# buuctf Crypto RSA1

原创

R-Mars 于 2021-03-16 22:02:30 发布 774 收藏 4

文章标签： 密码学



本文链接：https://blog.csdn.net/weixin_46244154/article/details/114903147



## buuctf RSA1

下载得到题目

```
p = 86376337672570085670996534865410911713204915094336154475391624379112441758856678063984117905240835534451581135022277452062053276909395040329946999020532290
q = 12640674973996472769176047937170883420927050821480010581593137135372473880595613737337630629752577346147039284030082593490776630572584959954205336880228469
dp = 65007957022168346211090423511932615306500438410562529309309496633586250168818328407280660261502646930761093548740998413804548817160977783072681169105829290
dq = 78347226367355344901953258038647067238057403355130388913791176043888168367455609809825679567351220196300217543876276751696804359958252753916081112055004 1
c = 24722305403887382073567316467649080662631552905960229399079107995602154418176056335800638887527614164073537657085079676157350205351945222989351316076486573599576041978339872265925062764318536089007310270278526159678937431903862892400747915525118983959970607934142974736675784325993445942031372107342103852
```

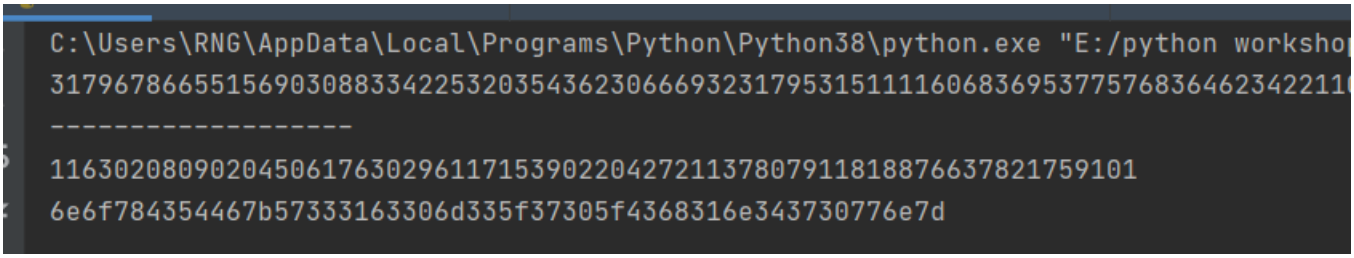
```
import gmpy2 as gp

p = gp.mpz(86376337672570085670996534865410911713204915094336154475391624379112441758856678063984117905240835534451581135022277452062053276909395040329946999020532290 )
q = gp.mpz(12640674973996472769176047937170883420927050821480010581593137135372473880595613737337630629752577346147039284030082593490776630572584959954205336880228469 )
dp = gp.mpz(65007957022168346211090423511932615306500438410562529309309496633586250168818328407280660261502646930761093548740998413804548817160977783072681169105829290 )
dq = gp.mpz(78347226367355344901953258038647067238057403355130388913791176043888168367455609809825679567351220196300217543876276751696804359958252753916081112055004 1 )
c = gp.mpz(24722305403887382073567316467649080662631552905960229399079107995602154418176056335800638887527614164073530437657085079676157350205351945222989351316076486573599576041978339872265925062764318536089007310270278526159678937431903862892400747915525118983959970607934142974736675784325993445942031372107342103852)

n = p*q
phin = (p-1)*(q-1)
dd = gp.gcd(p-1, q-1)
d=(dp-dq)//dd * gp.invert((q-1)//dd, (p-1)//dd) * (q-1) +dq
print(d)

m = gp.powmod(c, d, n)
print('--------------------')
print(m)
print(hex(m)[2:])
```

得到结果




将6e6f784354467b57333163306d335f37305f4368316e343730776e7d十六进制转一下得到
noxCTF{W31c0m3_70_Ch1n470wn}