

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](#)

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/m0_61290851/article/details/122451456

版权

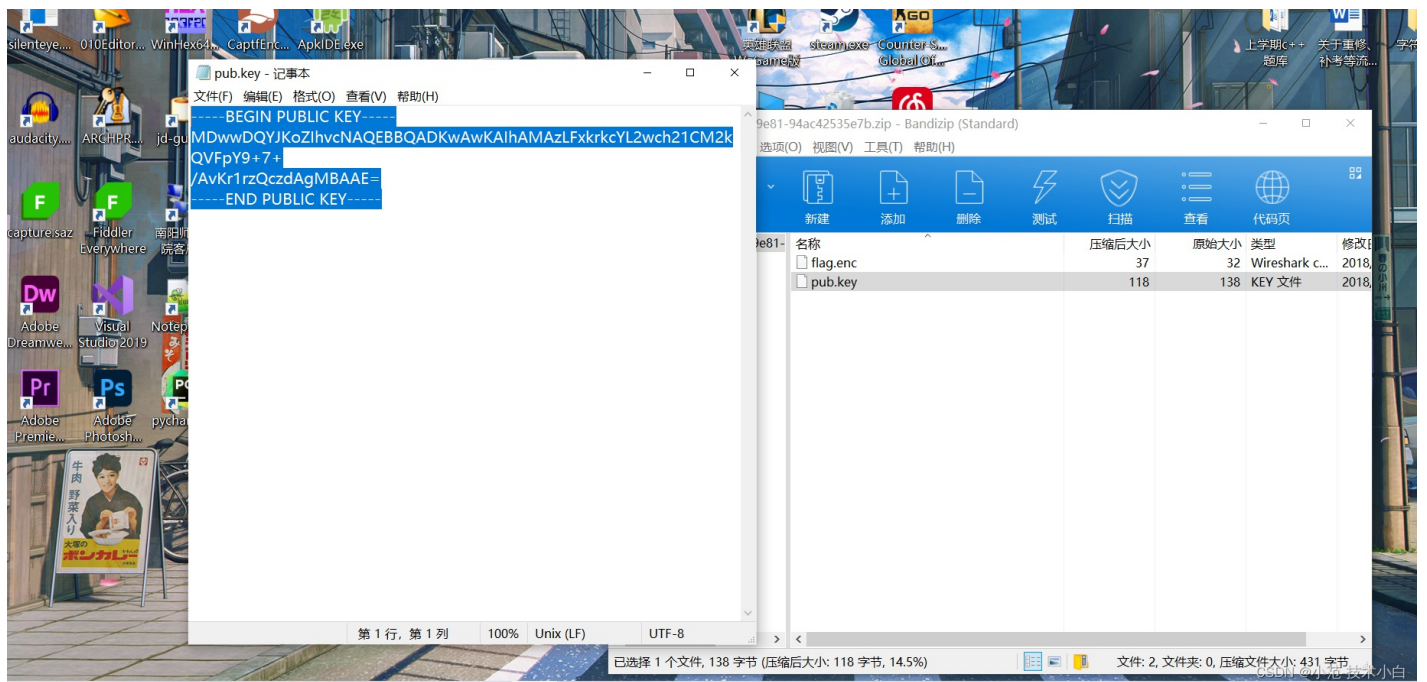


[CTF 专栏收录该内容](#)

2 篇文章 0 订阅

订阅专栏

打开压缩文件后



然后进行公钥解析

```
-----BEGIN PUBLIC KEY-----
MDUwDQYJKoZIhvcNAQEBBQADKwAwKAIhAMAzLFxkrkcYL2wch21CM2kQVFP.Y9+7+
/AvKrlrz0czdAgMBAAE=
-----END PUBLIC KEY-----
```

解析

详细信息

密钥类型	RSA
密钥强度	256
PN(e)	65537
PN(n)	8693448229604811919066606200349480058890565601720302561721665405 8378322103517
DER格式	303c300d06092a864886f70d0101010500032b003028022100c0332c5c64ae47182f6c1c876d42336910545a58f7eefefc0bcaaf5af341ccdd0203010001

CSDN @小范-技术小白

分解质因数n

www.factordb.com/index.php?query=86934482296048119190666062003494800588905656017203025617216654058378322103517

Search Sequences Report results Factor tables Status Downloads Login

8693448229604811919066606200349480058890565601720302561721665405 8378322103517 Factorize!

