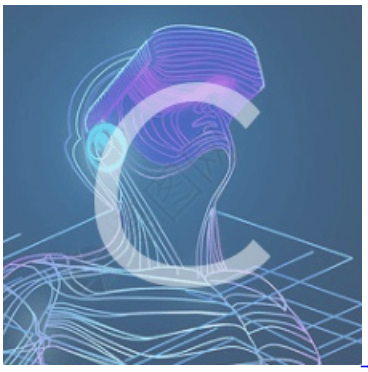
BUUCTF_RSA

原创

ZYen12138 于 2020-10-23 17:08:55 发布 593 收藏 3

分类专栏： # BUUCTF CTF

本文链接：https://blog.csdn.net/weixin_46009088/article/details/109245606



BUUCTF 同时被 2 个专栏收录

17 篇文章 2 订阅

订阅专栏

CTF

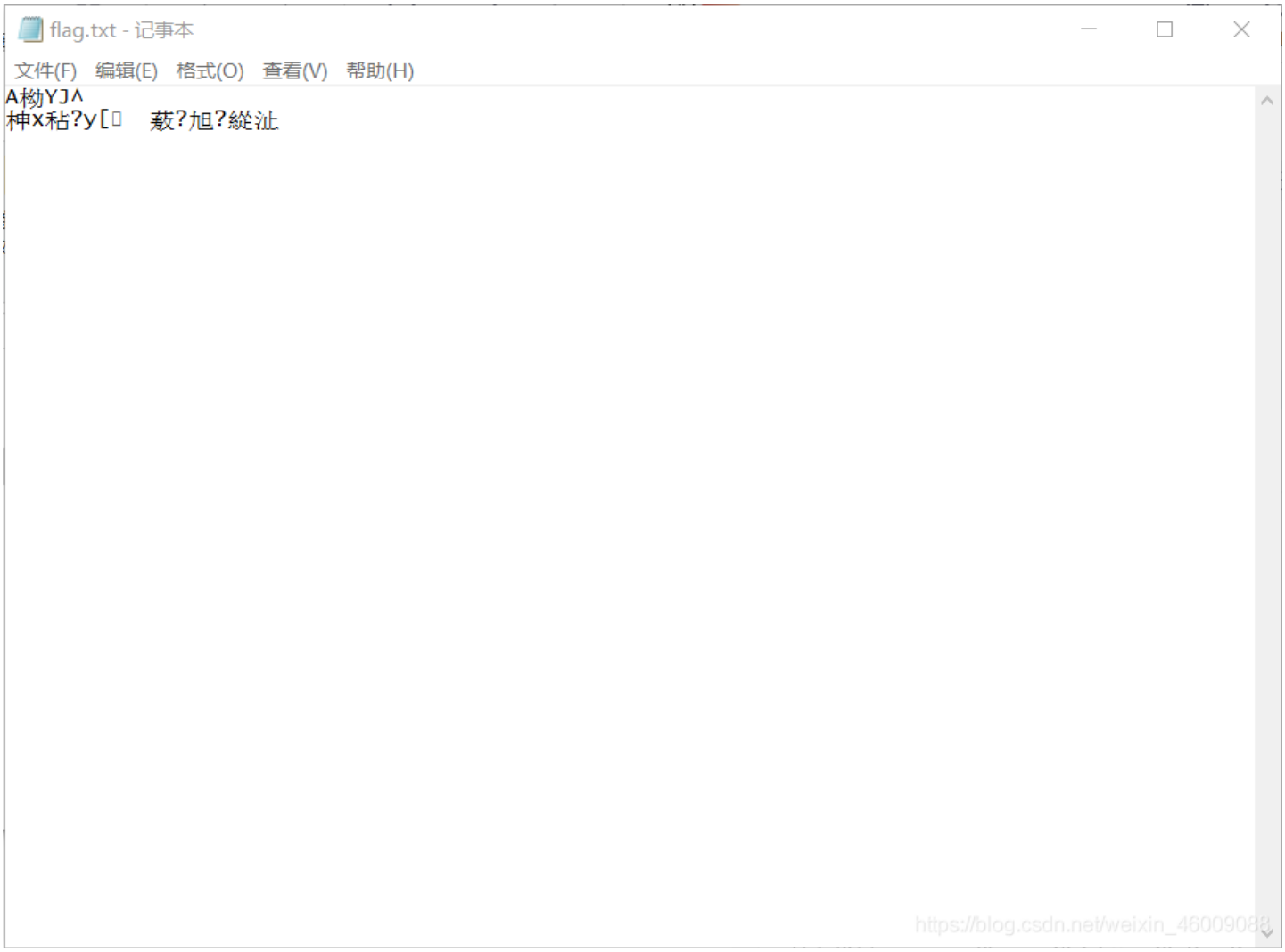
17 篇文章 0 订阅

订阅专栏

BUUCTF_RSA

下载文件解压得到两个文件

既然题目都说是RSA算法了，看文件名也能猜到一个是公钥文件(pub.key)一个是需要解密的文件(flag.enc)，将他们转化为txt格式查看:


flag.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
A桝YJ^
柙x秸?y[□ 薮?旭?縦沚
https://blog.csdn.net/weixin_46009088

