1.先开方分解n，求出pq

```
p1,s=gmpy2.iroot(n,2)
q=gmpy2.next_prime(p1)
p=n//q
```

2.利用威尔逊定理，通过补位的方式，求出c1，c2

```
for i in range(p-x+1,p-1):
    c1=(c1*i)%p
for i in range(q-y+1,q-1):
    c2=(c2*i)%q
```

3.分别求出m1，m2后，利用中国剩余求出明文

```
dp=libnum.invmod(p,q-1)
dq=libnum.invmod(q,p-1)
m1=pow(c1,dp,q)
m2=pow(c2,dq,p)
m=libnum.solve_crt([m1,m2],[q,p])
print(libnum.n2s(int(m)))
```

脚本全文：

```
n=
897311172704383526807303078615487268069837304377930913315276140803616804032479061062987869825451227304346135335871317658594433040162878266589782666093461 3
c1= 642847643171194223733465638504634752915052876401875494320709540366218258643 68
c2= 953679416950720982989213170443141934024415912036524909719031986611529591828 9

x=2293
y=2999

import gmpy2
import libnum
```

```
10
11 p1,s=gmpy2.iroot(n,2)
12 q=gmpy2.next_prime(p1)
13 p=n//q
14
15
16 for i in range(p-x+1,p-1):
17     c1=(c1*i)%p
18 for i in range(q-y+1,q-1):
19     c2=(c2*i)%q
20
21 dp=libnum.invmod(p,q-1)
22 dq=libnum.invmod(q,p-1)
23 m1=pow(c1,dp,q)
24 m2=pow(c2,dq,p)
25 m=libnum.solve_crt([m1,m2],[q,p])
26 print(libnum.n2s(int(m)))
```