Result:

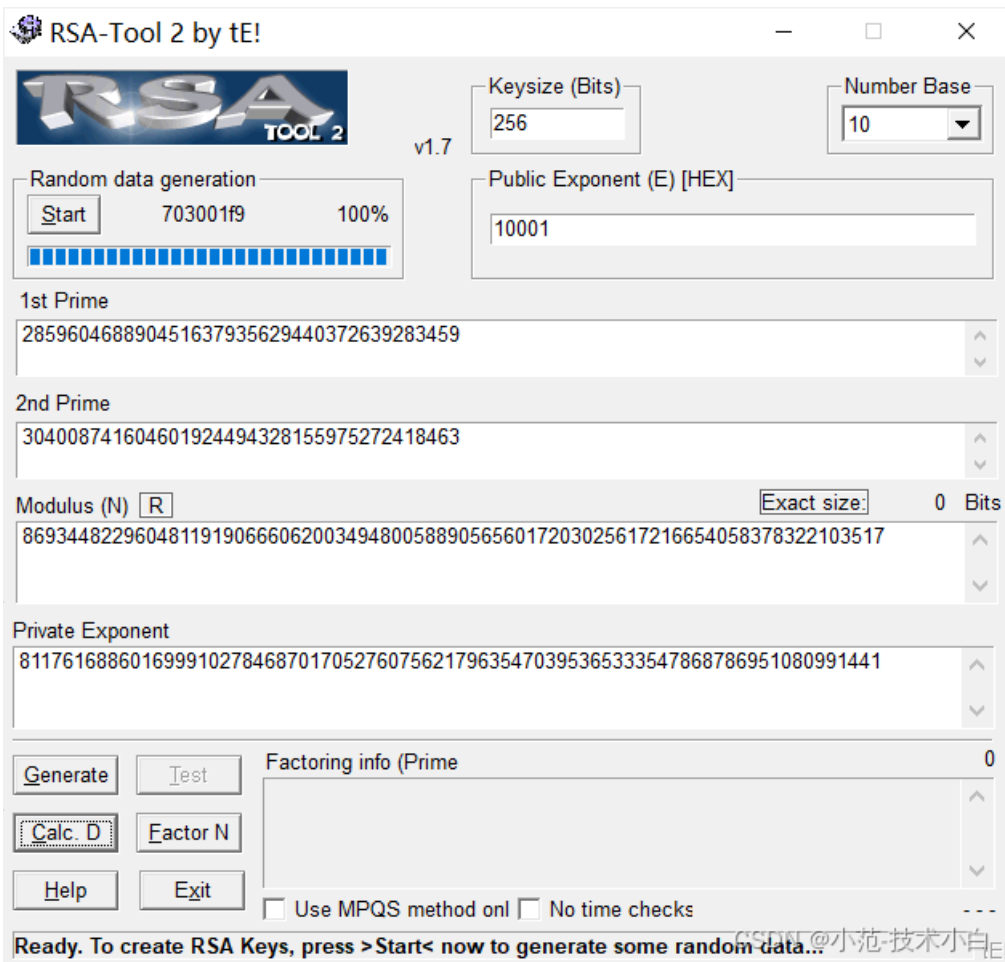
status (?)	digits	number
FF	77 (show)	8693448229...17<77> = 285960468890451637935629440372639283459<39> · 304008741604601924494328155975272418463<39>

More information ↗

ECM ↗

CSDN @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= 86934482296048119190666062003494800588905656017203025617216654058378322103517
p= 285960468890451637935629440372639283459
q= 304008741604601924494328155975272418463
d= 81176168860169991027846870170527607562179635470395365333547868786951080991441

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