CTF中的RSA套路之低加密指数攻击攻击和低解密指数攻击

原创

KogRow 于 2021-08-26 14:44:19 发布 2025 收藏 15

分类专栏： Crypto CTF 文章标签： Crypto CTF

本文链接：https://blog.csdn.net/shuaicenglou3032/article/details/119930783

一、低加密指数攻击

低加密指数攻击的原理此处不再赘述，仅列举题型和exp。

二、低加密指数广播攻击

识别：n非常大,e一般很小。

1.基础题型

加密指数e非常小

一般拿到的是多组n和c，且只有一个e，e还很小

且模数n不同，但使用相同的加密指数e进行多次加密

例题 BUUCTF Dangerous RSA

题目：

```
#n:  0x52d483c27cd806550fbe0e37a61af2e7cf5e0efb723dfc81174c918a27627779b21fa3c851e9e94188eaee3d5cd6f752406a43fbecb53e80836ff1e185d3ccd7782ea846c2e91a7b0808986666e0bdadbfb7bdd65670a589a4d2478e9adcafe97c6ee23614bcb2ecc23580f4d2e3cc1ecfec25c50da4bc754dde6c8bfd8d1fc16956c74d8e9196046a01dc9f3024e11461c294f29d7421140732fedacac97b8fe50999117d27943c953f18c4ff4f8c258d839764078d4b6ef6e8591e0ff5563b31a39e6374d0d41c8c46921c25e5904a817ef8e39e5c9b71225a83269693e0b7e3218fc5e5a1e8412ba16e588b3d6ac536dce39fcdfce81eec79979ea6872793L
#e:  0x3
#c:0x10652cdfaa6b63f6d7bd1109da08181e500e5643f5b240a9024bfa84d5f2cac9310562978347bb232d63e7289283871efab83d84ff5a7b64a94a79d34cfbd4ef121723ba1f663e514f83f6f01492b4e13e1bb4296d96ea5a353d3bf2edd2f449c03c4a3e995237985a596908adc741f32365
so,how to get the message?
```

题目给出了1组数据和极小的e，但是n非常大，因此可以考虑低加密指数攻击，直接上代码：

```
import gmpy2
import os
from functools import reduce
from Crypto.Util.number import long_to_bytes
def CRT(items):
    N = reduce(lambda x, y: x * y, (i[1] for i in items))
    result = 0
    for a, n in items:
        m = N // n
        d, r, s = gmpy2.gcdext(n, m)
        if d != 1:
            raise Exception("Input not pairwise co-prime")
        result += a * s * m
    return result % N, N
# e, n, c
e = 0x3
n=[0x52d483c27cd806550fbe0e37a61af2e7cf5e0efb723dfc81174c918a27627779b21fa3c851e9e94188eaee3d5cd6f752406a43fbecb
53e80836ff1e185d3ccd7782ea846c2e91a7b0808986666e0bdadbfb7bdd65670a589a4d2478e9adcafe97c6ee23614bcb2ecc23580f4d2e
3cc1ecfec25c50da4bc754dde6c8bfd8d1fc16956c74d8e9196046a01dc9f3024e11461c294f29d7421140732fedacac97b8fe50999117d2
7943c953f18c4ff4f8c258d839764078d4b6ef6e8591e0ff5563b31a39e6374d0d41c8c46921c25e5904a817ef8e39e5c9b71225a8326969
3e0b7e3218fc5e5a1e8412ba16e588b3d6ac536dce39fcdfce81eec79979ea6872793L]
c=[0x10652cdfaa6b63f6d7bd1109da08181e500e5643f5b240a9024bfa84d5f2cac9310562978347bb232d63e7289283871efab83d84ff5
a7b64a94a79d34cfbd4ef121723ba1f663e514f83f6f01492b4e13e1bb4296d96ea5a353d3bf2edd2f449c03c4a3e995237985a596908adc
741f32365]
data = list(zip(c, n))
x, n = CRT(data)
m = gmpy2.iroot(gmpy2.mpz(x), e)[0].digits()
print('m is: ' + long_to_bytes(m))
```

直接还原明文。

2.进阶之爆破e

有些题目中不直接给出e，只给出几组n和c，然后说明e1=e2=...=en，这种也简单，无非根据上述代码把n和c一组一组写进去，再多写一个循环，一个个爆破e就完了。

例题

```
n1 = 151558345122742722140230869081973367560530302423230480485121316809497417802991477396429152756523612081269324464403510588914780428583674103830380036467248779045865429180173771626555925084606640155208022598517331915416759
98796977690625295282942487921358909287151891024014877346470774030618403239619473160116278194168652577809272534421739253899557104677104226574616639904574493424733183128587308159599813172995669302313437832700325084051476508569
97601757502588227379814153746570320161115896657690074833984539351194285935976262756523982743681758788902822962921975844436457677581639506889569081828207975721783031051597812 7
c1 = 549445069175361291973785391513285583409676560533201545464036103223913292201258087416431455988423183488050927580330849151520054221692185516450243328260515765258746786292701559989609832318873662678624068837676559660769228946455381172698817158314409476422832235259866638736312667043187870883639945324381026855021558641614595449198721805829811885615794319234871221108196681763424874954149520251231893947863213669616177049596694545063893238643985317109795185477384842732796700539544725823890751732846292067298384354636845967510856538604837894948953873960102607200129938875485920575804532390319723834784402860715421847230 6
n2 = 188422100202148934472784337638599174416738568826009149301061274087850946828941625602943779429022349730170976578199028835097472146188453687730908813682162167464364421412495173795443222524702317353575905515762679352710446925187209895448093873784498678735876348227350417187257757760094145939033856009360762750318940970658865538736093640535679425744417887465003392277942733319615375535988809863173460419942688997757732995224166381003248893250191049830924399642651391875156082240527709123151032998883971376055043889743758299667915731570275632108241425754692753275615791058869259388747886296382570348606605995713681757984 61
c2 =  159109976846288369334966078222223383794066455120194326409186042196244474805329857680237143012909836083508710717161305182746001278588446791791943280694544107948910983071269617559682525127363497264884919876770720802275910959879892408578785502698132510962592568983421345017771518942533049475233751681087654771102990148574980948546759086490913649446588447759260243308849011880840463875554530892936518955919305089749909244140466268764218177691645306896408539927335143111514930315516393032537429055716026948436647564634267806350788287968489763798070921854026760570911269788980947146066539919072681502564571709211786568055 79
n3 = 222264648739133867571332470866726230154413224635943013991731102577470124383847552985995792754701791772679715992526929019994579994257083764140985071890611975328484744209806353983179925260585014865958175454663919290280162302348726291510086064425783110787606286286318542925488298926778733706663246113735257943963901963655948576295718915665792095155572293279909014783939726041557401577735090500158509021889087355650089726787693168888089071057664444471720064235894159749036338984736097762223161281286635023768927853330756883745773447834776857821277453695099496922614619729281134634089306504424506495607109730276938825234 77
c3 = 211081317872257552036186402545670846155891531243107266902743084244297232304733358938682766366230728293310454758269427316834135240922935537895704821444609279398917489798233085546225002753360621948555327464293938108879236521486870713889603601361869552578470703459525538207370487183190364857087558330215992979409896960829943536617897430402246698745993128439120691465797040456414853147554947069460427971376775029732184816684770646223198456801674366726256592315708165518260364901257953026748905709956113182683387117073817299210022130500692646919536977774983611517103490624173905092989626848539520033803817915575659603510 45
(e1=e2=e3)
```

