ezrsa:

打开附件，发现是一个平方剩余问题，求解x^2=a(mod p)，已知a和p，可以使用Tonelli-Shanks算法，编写python程序如下：

from Crypto.Util.number import \*  
  
c = 4124820799737107236308837008524397355107786950414769996181324333556950154206980059406402767327725312238673053581148641438494212320157665395208337575556385  
r = 13107939563507459774616204141253747489232063336204173944123263284507604328885680072478669016969428366667381358004059204207134817952620014738665450753147857  
  
  
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)  
 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  
 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  
  
  
result = Tonelli\_Shanks(c, r)  
print(result)  
print(r-result)  
print(long\_to\_bytes(result))  
print(long\_to\_bytes(r-result))

注意要有两个解需排除一个

运行结果如下：

b'\xfaFF"\x0bxn\x93\xd1\xfd8\x91\x8d;g\x8c\xf7Wj\xcf\x8c\xde\x94\x14\xea\xd9\xfdB\xd5\x16\xe4>\xe5\xdf%(\xb29^\x87v\x04\x9eOV\xc9\xd18\xc6o\x08\xb8vL\x16N\xb6\xede\xf9\x13\x90aT'

b'flag{9971e255f0c020e8e57fbae75f43d7fb}'

得到flag.