乱码不用管它.

pub.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
-----BEGIN PUBLIC KEY-----
MDwwDQYJKoZIhvcNAQEBBQADKwAwKAIhAMAzLFxkrkcYL2wch21CM2kQVFpY9+7+
/AvKr1rzQczdAgMBAAE=
-----END PUBLIC KEY-----
```


这个是公钥，用在线计算工具转换 ①

详细信息

密钥类型	RSA
密钥强度	256
PN(e)	65537
PN(n)	869344822960481191906660620034948005889056560172030256172166540583783221035 17
DER格式	303c300d06092a864886f70d0101010500032b003028022100c0332c5c64ae47182f6c1c876d42336910545a58f7eefefc0bcaaf5af341ccdd0203010001

得到e和n,我们拿n去求p和q ②

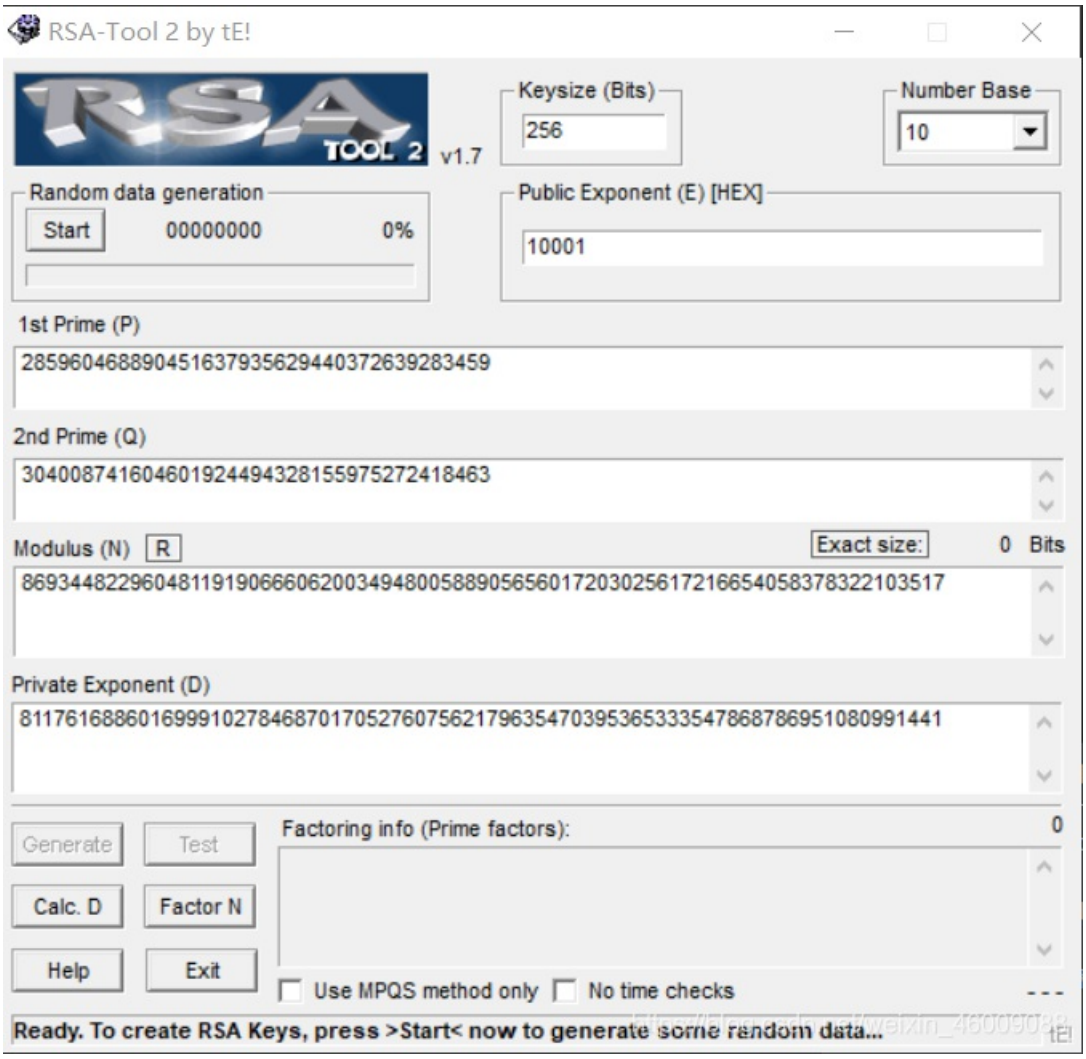
Search | Sequences | Report results | Factor tables | Status | Downloads | Login

869344822960481191906660620034948005889056560172030256172166540583783221035 17 Factorize! (?)