上面这道例题给了3组n和c，且说明e1=e2=e3，我们直接上代码爆破：

```
import gmpy2
import os
from functools import reduce
from Crypto.Util.number import long_to_bytes
def CRT(items):
    N = reduce(lambda x, y: x * y, (i[1] for i in items))
    result = 0
    for a, n in items:
        m = N // n
        d, r, s = gmpy2.gcdext(n, m)
        if d != 1:
            raise Exception("Input not pairwise co-prime")
        result += a * s * m
    return result % N, N
# e, n, c
e = 1
n=[151558345122742722140230869081973367560530302423230480485121316809497417802991477396429152756523612081269324464403510588914780428583674103830380036467248779045865429180173771626555925084606640155208022598517331915416759987969769062529528294248792135890928715189102401487734647077403061840323961947316011627819416865257780927253442176439253899557104677104226574616639904574493424733183128587308159599813172995669302313437832700325084051476508569976017575025882273798141537465703201611158966576900748339845393511942859359762627565239827436817587889028229629219758444364576775816395068895690818282079757217830310515978127
c1 = 549445069175361291973785391513285583409676560533201545464036103223913292201258087416431455988423183488050927580330849151520054221692185516450243328260515765258746786292701559989609832318873662678624068837676559660769228946455381172698817158314409476422832235259866638736312667043187870883639945324381026855021558641614595449198721805829811885615794319234871221108196681763424874954149520251231893947863213669616177049596694545063893238643985317109795185477384842732796700539544725823890751732846292067298384354636845967510856538604837894948953873960102607200129938875485920575804532390319723834784402860715421847230 6
n2 = 188422100202148934472784337638599174416738568826009149301061274087850946828941625602943779429022349730170976578199028835097472146188453687730908813682162167464364421412495173795443222524702317353575905515762679352710446925187209895448093873784498678735876348227350417187257757760094145939033856009360762750318940970658865538736093640535679425744417887465003392277942733319615375535988809863173460419942688997757732995224166381003248893250191049830924399642651391875156082240527709123151032998883971376055043889743758299667915731570275632108241425754692753275615791058869259388747886296382570348606605995713681757984 61
c2 =  159109976846288369334966078222223383794066455120194326409186042196244474805329857680237143012909836083508710717161305182746001278588446791791943280694544107948910983071269617559682525127363497264884919876770720802275910959879892408578785502698132510962592568983421345017771518942533049475233751681087654771102990148574980948546759086490913649446588447759260243308849011880840463875554530892936518955919305089749909244140466268764218177691645306896408539927335143111514930315516393032537429055716026948436647564634267806350788287968489763798070921854026760570911269788980947146066539919072681502564571709211786568055 79
n3 = 222264648739133867571332470866726230154413224635943013991731102577470124383847552985995792754701791772679715992526929019994579994257083764140985071890611975328484744209806353983179925260585014865958175454663919290280162302348726291510086064425783110787606286286318542925488298926778733706663246113735257943963901963655948576295718915665792095155572293279909014783939726041557401577735090500158509021889087355650089726787693168888089071057664444471720064235894159749036338984736097762223161281286635023768927853330756883745773447834776857821277453695099496922614619729281134634089306504424506495607109730276938825234 77
c3 = 211081317872257552036186402545670846155891531243107266902743084244297232304733358938682766366230728293310454758269427316834135240922935537895704821444609279398917489798233085546225002753360621948555327464293938108879236521486870713889603601361869552578470703459525538207370487183190364857087558330215992979409896960829943536617897430402246698745993128439120691465797040456414853147554947069460427971376775029732184816684770646223198456801674366726256592315708165518260364901257953026748905709956113182683387117073817299210022130500692646919536977774983611517103490624173905092989626848539520033803817915575659603510 45
(e1=e2=e3)

import gmpy2
import os
from functools import reduce
from Crypto.Util.number import long_to_bytes
def CRT(items):
    N = reduce(lambda x, y: x * y, (i[1] for i in items))
    result = 0
    for a, n in items:
        m = N // n
        d, r, s = gmpy2.gcdext(n, m)
        if d != 1:
            raise Exception("Input not pairwise co-prime")
        result += a * s * m
    return result % N, N
# e, n, c
e = 1
n=[151558345122742722140230869081973367560530302423230480485121316809497417802991477396429152756523612081269324464403510588914780428583674103830380036467248779045865429180173771626555925084606640155208022598517331915416759987969769062529528294248792135890928715189102401487734647077403061840323961947316011627819416865257780927253442176439253899557104677104226574616639904574493424733183128587308159599813172995669302313437832700325084051476509856997
```

```
59253899537104677104226574616639904574493424753181285875081595998151729956693025154378327605250840514765065997
60175750258822737981415374657032016111589665769007483398453935119428593597626275652398274368175878890282296292197
75844436457677581639506889569081828207975721783031051597812 7,
   188422100202148934472784337638599174416738568826009149301061274087850946828941625602943779429022349730170976578
78199028835097472146188453687730908813682162167464364421412495173795443222524702317353575905515762679352710446925
51872098954480938737844986787358763482273504171872577577600941459390338560093607627503189409706588655387360936405
53567942574441788746500339227794273331961537553598880986317346041994268899775773299522416638100324889325019104985
30924399642651391875156082240527709123151032998883971376055043889743758299667915731570275632108241425754692753275
56157910588692593887478862963825703486066059957136817579846 1,
   222264648739133867571332470866726230154413224635943013991731102577470124383847552985995792754701791772679715 9
92526929019994579994257083764140985071890611975328484744209806353983179925260585014865958175454663919290280162302
34872629151008606442578311078760628628631854292548829892677873370666324611373525794396390196365594857629571891566
57920951555722932799090147839397260415574015777350905001585090218890873556500897267876931688880890710576644444717
20064235894159749036338984736097762223161281286635023768927853330756883745773447834776857821277453695099496922614
61972928113463408930650442450649560710973027693882523477
   ]
c=[5494450691753612919737853915132855834096765605332015454640361032239132922012580874164314559884231834880509275803
30849151520054221692185516450243328260515765258746786292701559989609832318873662678624068837676559660769228946455
38117269881715831440947642283223525986663873631266704318787088363994532438102685502155864161459544919872180582981
18856157943192348712211081966817634248749541495202512318939478632136696161770495966945450638932386439853171097951
85477384842732796700539544725823890751732846292067298384354636845967510856538604837894948953873960102607200129938
87548592057580453239031972383478440286071542184723 06
,1591099768462883693349660782222233837940664551201943264091860421962444748053298576802371430129098360835087107171613
05182746001278588446791791943280694544107948910983071269617559682525127363497264884919876770720802275910959879892
40857878550269813251096259256898342134501777151894253304947523375168108765477110299014857498094854675908649091364
94465884477592602433088490118808404638755545308929365189559193050897499092441404662687642181776916453068964085399
27335143111514930315516393032537429055716026948436647564634267806350788287968489763798070921854026760570911269788
98094714606653991907268150256457170921178656805579,
21108131787225755203618640254567084615589153124310726690274308424429723230473335893868276636623072829331045475826942731683413524092293553789570482144460927939891748979823308554622500275336062194855532746429393810887923652148687071388960360136186955257847070345952553820737048718319036485708755833021599297940989696082994353661789743040224669874599312843912069146579704045641485314755494706946042797137677502973218481668477064622319845680167436672625659231570816551826036490125795302674890570995611318268338711707381729921002213050069264691953697777498361151710349062417390509298962684853952003380381791557565960351045
]
data = list(zip(c, n))
x, n = CRT(data)
for i in range(1,30):
    e = i
    m = gmpy2.iroot(gmpy2.mpz(x), e)[0].digits()
    print('m is: ' + long_to_bytes(m))
```

