

e=2, rabin算法, 代码如下

```
def func(n, p):
    if pow(n, (p-1)//2, p) != 1:
        return None
    q = p - 1
    s = 0
    while q % 2 == 0:
        q //= 2
        s += 1
    z = 1
    while pow(z, (p-1)//2, p) != p - 1:
        z += 1
    m = s
    c = pow(z, q, p)
    t = pow(n, q, p)
    r = pow(n, (q+1)//2, p)
    while t != 1:
        i = 0
        temp = t
        while temp != 1:
            temp = (temp * temp) % p
            i += 1
        b = pow(c, 1 << (m-i-1), p)
        m = i
        c = (b * b) % p
        t = (t * b * b) % p
        r = (r * b) % p
    return r, p-r

c =
412482079973710723630883700852439735510778695041476999618132433355695015420698005
9406402767327725312238673053581148641438494212320157665395208337575556385
p =
131079395635074597746162041412537474892320633362041739441232632845076043288856800
72478669016969428366667381358004059204207134817952620014738665450753147857
x, y = func(c, p)
print(bytes.fromhex(hex(x)[2:]))
print(bytes.fromhex(hex(y)[2:]))
```

输出为

```
b'\xfaFF"\x0bxn\x93\xd1\xfd8\x91\xd;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'f1ag{9971e255f0c020e8e57fbae75f43d7fb}'
```