

只解出来ezrsa 直接放脚本吧

```
from Crypto.Util.number import *
import random
#from secret import flag

#p = getPrime(512)
#print(p,pow(flag, 2, p))

d = 412482079973710723630883700852439735510778695041476999618132433355
p = 131079395635074597746162041412537474892320633362041739441232632845

def legendre(a,p):
    symbol = pow(a, (p - 1) // 2, p)
    if symbol == p - 1:
        return -1
    return symbol

def tonelli(a,p):
    if a == 0 or legendre(a,p) != 1:
        return 0
    q = p - 1
    s = 0
    while q % 2 == 0:
        q //= 2
        s += 1
    if s == 1:
        return pow(a, (p + 1) // 4, p)

    z = 2
    while legendre(z, p) != -1:
        z += 1

    m = s
    c = pow(z, q, p)
    t = pow(a, q, p)
    r = pow(a, (q + 1) // 2, p)

    while t != 1:
        t2 = t
        i = 0
        while t2 != 1 and i < m:
            t2 = pow(t2, 2, p)
            i += 1
```

```
b = pow(c, 2 ** (m - i - 1), p)
m = i
c = (b * b) % p
t = (t * c) % p
r = (r * b) % p
```

```
return r
```

```
f = tonelli(d,p)
print(f)
f = -f+p
print(long_to_bytes(f))
```