3.进阶之公因数求解

某些题目会给出多组n和c，但是e却不小，比如e=65537，这种情况下不建议使用中国剩余定理求解，可以尝试在n中寻找最大公约数gcd。

例题 BUUCTF RSA5

题：

```
m = xxxxxxxx
e = 65537
========== n c ==========
n = 20474918894051778533305262345601880928088284471121823754049725354072477155873778848055073843345820697886641086842612486541250183965966001591342031562953561793332341641334302847996108417466360688139866505179689516589305636902137210185624650854906780037204412206309949199080005576922775773722438863762117750429327585792093447423980002401200613302943834212820909269713876683465817369158585822294675056978970612202885426436071950214538262921077409076160417436699836138801162621314845608796870206834704116707763169847387223307828908570944984416973019427529790029089766264949078038669523465243837675263858062854739083634207
```

c = 97446390824333086572897876921359540078205339859689774131627572259641501891292950863739385091922496927176638871002519503989696195606289557006214694773634034292797499261667889337274426195417287349087880548324119634588172116407865115606711995781642276852444202568807946265675560598210417400163534587402213304540234401004596111172015199041203447775585180276906930906901873854185413018369220475876142712127998200299393974534369567190001529679063746488033737551153642479689099652668120063308684103632039584772593574475799301335280465057506813612929559130656921330015633365091079594680082006749414336488584289629112613732 0

n = 20918819960648891349438263046954902210959146407860980742165930253781318759285692492511475263234242002509419079545644051755251311392635763412553499744506421566074721268822337321637265942226790343839856182100575539845358877493718334237585821263388181126545189723429262149630651289446553402190531135520836104217160268349688525168375213462570213612845898989694324269410202496871688649978370284661017399056903931840656757330859626183773396574056413017367606446540199973155630466239453637232936904063706551160650295031273385619470740593510267285957905801566362502262757750629162937373721291789527659531499435235261620309759

c = 15819636201971185538694880505120469332582151856714070824521803121848292387556864177196229718923770810072104155432038682511434979353089791861087415144087855679134383396897817458726543883093567600325204596156649305930352575274039425470836355002691145864435755333821133969266951545158052745938252574301327696822347115053614052423028835532509220641378760800693351542633860702225772638930501021571415907348128269681224178300248272689705308911282208685459668200507057183420662959113956077584781737983254788703048275698921427029884282557468334399677849962342196140864403989162117738206246183665814938783122909930082802031855

n = 25033254625906757272369609119214202033162128625171246436639570615263949157363273213121556825878737923265290579551873824374870957467163989542063489416636713654642486717219231225074115269684119428086352535471683359486248203644461465935500517901513233739152882943010177276545128308412934555830087776128355125932914846459470221102007666912211992310538890654396487111705385730502843589727289829692152177134753098649781412247065660637826282055169991824099110916576856188876975621376606634258927784025787142263367152947108720757222446686415627479703666031871635656314282727051189190889008763055811680040315277078928068816491

c = 41853085294168740058312307810140924071984513859556773996685018339026234783956692794048839907251843327091524433725837010761987866352917393567708572867021071567300200043589556225110614106610589826220551997368208082038414467963052843946517144309186903894869205608346723161581464531837894121409390290293247560353580817544266451600332629243302486752161082709801570497054886202634851294809528147640028652800191851276624493183242793832777664162581422751439235321687984130110282715430852490290489974522125031117423023020654010514580665853953604684474606586729528516435471938227752183878536234536380254923891222045075559088620

n = 21206968097314131007183427944486801953583151151443627943113736996776787181111063957960698092696800555044199156765677935373149598221184792286812213294617749834607696302116136745662816658117055427803315230042700695125718401646810484873064775005221089174056824724922160855810527236751389605017579545235876864998419873065217294820244730785120525126565815560229001887622837549118168081685183371092395128598125004730268910276024806808565802081366898904032509920453785997056150497645234925528883879419642189109649009132381586673390027614766605038951015853086721168018787523459264932165046816881682774229243688581614306480751

c = 45210380110447584418911284684672330884938857508505889857085199111547780905971361261502890418934541266744681413934726623373503617122126948673116229704407077279411132638323571731417758552279737425710889745934763020841117706257642228383662775595608870429488598921385514726806545178149166092797483655806107122598566777405184770865315922331071754700682919036075057994329319896637074770179046114262137702383970057437303860800319556941584665584755997519402450391676291265767840244823484528683134174715429567782855677794359402671406799066865318624676272384010034591016371912972094224703881218025365697614144576182583435506 13

n = 22822039733049388110936778173014765663663303811791283234361230649775805923902173438553927805407463106104699773994158375040330934717613877998521683378952698052175361430789966901593138781992742187531630459152190159282381441775644769570104584677350862937139701305368455304218572505999679153239162642971241699499088969373280518194797007142930959961497377273655629940424642479166067925388494002172884690634419885477919195173971934290876133066191047711993342855077424291042095249692960568615479948783992342433635374744215357167806452076314979329436078782175170354328869672692390967039682155105304803561949970639111814506 7

c = 15406498580761780108625891878008526815145372096234083936681442225155097299264808624358826686906535594853622687379268969468433072388149786607395396424104318820879443743112358706546753935215756078345959375299650718555759698887852318017597503074317356745122514481807843745626429797861463012940172797612589031686718185390345389295851075279278516147076602270178540690147808314172798987497259330037810328523464851895621851859027823681655934104713689539848047163088666896473665500158179046196538210778897730209572708430067658411755959866033531700460551556380993982706171848970460224304996455600503982223448904878212849412357

n = 21574139855341432908474064784318462018475296809327285532337706940126942575349507668289214078026102682252713757703081553093108823214063791518482289846780197329821139507974763780260290309600884920811959842925540583967085670848765317877441480914852329276375776405689784571404635852204097622600656222714808541872252335877037561388406257181715278766652824786376262249274960467193961956690974853679795249158751078422296580367506219719738762159965958877806187461070689071290948181949561254144310776943334859775121650186245846031720507944987838489723127897223416800

