

这里推荐一个工具RsaCtfTool

下面可直接利用这个工具获得 p, q和d。

```
python RsaCtfTool.py --createpub -n
```

```
python RsaCtfTool.py --publickey test.pem --private > test.key
```

```
python RsaCtfTool.py --key test.key --dumpkey
```

注意:

生成公钥或者私钥文件可能有乱码, 运行出现格式错误, 删除即可

```
root@kali:~/media/root/.local/share/flatpak/exports/share/flatpak/overrides/CTF_Tool/Crypto/RsaCtfTool# ./RsaCtfTool.py --createpub -n 4005781386428960989637205658554417248531811702624626389974432
923745278182862721955607788280591191361738959890013821315369085382326382892363142604314518060388708082899248800814861248195977326277895645328954977897459168538098776
807293895728108197009429371690324377522718700141828104991149324793998722997 -# 334411824413073728050721818279258991882433828273718931889332794483910344456028094248
43589487834465770489532371817125181554614722985183791528916212839348121066835410880802815345805868236527677122716257852842809846808048032830812484988677185382353772
70892578182711682139182621897232837814967947827619
private argument is not set, the private key will not be displayed, even if recovered.
-----BEGIN PUBLIC KEY-----
MIIEDwIBAQgP/3S15vKqWset/SekwPwMhXbELxLSaFxFwEDFHYGhC
MhXbELxLSaFxFwEDFHYGhCttrC08hXbUuXpDkCjJ2ey1tdk17uWof
IhKjvW1wCYYqk0vImwKcSf3FhWwGMS1J2M5L31dHvGuFz2ipmBnEt3Mt
+5FHCePdtbmlqR8I8JQK8GQh+6Q8S337aMgkxsp5AdGqzJNK281zBaPQ
kI8Mk0F3W7qC0mPKHzyYH5Gcb8MhAB107h11eQ01CF56mCOLQ5FgpWtP6QRtToE0Bfj8BPMhXpTG/XMhWBE
8MhAB107h11eQ01CF56mCOLQ5FgpWtP6QRtToE0Bfj8BPMhXpTG/XMhWBE
Zj9R250U1CpmEiV2s9MkQoaJ55s145K900WkX7E36pzdPZ081FewsVTr1T/
CqZAffmWtGtEkw1SMhrraVZbcJ3t+CNQFkQc9YkkyLE4R0TeIyKcIBJfouTD
Taz1WQZCbfG14b41kxkWP3MCRQAQ31M11A8SV00QJvGEdK9f9P0NKAD7K/P
MhXbELxLSaFxFwEDFHYGhCttrC08hXbUuXpDkCjJ2ey1tdk17uWofIhKjvW1wCYYqk0vImwKcSf3FhWwGMS1J2M5L31dHvGuFz2ipmBnEt3Mt+5FHCePdtbmlqR8I8JQK8GQh
-----END PUBLIC KEY-----
root@kali:~/media/root/.local/share/flatpak/exports/share/flatpak/overrides/CTF_Tool/Crypto/RsaCtfTool# ./RsaCtfTool.py --publickey flag1.pem --private
[*] Testing key flag1.pem.
[*] Performing factordb attack on flag1.pem.
[*] Attack success with factordb method !
Results for flag1.pem:
Private key :
-----BEGIN RSA PRIVATE KEY-----
MIIEDwIBAQgP/3S15vKqWset/SekwPwMhXbELxLSaFxFwEDFHYGhC
MhXbELxLSaFxFwEDFHYGhCttrC08hXbUuXpDkCjJ2ey1tdk17uWofIhKjvW1wCYYqk0vImwKcSf3FhWwGMS1J2M5L31dHvGuFz2ipmBnEt3Mt+5FHCePdtbmlqR8I8JQK8GQh
+6Q8S337aMgkxsp5AdGqzJNK281zBaPQkI8Mk0F3W7qC0mPKHzyYH5Gcb
8MhAB107h11eQ01CF56mCOLQ5FgpWtP6QRtToE0Bfj8BPMhXpTG/XMhWBE
Hf5Y2DyV58Rya5KqAoLdab8MhX2LXkgCT2Q8VowIgEkn1SMhrraVZbcJ3t+CN
QFkQc9YkkyLE4R0TeIyKcIBJfouTDfzaz1WQZCbfG14b41kxkWP3MCRQAQ31M11A8SV00QJvGEdK9f9P0NKAD7K/P
MhXbELxLSaFxFwEDFHYGhCttrC08hXbUuXpDkCjJ2ey1tdk17uWofIhKjvW1wCYYqk0vImwKcSf3FhWwGMS1J2M5L31dHvGuFz2ipmBnEt3Mt+5FHCePdtbmlqR8I8JQK8GQh
-----END RSA PRIVATE KEY-----
CSDN @彬彬有礼am_03
```

```
