七七的欧拉-wp

出题人：D0UBL3SEV3N

考点:无 q 如何求 phi;欧拉函数性质，RSA

下载附件

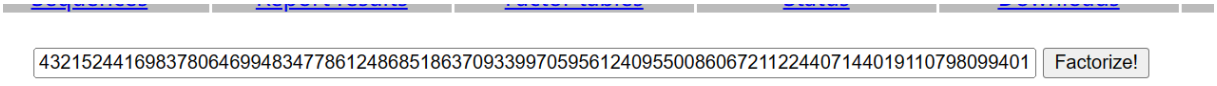
```
import gmpy2
import libnum
from crypto.Util.number import *

flag=b'ISCTF{************}'
m=bytes_to_long(flag)

p=libnum.generate_prime(1024)
e=libnum.generate_prime(512)

c=pow(m,e,n)
output = open('output1.txt', 'w')
output.write('e=' + str(e) + '\n')
output.write('n=' + str(n) + '\n')
output.write('c=' + str(c) + '\n')
output.close()
```

不难看出这是一道 RSA 题。附件给出了 e,n 和 c，但是没有 p 和 q。无法求出 phi，直接分解 n。不过注意一点，此时的 n 不是两个大素数相乘的形式，而是 p 的 8 次方。



Result:	
	number
show)	(9004396726...03<308>)^8 = (9004396726...03<308>)^8

http://www.factordb.com/index.php

了解欧拉函数后得到：phi=（p**k）-(p**k-1)。这里的 k 就是 8。那么可以计算 phi=（p**8）-(p**7)

进而求出私钥 d 和明文 m

代码如下：

```
import gmpy2
import libnum
from crypto.Util.number import *

# 解密脚本
e=840128542307549798996357288860137631337582772285888376756449906
647310161508421497304184487866483760615725703935884958304985616162
8241418012475432529735909
n=432152441698378064699483477861248685186370933997059561240955008
606721122440714401911079809940166001030564568154898016056321610178
864478752319768351155313753726788863395874802512110728941865586278
973537930986087668680670295786671714198901505996407815947550803914
894474620421675292033892360657272741660917412270684699876810837941
399253275458100240389371324635182256115787277379407467848918675324
981846428928265697775591076094932123320545593664090076855047681633
762502816440040677450878996537780234141059730476200412881184046579
346892531920437285902316181327165670846216700742563129393052652444
861457586099712490776390852046809231081324152165435414725345804142
742509799403304595515368302684285082178210606042608051090715344578
083556643299027796030508780556907724308428657012493780967758997782
558487731711083413311286732498990371338515355565159616999258091394
765768255241351112372497092415799038071792520110107948672697151707
398953923759207575597215160506806666587199904978636469893389602618
447621271424394862752946708581140796875722433121842221267109677449
717755857230455244677083870510347602087689568899390504981391893528
420872781251739571828041160524027784162166695223096922660360943713
081666637382842096152120165641710758744214720704224163189019265257
194859917921114143333980044331437519081993588615147253133343337035
392394148067737439419861649816425176731174126664304633185095717577
665108356007580609768483743533522390449080345014772956966842948160
918019441638775095589090407539075846723908238939916722467260262169
730133303139710075140648318015647033645916966109000892283029365958
480246166918784376187988641866348026475682395267711513236096505981
567015952658767367126706774520130543933362944834524802132710324882
012599907822890471321059898469724620943021325648090258024210575370
918709320148846068638072605211230844236894944019000142322573818015
907837355955752581602742484944985505836736887542208601424136315212
794643189874254473021354440936630345984556949011993124974592282547
464512330789549041599832695858831469599282269867241364836439112169
609228784893156579855721789767822137945104230481144941598243405552
259982984348281002578034928454749176721922151035141119225123651734
182661933808434813653912141521034548835956398504613663207766546079
334634505121301483608833326691162
```

得到 flag：

```
ISCTF{3237saq-21se82-3s74f8-8h84ps7-9qw45v7-6bs531-s26h23-c7iu01}
```