24360212786712372279936867919447114223450004797511187704426369
c = 20366856150710305124583065375297661819795242238376485264951185336996083744604593418983336285185491197426018595031444652123288461491879021096028203694136683203441692987069563513026001861435722117985559909692670907347563594578265880806540396777223906955491026286843168637367593400342814725694366078337030937104035993569672959361347287894143027186846856772983058328919716702982222142848848117768499996617588305301483085428547267337070998767412540225911508196842253134355901263861121500650240296746702967594224401650220168780537141654489215019142122284308116284129004257364769474080721001708734051264841350424152506027932
n = 25360227412666612490102161131174584819240931803196448481224305250583841439581008528535930814167338381983764991296575637231916547647970573758269411168219302370541684789125112505021148506809643081950237623703181025696585998044695691322012183660424636496897073045557400768745943787342548267386564625462143150176113656264450210023925571945961405709276631990731602198104287528528055650050486159837612279600415259486306154947514005408907590083747758953115481612486548672063382055913506344094252803140295195855763083350377511201071560427811432552899377108123353524711848176585227325240496343079289894821953947331246297984913 7
c = 19892772524651452341027595619482734356243435671592398172680379981502759695784087900669089919987705675895945658643800090272599154590123082189645021800958076861518397325439521139995652026377132368232502108620033400051346127757698623886142621793423225749240286511666556091787851683978017506983310073524398287279737680091787333547538239920607761080988243639547570818363788673249582783015475682109984715293163137324439862838574460108793714172603672477766831356411304446881998674779501188163600664488032943639694828698984739492200699684462748922883550002652913518229322945040819064133350314536378694523704793396169065179
n = 22726855244632356029159691753451822163331519237547639938779517751496498713174588935566576167329576494790219360727877166074136496129927296296996970048082870488804456564986667129388136556137013346228118981936899510687585585286517151323048293150257036847475424044378109168179412287889340596394755257704938006162677656581509375471102546261355748251869048003600520034656264521931808651038524134185732929570384705918563982065684145766427962502261522481994191989820110575981906998431553107525542001187655703534683231777988419268338249547641335718393312295800044734534761692799403469497954062897856299031257454735945867491191
c = 60401197951758564075410823600235322046147238586886367248227127175727597939602463418003081497398098712343130496297329347975697810530006861856663748339784032905250725987740017313502447445907727957010651295618981165764999841859206612711236653561327191936654742355968842391080306058827778688561223782226811405705191803212869769471540422726224113039810113025862256308598927317246405746581254782871151984062538473679798837680008126053954829526986896044777194789475954421859214806526378683356732332006621006210250615008957296053056658646931229525573618715231653002060703256603530955927780377673953603292313313228236100600006
n = 23297333791443053297363000786835336095252290818461950054542658327484507406594632785712767459958917943095522594228205423428207345128899745800927319147257669773812669542782839237744305180098276578841929496345963997512244219376701787616046235397139381894837435562662591060768476997333538748065294033141610502252325292801816812268934171361934399951548627267791401089703937389012586581080223313060159456238857080740699528666411303029934807011214953984169785844714159627792016926490955282697877141614638806397689306795328344778478692084754216753425842557818899467945102646776342655167655384224860504086083147841252232760941
c = 54181203012083787131158894655799642578718141145150460960909601597378590768292585169203615778539039259541984068437573036875578483023022002292959169024302057378436018067007382347566985757086124249284804408687391200758886816720622065291565664212766111078029174189936250296906271968138303263698742497776192396033006058768659675157190797971159105786535627878990193101399459049580248824178337363048947654334894762345753567552751472565773870228733489069001496349407471045138501541181069911370726433086202846631082830522457509452289953878034321288421522515492926989474076636438958534326500293520920183728344570542711028169340
n = 28873667904715682722987234293493200306976947898711255064125115933666968678742598858722431426218914462903521596341771131695619382266194233561677824357379805303885993804266436810606263022097900266975250431575654686915049693091467864820512767070713267708993899899011156106766178906700336111712803362113039613548672937053397875663144794018087017731949087794894903737682383916173267421403408140967713071026001874733487295007501068871044649170615709891451856792232315526696220161842742664778581287321318748202431466508948902745314372299799561625186955234673012098210919745879882268512656931714326782335211089576897310591491
c = 99198804637868366849879579790915274774714449963923752440755278418655091601816665430163176349635124375103241987024162284137748941702957238847445007580146299682524465753028610742818635417283671650281760907059029769261932324275353289939302536440310628698349244872064005700644522023727670950787924296004296883032978941200883362653993351638545860207179022472492671256630427228461852668118035317021428675954874947015197745916918197725121122236369382741533983023462255913924692806249387449016629865823316402366017657844166919846683497851842388058283856219900535567427103603869955066193425501385255322097901531402103883869
n = 22324685947539653722499932469409607533065419157347813961958075689047690465266404384199483683908594787312445528159635527833904475801890381455653807265501217328757871352731293000303438205315816792663917579066674842307743845261771032363928568844669895768092515658328756229245837025261744260614860746997931503548788509983868038349720225305730985576293675269073709022350700836510054067641753713212999954307022524495885583361707378513742162566339010134354907863733205921845038918224463903789841881400814074587261720283879760122070901466517118265422863420376921532

