

WhiteGiveRSA

百度查一下是 RSA 加密，先用 yafu 算出 p 和 q

```
命令提示符
fac: using pretesting plan: normal
fac: no tune info: using qs/gnfs crossover of 95 digits
div: primes less than 10000
fmt: 1000000 iterations
rho: x^2 + 3, starting 1000 iterations on C60
rho: x^2 + 2, starting 1000 iterations on C60
rho: x^2 + 1, starting 1000 iterations on C60
pml: starting B1 = 150K, B2 = gmp-ecm default on C60
ecm: 30/30 curves on C60, B1=2K, B2=gmp-ecm default
ecm: 49/49 curves on C60, B1=11K, B2=gmp-ecm default

starting SIQS on c60: 882564595536224140639625987659416029426239230804614613279163

==== sieving in progress (1 thread): 3888 relations needed ====
==== Press ctrl-c to abort and save state ====
3817 rels found: 1917 full + 1900 from 17991 partial, (10286.53 rels/sec)

SIQS elapsed time = 2.0396 seconds.
Total factoring time = 3.1523 seconds

***factors found***
P31 = 1029224947942998075080348647219
P30 = 857504083339712752489993810777

ans = 1

C:\Users\PC>
```

太大了手算不了，然后从网上找了一篇计算明文的代码，输入进去参数，得出结果

```
1 import gmpy2
2 from Crypto.Util.number import long_to_bytes
3 def D(c, e, p, q):
4     L = (p - 1) * (q - 1)
5     d = gmpy2.invert(e, L)
6     n = p * q
7     m = gmpy2.powmod(c, d, n)
8     flag = long_to_bytes(m)
9     print(flag)
10 if __name__ == '__main__':
11     p = 857504083339712752489993810777
12     q = 1029224947942998075080348647219
13     e = 65537
14     c = 747831491353896780365654517748216624798517769637260742155527
15     D(c, e, p, q)
```

尝试新的跨平台 PowerShell http

```
PS C:\Code\python> & C:/Python
hgame{w0w~yOU_kNoW+R5@!}
PS C:\Code\python>
```