

# ezrsa

一看题目,  $c = pow(m, 2, p)$ , 即 $m^2 = c + kp$ .

其中k未知且 $k > 0$ , 穷举爆破:

```
from Crypto.Util.number import *
import gmpy2
c = 4124820799737107236308837008524397355107786950414769996181324333556950154206980059406402767327725312238673053581148641438494212320157665395208337
p = 1310793956350745977461620414125374748923206333620417394412326328450760432888568007247866901696942836666738135800405920420713481795262001473866549
for k in range(100000):
    m = gmpy2.iroot(c+k*p, 2) [0]
    flag = long_to_bytes(m)
    try:
        if flag.decode("utf-8").startswith("flag("):
            print(flag)
    except Exception:
        continue
```

结果发现出不了, 应该是m太大, 导致k太大, 没法在短时间内爆破出来。

那直接用sage解方程:

```
from Crypto.Util.number import *
c = 4124820799737107236308837008524397355107786950414769996181324333556950154206980059406402767327725312238673053581148641438494212320157665395208337
p = 1310793956350745977461620414125374748923206333620417394412326328450760432888568007247866901696942836666738135800405920420713481795262001473866549
R.<m> = PolynomialRing(Zmod(p))
f = (m^2) - c
mlist = f.roots() #所有解都在mlist里
print(mlist)
```

打印后发现有两个解:

```
[ (131079395635074597746162041412537474892320633362041739441232632714675998460651539786579753982613025359681991275971458280047271190476571795350388106,
```

将它们转化为字节串打印:

```
print(long_to_bytes(int(mlist[0][0])))
print(long_to_bytes(int(mlist[1][0])))
```

输出结果:

```
b' \xfaFF"\x0b\xn\x93\xd1\xfd8\x91\x8d;g\x8c\xf7Wj\xcf\x8c\xde\x94\x14\xea\xd9\xfdB\xd5\x16\xe4>\xe5\xdf%(\xb29`\x87v\x04\x9e0V\xc9\xd18\xc6o\x08\xb8v'
b' flag{9971e255f0c020e8e57fbae75f43d7fb}'
```

第二个解即是我们想要的flag。