

Crypto: ezrsa

核心思路：我们用 Tonelli-Shanks 算法来计算二次同余方程的大数解

代码实现：

```
from Crypto.Util.number import *
```

```
c=412482079973710723630883700852439735510778695041476999618132433355695015
420698005940640276732772531223867305358114864143849421232015766539520833757
5556385
r=1310793956350745977461620414125374748923206333620417394412326328450760432
888568007247866901696942836666738135800405920420713481795262001473866545075
3147857
```

```
def Legendre(n, p):
    return pow(n, (p - 1) // 2, p)
```

```
def Tonelli_Shanks(n, p):
    assert Legendre(n, p) == 1
    if p % 4 == 3:
        return pow(n, (p + 1) // 4, p), pow(p - (p + 1) // 4, n, p)
    q = p - 1
    s = 0
    while q % 2 == 0:
        q = q // 2
        s += 1
    for z in range(2, p):
        if Legendre(z, p) == p - 1:
            c = pow(z, q, p)
            break
    r = pow(n, (q + 1) // 2, p)
    t = pow(n, q, p)
    m = s
    if t % p == 1:
        return r, p - r
    else:
        i = 0
        while t % p != 1:
            temp = pow(t, 2 ** (i + 1), p)
            i += 1
            if temp % p == 1:
                b = pow(c, 2 ** (m - i - 1), p)
                r = (r * b) % p
                c = (b * b) % p
```

```

        t = (t * c) % p
        m = i
        i = 0
    return r, p - r

```

```

result1, result2 = Tonelli_Shanks(c, r)
print(result1)
print(long_to_bytes(result1))
print(result2)
print(long_to_bytes(result2))

```

具体代码思路:

- ①从 $p-1$ 中除去所有因子 2，设 $p-1=Q*2^S$ ，其中 Q 是奇数（也就是除去所有因子 2 的结果）。如果 $S=1$ ，即 $p \equiv 3 \pmod{4}$ ，那么直接返回 $R = \pm n^{(p+1)/4}$ 。
- ②选择一个 z ，使得勒让德符号 $L(z,p) = -1$ （即， z 是 p 的二次非剩余），令 $c \equiv z^Q$ 。
- ③令 $R \equiv n^{(Q+1)/2}$ ， $t \equiv n^Q$ ， $M=S$ 。
- ④循环：
 - 1.若 $t \equiv 1$ ，返回 R ，程序终止。
 - 2.否则，找出最小的 i ，使得 $0 < i < M$ ，且 $t^{2^i} \equiv 1$ 。可以重复做平方完成这一点。
 - 3.令 $b \equiv c^{2^{M-i-1}}$ ，令 $R \equiv R*b$ ， $t \equiv t*b^2$ ， $c \equiv b^2$ ， $M=i$ 。
 如果得到了一个解 R 另一个解就是 $p-R$ 。