67348455021002514608724991222366868321895496980207371766830 19
c = 14915270502032949898828292485603951848049772777471261431039572191646241875284410478373512635804406864747673804640055402646279101264831299306683440958145475921150610578434701314980750604203951110086190271990370199257012366601665306824568397578776280435952016470169169091648259102613858270555824686949616275978087843713796082300004398822730300387641050312137016330371160335943076453933759786686250845152815828510325181005874187968787521838416028250617270661335947765721542073481604939333959375548921858879660706026189790523345326867141161063104734045948793747951193345036946221379573893301900147180315760779173853846 7
n = 27646746423759020111007828653264027999257847645666129907789026054594393648800236117046769112762641778865620892443423100189619327585811384883515424918752749559627553637785037359639801125213256163008431942593727931931898199727552768626775618479833029101249692573716030706695702510982283555740851047022672485743432464647772882314215176114732257497240284164016914018689044557218920300262234652840632406067273375269301008409860193180822366735877288205783314326102263756503786736122321348320031950012144905869556204017430593656052867939493633163499580242224763404338807022510136217187779084917996171602737036564991036724299
c = 21991524128957260536043771284854920393105808126700128222125856775506885721971193109361315961129190814674647136464887087893990660894961612838205086401018885457667488911898654270235561980111174603323721280911197488286585269356849579263043456316319476495888696219344219866516861187654180509247881251251278919346267129904739277386289240394384575124331135655943513831009934023397457082184699737734388823763306805326430395849935770213817533387235486307008892410920611669932693018165569417445885810825749609388627231235840912644654685819620931663346297596334834498661789016450371769203650109994771872404185770230172934013971
n = 20545487405816928731738988374475012686827933709789784391855706835136270270933401203019329136937650878386117187776530639342572123237188053978622697282521473917978282830432161153221216194169879669541998840691383025487220850872075436064308499924958517979727954402965612196081404341651517326364041519250125036424822634354268773895465698920883439222996581226358595873993976604699830613932320720554130011671297944433515047180565484495191003887599891289037982010216357831078328159028953222056918189365840711588671093333013117454034313622855082795813122338562446223041211192277089225078324682108033843023903550172891959673551
c = 14227439188191029461250476692790539654619199888487319429114414557975376308688908028140817157205579804059783807641305577385724758530138514972962209062230576107406142402603484375626077345190883094097636019771377866339531511965136650567412363889183159616188449263752475328663245311059988337996047359263288837436305588848044572937759424466586870280512424336807064729894515840552404756879590698797046333336445465120445087587621743906624279621779634772378802959109714400516183718323267273824736540168545946444437586299214110424738159957388350785999348535171553569373088251552712391288365295267665691357719616011613628772175
n = 27359727711584277234897157724055852794019216845229798938655814269460046384353568138598567755392559653460949444557879120040796798142218939251844762461270251672399546774067275348291003962551964648742053215424620256999345448398805278592777049668281558312871773979931343097806878701114056030041506690476954254006592555275342579529625231194321357904668512121539514880704046969974898412095675082585315458267591016734924646294357666924293908418345508902112711075232047998775303603175363964055048589769318562104883659754974955561725694779754279606726358588862479198815999276839234952142017210593887371950645418417355912567987
c = 37885297842482550270816745408770163728078482227768879204534888782471379305782967974376479224945104837676511504929333560932889659437415702689438619870242766107127174091399464095139630431144639331460884300042377471634228029592502966025706493630161515813640067958942265995847080725826969967405188876067854607758510298142803593857630910789023019572264846204285136046305851315111670157631905912258842027728404565636431595078057110041139014175037511810508236382078035331114295109116161608513917547544347648195680548508238109011598212978497900056461021293540357353501244768387866615420890455096569103486767428449570088574 57
n = 27545937603751737248785220891735796468973329738076209144079921449967292572349424539010502287564030116831261268197384650511043068738911429169730640135947800885987171539267214611907687570587001933829208655100828045651391618089603288456570334500533178695238407684702251252671579371018651675054368606282524673369983034682330578308769886456335818733827237294570476853673552685361689144261552895758266522393004116017849397346259119221063821663280935820440671825601452417487330105280889520007917979115568067161590058277418371493228631232457972494285014767469893647892888681433965857496916110704944758070268626897045014782837
c = 14069112970608895732417039977542732665796601893762401500878786871680645798754783315693511261740059725171342404186571066972546332813667711135661176659424619936101038903439144294886379322591635766682645179888058617577572409307484708171144488708410543462972008179994594087473935638026612679389759756811490524127195628741262871304427908481214992471182859308828778119005750928935764927967212343526503410515793717201360360437981322576798056276657140363337007147322248483468089639923024090377060945889641702395211935894700708397904045972529908185837178691402298117122950057105404763567433789066422670457236338740116492598 42
n = 25746162075697911560263181791216433062574178572424600336856278176112733054431463253903433128232709054141607100891177804285813783247735063753406524678030561284491481221681954564804141454666928657549670266775659862814924386584148785453647316864935942772919140563506305666207816897601862713092809234429096584753263707828899780979223118181009293655563146526792388913462557306433664296966331469906428665127438829399703002867800269947855869262036714 2

```
56550075520193125987011945192273531732276641728008406855871598678936585324782438668746810516660152018244253008092470066555687277138937298747951929576231036251316270602513451
c = 17344284860275489477491525819922855326792275128719709401292545608122859829827462088390044612234967551682879954301458425842831995513832410355328065562098763660326163262033200347338773439095709944202252494552172589503915965931524326523663289777583152664722241920800537867331030623906674081852296232306336271542832728410803631170229642717524942332390842467035143631504401140727083270732464237443915263865880580308776111219718961746378842924644142127243573824972533819479079381023103585862099063382129757560124074676150622288706094110075567706403442920696472627797607697962873026112240527498308535903232663939028587036724
n = 23288486934117120315036919418588136227028485494137930196323715336208849327833965693894670567217971727921243839129969128783853015760155446770590696037582684845937132790047363216362087277861336964760890214059732779383020349204803205725870225429985939570141508220041286857810048164696707018663758416807708910671477407366098883430811861933014973409390179948577712579749352299440310543689035651465399867908428885541237776143404376333442949397063249223702355051571790555151203866821867908531733788784978667478707672984539512431549558672467752712004519300318999208102076732501412589104904734983789895358753664077486894529499
c = 10738254418114076548071448844964046468141621740603214384986354189105236977071001429271560636428075970459890958274941762528116445171161040040833357876134689749846940052619392750394683504816081193432350669452446113285638982551762586656329109007214019944975816434827768882704630460001209452239162896576191876324662333153835533956600295255158377025198426950944040643235430211011063586032467724329735785947372051759042138171054165854842472990583800899984893232549092766400510300083585513014171220423103452292891496141806956300396540682381668367564569427813092064053993103537635994311143010708814851867239706492577203899024
n = 19591441383958529435598729113936346657001352578357909347657257239777540424811749817783061233235817916560689138344041497732749011519736303038986277394036718790971374656832741054547056417771501234494768509780369075443550907847298246275717420562375114406055733620258777905222169702036494045086017381084272496162770259955811174440490126514747876661317750649488774992348005044389081101686016446219264069971370646319546429782904810063020324704138495608761532563310699753322444871060383693044481932265801505819646998535192083036872551683405766123968487907648980900712118052346174533513978009131757167547595857552370586353973
c = 38349170988872029319819687046591193416244322947593619195539375510534996074403332340181891419702463022993857425482785898960332828949812003532706371272134831721825298904959034256491167559016311016658763017998656127177503600890851791427506646034541936420530163847145158555868368723508922271767190285521137785688075622832924829248362774476456232826885801046969384519549385428259591566716890844604696258783639390854153039329480726205147199247183621535172450825979047132495439603840806501254997167051142427157381799890725323765558803808030109468048682252028720241357478614704610089120810367192414352034177484688502364022887
n = 19254242571588430171308191757871261075358521158624745702744057556054652332495961196795369630484782930292003238730267396462491733557715379956969694238267908985251699834707734400775311452868924330866502429576951934279223234676654749272932769107390976321208605516299532560054081301829440688796904635446986081691156842271268059970762004259219036753174909942343204432795076377432107630203621754552804124408792358220071862369443201584155711893388877350138023238624566616551246804054720492816226651467017802504094070614892556444425915920269485861799532473383304622064493223627552558344088839860178294589481899206318863310603
c = 67905535339912972058045619912254931053123988251876822507801975107847652264296632842204004805630393419385997833467240510762112656634686438264301090132450140358111782950819399586870874773128677202899645060978197620952444791293599988676718118197381966878846966804634586613743109946107600094742641157502049208755274344864375366235896845194115191001702914233674249385668203154865074442020224080038791184657612739167552908981129915255461141910640229913297243700646325699038561892361778940077666907826302474438953588939837358228242434871818510987872712702567808910944051219476310887299173983176523204977651017901326791718890
n = 26809700251171279102974962949184411136459372267620535198421449833298448092580497485301953796619185339316064387798092220298630428207556482805739803420279056191119436004965176741257260918768050807307465329135099825393879326921423045711719443485388876530340338582478623185945035121244940487077632029741971248657480479432560276034730643292728171616036883018794494012890797102783851007951946684617610656516473096398889240024006308939772041492139893639992794823519508520217126472881618453265113822186224096965518559662828581405708244832174956794394627377618465769810446506274924432709258823792799641962017025442383787680665919
c = 38621355660843401376986472712387941204199127152899052854850745121069261898665287042463221942460167752426501104314674830977406789498506928806795254613941681940403968845475604486278463088283349609082256858057285902980064667130174890152813215371291330117925487987744132228591454497451972730731100233035053485786751646661247476975357785866007583059289140355186724605739783968832917253017718704222902868586203614077906577106193352813742301940731147358183240589908970925174700278803200209449537961468654467296907324930970348255638602462281473101576781004296981375254861746497491571442559535194026607702167240985864542734 6
```