Result:

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

然后把 p,q,e,n 输入到 RSA-Tool 2 by tE! 上，把 Number Base 改成 10 ,得到 d ， 如图：



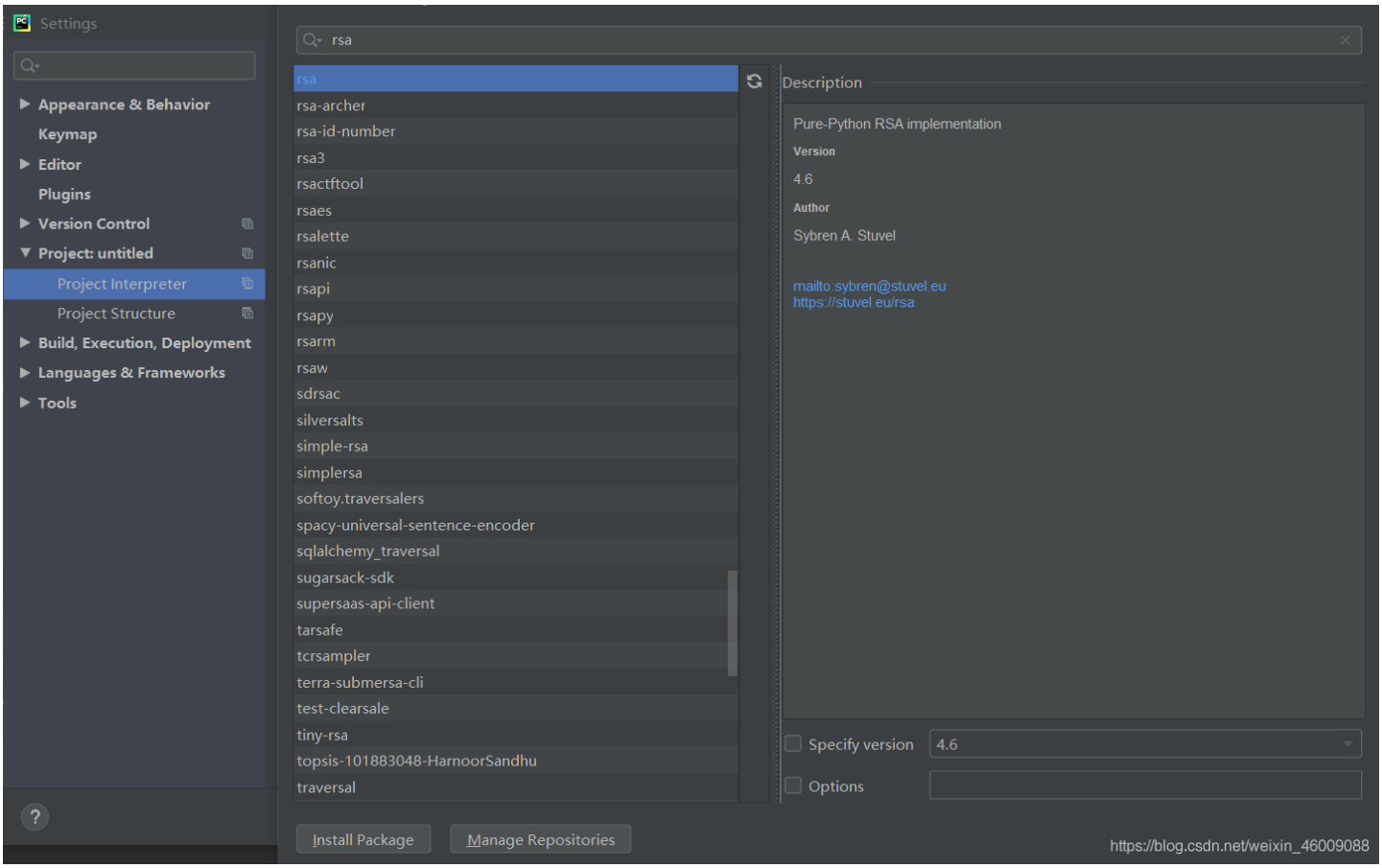
写个python脚本将密文解密，如下：

```
import rsa

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

key = rsa.PrivateKey(n,e,d,q,p)
with open('D:/applicance/reverse\ctf/buuctf/output/flag.txt','rb')as data:
    data = data.read()
    print(rsa.decrypt(data,key))
```

(pycharm安装RSA模组 :File ->Settings ->Project : untitled -> Project Interpreter,点 + 搜索rsa安装)，如图：



最后，运行得到结果：

```
b'flag{decrypt_256}\n'
```

①计算n和e的网站：http://ctf.ssleye.com/pub_asys.html
②用n计算p,q的网站：http://factordb.com/index.php