root@kali:~/media/root/.local/share/flatpak/exports/share/flatpak/overrides/CTF_Tool/Crypto/RsaCtfTool# ./RsaCtfTool.py --key flag1.key --dumpkey
private argument is not set, the private key will not be displayed, even if recovered.
n: 460657813864289609896372056585544172485318117026246263899744329237452781828627219556077882805911913617389598900138213153690853823263828923631426043145180603887860
029824880814861248195977326277895645328954977897459168538098776
e: 35461110244130757205657218182792589518834350228753730931089393275463916544566268942454158961878344657784095323731871253185546147225993017915289162128393881210660355
43088082615345005868236527677122716257852842809846808046803283001274849680477185382519377370925781827116821391826218972328377614967547827619
d: 82646697229427581729339772371833216882149471976834221882393409363691895
p: 15991846970932132207262690156074993288632576648314846402341810735319249066370916096064926219079368845510444831408322229147771682961132420481897362843199
q: 288057917126225948085690272901843868667835444129624714820786283600465784973534361820789816390178728736856976847252134463567334299356760080507454648207083
root@kali:~/media/root/.local/share/flatpak/exports/share/flatpak/overrides/CTF_Tool/Crypto/RsaCtfTool#
```

```
#!/usr/bin/python
# -*- coding=utf8 -*-
import gmpy2
from libnum import n2s

n = '46065781388428960989637205658554417248531811702624626389974432923749270182062721955600778820059011913617389
5989001382151536006853823326382892363143604314518686388786002989248800814861248595075326277099645338694977097459
168530898776007293695728101976069423971696524237755227187061418202849911479124793990722597'

e = '35461110244130757205657218182792589919834535022875373093108939327546391654445662689424541509610783446577840
9532373187125318554614722599301791528916212839368121066035541008808261534500586023652767712271625785204280964688
004680328300124849680477105302519377370092578107827116821391826210972320377614967547827619'

enc = '382309913162293996518235675906923010600446204121917377646323846805462562284515182388429652213947118483378
3245944384444688946836215418821484073674465788585894381017767587199111146665315825719113960569991634730829499566
453028081685048274053060225455912375912110633835922024263775919026933563326069449424391192'

p = '15991846970993213322072626901560749932686325766403404864023341810735319249066370916090640926219079368845510
444031400322229147771682961132420481897362843199'

q = '28805791771260259486856902729020438686670354441296247148207862836064657849735343618207098163901787287368569
768472521344635567334299356760080507454640207003'

d = '8264667972294275017293339772371783322168822149471976834221082393409363691895'

n1 = gmpy2.mpz(n)
enc1 = gmpy2.mpz(enc)
d1 = gmpy2.mpz(d)

r = gmpy2.powmod(enc1, d1, n1)
print (r)
s = n2s(r)
print (s)
```

结果为:

```
root@kali:~# python Rsa.py
flag{Wien3r_4tt@ck_1s_3AsY}
```

flag{Wien3r_4tt@ck_1s_3AsY}