这里的e达到了65537，考虑在不同的n中试试寻找公因数求解，求出不同n之间的最大公约数 gcd()从而得到p或q,进而可得d，有私钥d就能得到明文。：

```
import gmpy2
import libnum

e = 65537

n0 = 20474918894051778533305262345601880928088284471121823754049725354072477155873778848055073843345820697886641
08684261248654125018396596600159134203156295356179333234164133430284799610841746636068813986650517968951658930563690213721018562465085490678003720441220630994919908000557692277577372243886376211775042932758579209344742398000240120061330294383421282090926971387668346581736915858582229467505697897061220288542643607195021453826292107740907616041743669983613880116262131484560879687020683470411670776316984738722330782890857094498441697301942752979002908976626494907803866952346524383767526385806285473908363420 7
c0 = 97446390824333086572897876921359540078205339859689774131627572259641501891292950863739385091922496927176638871002519503989696195606289557006214694773634034292797499261667889337274426195417287349087880548324119634588172116407865115606711995781642276852444202568807946265675560598210417400163534587402213304540234401004596111172015199041203447775585180276906930906901873854185413018369220475876142712127998200299393974534369567190001529679063746488033737551153642479689099652668120063308684103632039584772593574475799301335280465057506813612929559130656921330015633365091079594680082006749414336488584289629112613732 0
n1 = 20918819960648891349438263046954902210959146407860980742165930253781318759285692492511475263234242002509419079545644051755251311392635763412553499744506421566074721268822337321637265942226790343839856182100575539845358877493718334237585821263388181126545189723429262149630651289446553402190531135520836104217160268349688525168375213462570213612845898989694324269410202496871688649978370284661017399056903931840656757330859626183773396574056413017367606446540199973155630466239453637232936904063706551160650295031273385619470740593510267285957905801566362502262757750629162937373721291789527659531499435235261620309759
c1 = 15819636201971185538694880505120469332582151856714070824521803121848292387556864177196229718923770810072104155432038682511434979353089791861087415144087855679134383396897817458726543883093567600325204596156649305930352575274039425470836355002691145864435755333821133969266951545158052745938252574301327696822347115053614052423028835532509220641378760800693351542633860702225772638930501021571415907348128269681224178300248272689705308911282208685459668200507057183420662959113956077584781737983254788703048275698921427029884282557468334399677849962342196140864403989162117738206246183665814938783122909930082802031855

n2 = 25033254625906757272369609119214202033162128625171246436639570615263949157363272321312155682587873792326529057955187382437487095746716398954206348941663671365464248671721923122507411526968411942808635253547168335948624820364446146593550051790151323373915288294301017727654512830841293455583008777612835512593291484645947022110200766691221199231053889065439648711170538573050284358972728982969215217713475309864978141224706566063782628205516999182409911091657685618887697562137660663425892778402578714226336715294710872075722244668641562747970366603187163565631428272705118919088900870630558116800403152770789280688164 91
c2 = 41853085294168740058312307810140924071984513859556773996685018339026234783956692794048839907251843327091524433725837010761987866352917393567708572867021071567300200043589556225110614106610589826220551997368208082038414467963052843946517144309186903894869205608346723161581464531837894121409390290293247560353580817544266451600332629243302486752161082709801570497054886202634851294809528147640028652800191851276624493183242793832777664162581422751439235321687984130110282715430852490290489974522125031117423023020654010514580665853953604684474606586729528516435471938227752183878536234536380254923891222045075559088 62

n3 = 21206968097314131007183427944486801953583151151443627943113736996776787181111063957960698092696800555044199156765677935373149598221184792286812213294617749834607696302116136745662816658117055427803315230042700695125718401646810484873064775005221089174056824724922160855810527236751389605017579545235876864998419873065217294820244730785120525126565815560229001887622837549118168081685183371092395128598125004730268910276024806808565802081366898904032509920453785997056150497645234925528883879419642189109649009132381586673390027614766605038951015853086721168018787523459264932165046816881682774229243688581614306480751
c3 = 45210380110447584418911284684672330884938857508505889857085199111547780905971361261502890418934541266744681413934726623373503617122126948673116229704407077279411132638323571731417758552279737425710889745934763020841117706257642228383662775595608870429488598921385514726806545178149166092797483655806107122598566777405184770865315922331071754700682919036075057994329319896637074770179046114262137702383970057437303860800319556941584665584755997519402450391676291265767840244823484528683134174715429567782855677794359402671406799066865318624676272384010034591016371912972094224703881218025365697614144576182583435506 13
```

```
n4 = 228220397330493881109367781730147656636633038117912832343612306497758059239021734385539278054074631061046997739941583757040330934717613877998521683378985269805217536143078996690159313878199274218753163045915219015928238144177564476957010458467735086293713970130536845530421857250599967915323916264297124169949908896937328051819479700714293095996149737727365562994042464247916606792538849400217288469063441988547791919517397193429087613306619104771199334285507742429104209524969296056861547994878399234243363537474421535716780645207631497932943607878217517035432886967269239096703968215510530480356194997063911181450670354328869672692390967039682155105304803561949970639111814506703
c4 = 154064985807617801086258918780085268151453720962340839366814422251550972992648086243588266869065355948536226873792689694684330723881497866073953964241043188208794437431123587065467539352157560783459593752996507185557596988878523180175975030743173567451225144818078437456264297978614630129401727976125890316867181853903453892958510752792785161470766022701785406901478083141727989874972593300378103285234648518956218518590278236816559341047136895398480471630886668964736655001581790461965382107788977302095727084300676584117559598660335317004605515563809939827061718489704602243049964556005039822234489048782128494123570354328869672692390967039682155105304803561949970639111814506703
c5 = 203668561507103051245830653752976618197952422383764852649511853369960837446045934189833362851854911974260185950314446521232884614918790210960282036941366832034416929870695635130260018614357221179855599096926709073475635945782658808065403967772239069554910262868431686373675934003428147256943660783370309371040359935696729593613472878941430271868468567729830583289197167029822221428488481177684999661758830530148308542854726733707099876741254022591150819684225313435590126386112150065024029674670296759422440165022016878053714165448921501914212228430811628412900425736476947408072100170873405126484135042415250602793
n6 = 253602274126666124901021611311745848192409318031964484812243052505838414395810085285359308141673383819837649912965756372319165476479705737582694111682193023705416847891251125050211485068096430819502376237031810256965859980446956913220121836604246364968970730455574007687459437873425482673865646254621431501761136562644502100239255719459614057092766319907316021981042875285280556500504861598376122796004152594863061549475140054089075900837477589531154861248654867206338205591350634409425280314029519585576308335037751120107156042781143255289937710812335352471184817658522732524049634307928989482195394733124629798491377
c6 = 198927725246514523410275956194827343562434356715923981726803799815027596957840879006690899199877056758999456586486238000902725991545901230821896450218009580768615183973254395211399956520263771323682325021086200334000513461277576986238861426217934232257492402865116665560917878516839780175069833100735243982872797376800917873335475382399206077610809882436395475708183637886732495827830154756821099847152931631373244398628385744601087937141726036724777668313564113044468819986747795011881636006644880329436396948286989847394922006996844627489228835500026529135182293229450408190641333503145363786945237047933961690651791
n7 = 227268552446323560291596917534518221633315192375476399387795177514964987131745889355665761673295764947902193607278771660741364961299272962969969700480828704888044565649866712938813655613701334622811898193689951068758958528651715132304829315025703684747542404437810916817941228788934059639475525770493800616267765658150937547110254626135574825186904800360052003465626452193180865103852413418573292957038470591856398206568414576642796250226152248199419198982011057598190699843155310752554200118765570353468323177798841926833824954764133571839331229580004473453476169279940346949795406289785629903125745473594586749119
c7 = 604011979517585640754108236002353220461472385868863672482271271757275979396024634180030814973980987123431304962973293479756978105300068618566637483397840329052507259877400173135024474459077279570106512956189811657649998418592066127112366535613271919366547423559688423910803060588277786885612237822268114057051918032128697694715404227262241130398101130258622563085989273172464057465812547828711519840625384736797988376800081260539548295269868960447771947894759544218592148065263786833567323320066210062102506150089572960530566586469312295255736187152316530020607032566035309559277803776739536032923133132282361006000
n8 = 232973337914430532973630007868353360952522908184619500545426583274845074065946327857127674599589179430955225942282054234282073451288997458009273191472576697738126695427828392377443051800982765788419294963459639975122442193767017876160462353971393818948374355626625910607684769973335387480652940331416105022523252928018168122689341713619343999515486272677914010897039373890125865810802233130601594562388570807406995286664113030299348070112149539841697858447141596277920169264909552826978771416146388063976893067953283447784786920847542167534258425578188994679451026467763426551676553842248605040860831478412522327609410
c8 = 541812030120837871311588946557996425787181411451504609609096015973785907682925851692036157785390392595419840
```

```
06843757303687557848302302200229295916902430205737843601806700738234756698575708612424928480440868739120075886816720622065291565664212766111078029174189936250296906271968138303263698742497776192396033006058768659675157190797971159105786535627878990193101399459049580248824178337363048947654334894762345753567552751472565773870228733489069001496349407471045138501541181069911370726433086202846631082830522457509452289953878034321288421522515492926989474076636438958534326500293520920183728344570542711028169345
```

```
n9 = 28873667904715682722987234293493200306976947898711255064125115933666968678742598858722431426218914462903521596341771131695619382266194233561677824357379805303885993804266436810606263022097900266975250431575654686915049693091467864820512767070713267708993899899011156106766178906700336111712803362113039613548672937053397875663144794018087017731949087794894903737682383916173267421403408140967713071026001874733487295007501068871044649170615709891451856792232315526696220161842742664778581287321318748202431466508948902745314372299799561625186955234673012098210919745879882268512656931714326782335211089576897310591491
c9 = 99198804637868366849879579790915274774714449963923752440755278418655091601816665430163176349635124375103241987024163228413774894170295723884744500758014629968252446575302861074281863541728367165028176090705909297692619323242753532899393025364403106286983492448720640057006445202237276709507879242960042968830329789412008833626539933516385458602071790224724926712566304272284618526681180353170214286759548749470151977459169181977251211222363693827415339830234622559139246928062493874490166298658233164023660176578441669198466834978518423880582838562199005355674271036038699550661934255013852553220979015314021038838691
