLIC KEY-----
CSDN @半杯雨水敬过客
```

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](#)

factordb.com/index.php?query=86934482296048119190666062003494800588905656017203025617

Search Sequences Report results Factor tables Status Downloads Login

8693448229604811919066606200349480058890565601720302561721665405 8378322103517 Factorize!

Result:

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

More information

ECM

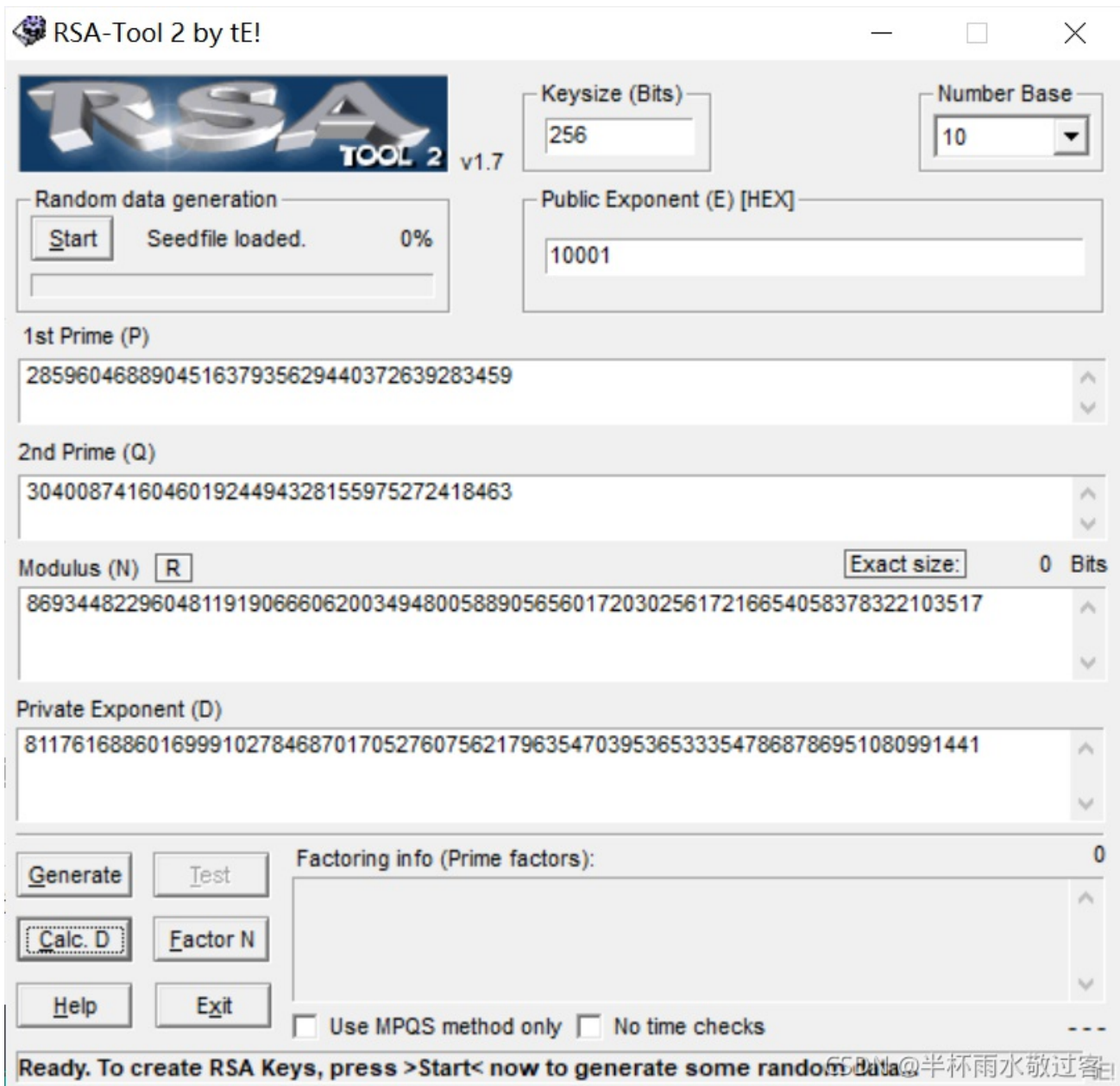
CSDN @半杯雨水敬过客

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 = 86934482296048119190666062003494800588905656017203025617216654058378322103517
p = 285960468890451637935629440372639283459
q = 304008741604601924494328155975272418463
d = 81176168860169991027846870170527607562179635470395365333547868786951080991441

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}