c10 = 14915270502032949898828292485603951848049772777471261431039572191646241875284410478373512635804406864747673804640055402646279101264831299306683440958145475921150610578434701314980750604203951110086190271990370199257012366601665630682456839757877628043595201647016916909164825910261385827055582468694961627597808784371379608230000439882273030038764105031213701633037116033594307645393375978668625084515281582851032518100587418796878752183841602825061727066133594776572154207348160493933395937554892185887966070602618979052334532686714116106310473404594879374795119334503694622137957389330190014718031576077917385384671
```

```
n11 = 27646746423759020111007828653264027999257847645666129907789026054594393648800236117046769112762641778865620892443423100189619327585811384883515424918752749559627553637785037359639801125213256163008431942593727931931898199727552768626775618479833029101249692573716030706695702510982283555740851047022672485743432464647772882314215176114732257497240284164016914018689044557218920300262234652840632406067273375269301008409860193180822366735877288205783314326102263756503786736122321348320031950012144905869556204017430593656052867939493633163499580242224763404338807022510136217187779084917996171602737036564991036724299
c11 = 21991524128957260536043771284854920393105808126700128222125856775506885721971193109361315961129190814674647136464887087893990660894961612838205086401018885457667488911898654270235561980111174603323721280911197488286585269356849579263043456316319476495888696219344219866516861187654180509247881251251278919346267129904739277386289240394384575124331135655943513831009934023397457082184699737734388823763306805326430395849935770213817533382354863070088924109206116699326930181655694174458858108257496093886272312358409126446546858196209316633462975963348344986617890164503717692036501099947718724041857702301729340139711
```

```
n12 = 20545487405816928731738988374475012686827933709789784391855706835136270270933401203019329136937650878386117187776530639342572123237188053978622697282521473917978282830432161153221216194169879669541998840691383025487220850872075436064308499924958517979727954402965612196081404341651517326364041519250125036424822634354268773895456569892088343922299658122635859587399397660469983061393232072055413001167129794443351504718056548449519100388759989128903798201021635783107832815902895322205691818936584071158867109333301311745403431362285508279581312233856244622304121119227708922507832468210803384302390355017289195967355111
c12 = 14227439188191029461250476692790539654619199888487319429114414557975376308688908028140817157205579804059783807641305577385724758530138514972962209062230576107406142402603484375626077345190883094097636019771377866339531511965136650567412363889183159616188449263752475328663245311059988337996047359263288837436305588848044572937759424466586870280512424336807064729894515840552404756879590698797046333336445465120445087587621743906624279621779634772378802959109714400516183718323267273824736540168545946444437586299214110424738159957388350785999348535171553569373088251552712391288365295267665691357719616011613628772175
```

```
n13 = 27359727711584277234897157724055852794019216845229798938655814269460046384353568138598567755392559653460940
```

```
944455787912004079679814221893925184476246127025167239954677406727534829100396255196464874205321542462025699934544839880527859277704966828155831287177397993134309780687870111405603004150669047695425400659255527534257952962523119432135790466851212153951488070404696997489841209567508258531545826759101673492464629435766692429390841834550890211271107523204799877530360317536396405504858976931856210488365975497495556172569477975427960672635858886247919881599927683923495214201721059388737195064541841735591256798700
c13 = 37885297842482550270816745408770163728078482227768879204534888782471379305782967974376479224945104837676511504929333560932889659437415702689438619870242766107127174091399464095139630431144639331460884300042377471634228029592502966025706493630161515813640067958942265995847080725826969967405188876067854607758510298142803593857630910789023019572264846204285136046305851315111670157631905912258842027728404565636431595078057110041139014175037511810508236382078035331114295109116161608513917547544347648195680548508238109011598212978497900056461021293540357353501244768387866615420890455096569103486767428449570008857457

n14 = 27545937603751737248785220891735796468973329738076209144079921449967292572349424539010502287564030116831261268197384650511043068738911429169730640135947800885987171539267214611907687570587001933829208655100828045651391618089603288456570334500533178695238407684702251252671579371018651675054368606282524673369983034682330578308769886456335818733827237294570476853673552685361689144261552895758266522393004116017849397346259119221063821663280935820440671825601452417487330105280889520007917979115568067161590058277418371493228631232457972494285014767469893647892888681433965857496916110704944758070268626897045014782837
c14 = 14069112970608895732417039977542732665796601893762401500878786871680645798754783315693511261740059725171342404186571066972546332813667711135661176659424619936101038903439144294886379322591635766682645179888058617577572409307484708171144488708410543462972008179994594087473935638026612679389759756811490524127195628741262871304427908484812149924711828593088287781190057509289357649279672123435265034105157937172013603604379813225767980562766571403633327007147322248483468089639923024090377060945889641702395211935894700708397904045972529908185837178691402298117122950057105404763567433789066422670457236338740116492598420
n15 = 25746162075697911560263181791216433062574178572424600336856278176112733054431463253903433128232709054141607100891177804285813783247735063753406524678030561284491481221681954564804141454666928657549670266775659862814924386584148785453647316864935942772919140563506305666207816897601862713092809234429096584753263707828899780979223118181800929365556314652679238891346255730643366429696633146990642866512743882939970300286780026994785586926203671425655007552019312598701194519227353173227664172800840685587159867893658532478243866874681051666015201824425300809247006655568727713893729874795192957623103625131627060251345 1
c15 = 17344284860275489477491525819922855326792275128719709401292545608122859829827462088390044612234967551682879954301458425842831995513832410355328065562098763660326163262033200347338773439095709944202252494552172589503915965931524326523663289777583152664722241920800537867331030623906674081852296232306336271542832728410803631170229642717524942332390842467035143631504401140727083270732464237443915263865880580308776111219718961746378842924644142122743573824972533819479079381023103585862099063382129757560124074676150622288706094110075567706403442920696472627797607697962873026112240527498308535903232663939028587036724

n16 = 232884869341171203150369194185881362270284854941379301963237153362088493278339656938946705672179717279212438391299691287838530157601554467705906960375826848459371327900473632163620872778613369647608902140597327793830203492048032057258702254299859395701415082200412868578100481646967070186637584168077089106714774073660988834308118619330149734093901799485777125797493522994403105436890356514653998679084288855412377761434043763334429493970632492237023550515717905551512038668218679085317337887849786674787076729845395124315495586724677527120045193003189992081020767325014125891049047349837898953587536640774868945294 99
c16 = 10738254418114076548071448844964046468141621740603214384986354189105236977071001429271560636428075970459890958274941762528116445171161040004083335787613468974984694005261939275039468350481608119343235066945244611328563898255176258665632910900721401994497581643482776888270463046000120945223916289657619187632466233315383553395660029525515837702519842695094404064323543021101106358603246772432973578594737205175904213817105416585484247299058380089998489323254909276640051030008358551301417122042310345229289149614180695630039654068238166836756456942781309206405399310353763599431114301070881485186723970649257720389902 4
n17 = 19591441383958529435598729113936346657001352578357909347657257239777540424811749817783061233235817916560689138344041497732749011519736303038986277394036718790971374656832741054547056417771501234494768509780369075443550907847298246275717420562375114406055733620258777905222169702036494045086017381084272496162770259955811174440490126514747876661317750649488774992348005044389081101686016446219264069971370646319546429782904810063020324704138495608761532563310699753322444871060383693044481932265801505819646998535192083036872551683405766123968487907648980900712118052346174533513978009131757167547595857552370586353973
c17 = 38349170988872029319819687046591193416244322947593619195539375510534996074403332340181891419702463022993857425482785898960332828949812003532706371272134831721825298904959034256491167559016311016658763017998656127177503600890851791427506646034541936420530163847145158558683687235089222717671902855211377856880756228329248292483627744764562328268858010469693845195493854282595915667168908446046962587836393908541530393294807262051471992471836 21
```

```
535172450825979047132495439603840806501254997167051142427157381799890725323765558803808030109468048682252028720241357478614704610089120810367192414352034177484688502364022887

n18 = 192542425715884301713081917578712610753585211586247457027440575560546523324959611967953696304847829302920032387302673964624917335577153799569696942382679089852516998347077344007753114528689243308665024295769519342792232346766547492729327691073909763212086055162995325600540813018294406887969046354469860816911568422712680599707620042592190367531749099423432044327950763774321076302036217545528041244087923582200718623694432015841557118933888773501380232386245666165512468040547204928162266514670178025040940706148925564444259159202694858617995324733833046220644932236275525583440888398601782945894818992063188633106 03
c18 = 679055353399129720580456199122549310531239882518768225078019751078476522642966328422040048056303934193859978334672405107621126566346864382643010901324501403581117829508193995868708747731286772028996450609781976209524447912935999886767181181973819668788469668046345866137431099461076000947426411575020492087552743448643753662358968451941151910017029142336742493856682031548650744420202240800387911846576127391675529089811299152554611419106402299132972437006463256990385618923617789400776669078263024744389535889398373582282424348718185109878727127025678089109440512194763108872991739831765232049776510179013267917188 9

n19 = 268097002511712791029749629491844111364593722676205351984214498332984480925804974853019537966191853393160643877980922202986304282075564828057398034202790561911943600496517674125726091876805080730746532913509982539387932692142304571171944348538887653034033858247862318594503512124494048707763202974197124865748047943256027603473064329272817161603688301879449401289079710278385100795194668461761065651647309639888924002400630893977204149213989363999279482351950852021712647288161845326511382218622409696551855966282858140570824483217495679439462737761846576981044650627492443270925882379279964196201702544238378768066 59
c19 = 386213556608434013769864727123879412041991271528990528548507451210692618986652870424632219424601677524265011043146748309774067894985069288067952546139416819404039688454756044862784630882833496090822568580572859029800646671301748901528132153712913301179254879877441322285914544974519727307311002330350534857867516466612474769753577858660075830592891403551867246057397839688329172530177187042229028685862036140779065771061933528137423019407311473581832405899089709251747002788032002094495379614686544672969073249309703482556386024622814731015767810042969813752548617464974915714425595351940266077021672409858645427346

n=[n0,n1,n2,n3,n4,n5,n6,n7,n8,n9,n10,n11,n12,n13,n14,n15,n16,n17,n18]
c=[c0,c1,c2,c3,c4,c5,c6,c7,c8,c9,c10,c11,c12,c13,c14,c15,c16,c17,c18]

for i in range(len(n)):
    for j in range(len(n)):
        if(i!=j):
            if(gmpy2.gcd(n[i],n[j])!=1):    #对不同的n进行 欧几里得算法，以求出最大公约数(p)
                print(i,j)                  #输出对应的n的序号
                p = gmpy2.gcd(n[i],n[j])
                print("p = ",p)
                q = n[i] // p
                print("q = ",q)
                d = gmpy2.invert(e , (p-1)*(q-1))
                print("d = ",d)
                m = pow(c[i],d,n[i])
                print("m = ",m)
print(libnum.n2s(int(m)))
```

三、低解密指数攻击

识别：e特别大

在RSA中d也称为解密指数，当d比较小的时候，e也就显得特别大了，所以发现e特别大的时候可以考虑低解密指数攻击。

例题 BUUCTF rsa2

题：

```
N = 10199180977755325347027675139926474013115768232925267350179215450700615843443200914199536724196252570595004625340018888465826249653470643879151507188586089755273665689956691573129722581725063987364337631010399217064690655724283289391490205358108750251278730332274778042021088485216658671763655905815254497947 1
e = 46731919563265721307105180410302518676676135509737992912625092976849075262192092549323082367518264378630543338219025744820916471913696072050291990620486581719410354385121760761374229374847695148230596005409978383369740305816082770283909611956355972181848077519920922059268376958811713365106925235218265173085

import hashlib
flag = "flag{" + hashlib.md5(hex(d)).hexdigest() + "}"
```

```
#该代码在python2.7下运行
import gmpy2
from Crypto.Util.number import long_to_bytes


def continuedFra(x, y):
    cF = []
    while y:
        cF += [x // y]
        x, y = y, x % y
    return cF


def Simplify(ctnf):
    numerator = 0
    denominator = 1
    for x in ctnf[::-1]:
        numerator, denominator = denominator, x * denominator + numerator
    return (numerator, denominator)


def calculateFrac(x, y):
    cF = continuedFra(x, y)
    cF = list(map(Simplify, (cF[0:i] for i in range(1, len(cF)))))
    return cF


def solve_pq(a, b, c):
    par = gmpy2.isqrt(b * b - 4 * a * c)
    return (-b + par) / (2 * a), (-b - par) / (2 * a)


def wienerAttack(e, n):
    for (d, k) in calculateFrac(e, n):
        print(e)
        print(d)
        print(k)
        if k == 0:
            continue
        if (e * d - 1) % k != 0:
            continue
        phi = (e * d - 1) / k
        p, q = solve_pq(1, n - phi + 1, n)
        if p * q == n:
            return abs(int(p)), abs(int(q))
    print('[!]not find!')
n = 10199180977755325347027675139926474013115768232925267350179215450700615843443200914199536724196252570595004625340018888465826249653470643879151507188586089755273665689956691573129722581725063987364337631010399217064690655724283289391490205358108750251278730332274778042021088485216658671763655905815254497947 1
```

```
572428328939149020535810875025127873033227477804202108848521665867176365590581525449794 71
e = 467319195632657213071051804103025186766761355097379929126250929768490752621920925493230823675182643786305433382190257448209164719136960720502919906204865817194103543851217607613742293748476951482305960054099783833697403058160827702839096119563559721818480775199209220592683769588117133651069252352182651730 85
p, q = wienerAttack(e, n)
print('[+]Found!')
print('[-]p =', p)
print('[-]q =', q)
d = gmpy2.invert(e, (p-1)*(q-1))
import hashlib
flag = "flag{" + hashlib.md5(hex(int(gmpy2.digits(d)))).hexdigest() + "}"
print (flag)
```

这里计算出来的d是gmpy库中的mpz类型，因此直接计算md5会导致摘要值错误，要把d转换成int之后再计算md5才能得到正确的值。