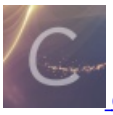
buuctf rsa刷题记录（记几种类型的RSA攻击二）

原创

舞动的獾 于 2019-12-06 23:07:55 发布 5480 收藏 30

分类专栏： crypto 文章标签： buuctf RSA

本文链接：https://blog.csdn.net/Yu_csdnstory/article/details/103430491



前言

最近学习了点儿rsa这里总结以下我的buctf rsa部分刷题记录

dp,dp泄露

场景描述：

假设题目仅给出p，q，dp，dq，c，即不给公钥e

这种参数是为了让解密的时候更快速产生的

```
dp=d%(p-1)
dq=d%(q-1)
```

例如：

buuctf RSA1

```
p = 86376337672570085670996534865410911713204915094336154475391624379112441758856678063984117905240835534451581135022277452062053276909395040329946999020532 29
q = 12640674973996472769176047937170883420927050821480010581593137135372473880595613737337630629752577346147039284030082593490776630572584959954205336880228469
dp = 65007957022168346211090423511932615306500438410562529309309496633586250168818328407280660261502646930761093548740998413804548817160977783072681169105829 29
dq = 78347226367355344901953258038647067238057403355130388913791176043888168367455609809825679567351220196300217543876276751696804359958252753916081112055004 1
c = 24722305403887382073567316467649080662631552905960229399079107995602154418176056335800638887527614164073530437657085079676157350205351945222989351316076486573599576041978339872265925062764318536089007310270278526159678937431903862892400747915525118983959970607934142974736675784325993445942031372107342103852
```

解密脚本：

```
import gmpy2
import binascii
def decrypt(dp,dq,p,q,c):
    InvQ = gmpy2.invert(q,p)
    mp = pow(c,dp,p)
    mq = pow(c,dq,q)
    m=(((mp-mq)*InvQ)%p)*q+mq
    print (binascii.unhexlify(hex(m)[2:]))
p = 86376337672570085670996534865410911713204915094336154475391624379112441758856678063984117905240835534451581135022277452062053276909395040329946999020532 29
q = 12640674973996472769176047937170883420927050821480010581593137135372473880595613737337630629752577346147039284030082593490776630572584959954205336880228469
dp = 65007957022168346211090423511932615306500438410562529309309496633586250168818328407280660261502646930761093548740998413804548817160977783072681169105829 29
dq = 78347226367355344901953258038647067238057403355130388913791176043888168367455609809825679567351220196300217543876276751696804359958252753916081112055004 1
c = 24722305403887382073567316467649080662631552905960229399079107995602154418176056335800638887527614164073530437657085079676157350205351945222989351316076486573599576041978339872265925062764318536089007310270278526159678937431903862892400747915525118983959970607934142974736675784325993445942031372107342103852
decrypt(dp,dq,p,q,c)
```

dp泄露

场景描述

题目给出公钥n,e以及dp

推导

首先dp是

```
dp=d%(p-1)
```

以下推导过程如果有问题欢迎指正

现在我们可以知道的是

```
c≡m^e mod n
m≡c^d mod n
φ(n)=(p-1)*(q-1)
d*e≡1 mod φ(n)
dp≡d mod (p-1)
```

由上式可以得到

```
dp*e≡d*e mod (p-1)
```

因此可以得到

```
d*e=k*(p-1)+dp*ed*e≡1 mod φ(n)
```

我们将式1带入式2可以得到

```
k*(p-1)+dp*e≡1 mod (p-1)*(q-1)
```

故此可以得到

```
k2*(p-1)*(q-1)+1=k1*(p-1)+dp*e
```

变换一下

```
(p-1)*[k2*(q-1)-k1]+1=dp*e
```

因为

```
dp<p-1
```

可以得到

```
e>k2*(q-1)-k1
```

我们假设

```
x=k2*(q-1)-k1
```

可以得到x的范围为

```
(0,e)
```

因此有

```
x*(p-1)+1=dp*e
```

那么我们可以遍历

```
x∈(0,e)
```

求出p-1，求的方法也很简单，遍历65537种可能，其中肯定有一个p可以被n整除那么求出p和q，即可利用

```
φ(n)=(p-1)*(q-1)d*e≡1 mod φ(n)
```

推出

```
d≡1*e-1 mod φ(n)
```

注：这里的-1为逆元，不是倒数的-1

题目：

buuctf RSA2

```
e = 65537
n = 248254007851526241177721526698901802985832766176221609612258877371620580060433101538328030305219918697643619
814200930679612109885533801335348445023751670478437073055544724280684733298051599167660303645183146161497485358633681492129668802402065797789905550489547645118787266601929429724133167768465309665906113
dp = 905074498052346904643025132879518330691925174573054004621877253318682675055421970943552016695528560364834446303196939207056642927148093290374440210503657
c = 140423670976252696807533673586209400575664282100684119784203527124521188996403826597436883766041879067494280957410201958935737360380801845453829293997433414188838725751796261702622028587211560353362847191060306578510511380965162133472698713063592621028959167072781482562673683090590521214218071160287665180751
```

解密脚本

```
import gmpy2
import binascii

def getd(n,e,dp):
    for i in range(1,e):
        if (dp*e-1)%i == 0:
            if n%(((dp*e-1)/i)+1)==0:
                p=((dp*e-1)/i)+1
                q=n/(((dp*e-1)/i)+1)
                phi = (p-1)*(q-1)
                d = gmpy2.invert(e,phi)%phi
                return d

e = 65537
n = 24825400785152624117772152669890180298583276617622160961225887737162058006043310153832803030521991869764361981420093067961210988553380133534844502375167047843707305554472428068473329805159916766030364518314616149748535863368149212966880240206579778990555048954764511878726660192942972413316776846530966590611 3
dp = 90507449805234690464302513287951833069192517457305400462187725331868267505542197094355201669552856036483444630319693920705664292714809329037440210503657
c = 14042367097625269680753367358620940057566428210068411978420352712452118899640382659743688376604187906749428095741020195893573736038080184545382929399743341418883872575179626170262202858721156035336284719106030657851051138096516213347269871306359262102895916707278148256267368309059052121421807116028766518075 1
d=getd(n,e,dp)
m=pow(c,d,n)
print binascii.unhexlify(hex(m)[2:])
```

多n的因式分解

场景描述

题目给出多个c,n,给出e，e是正常的值

解法

试图找到每个n的最大公因式，从而分解n，得到p，q

题目

buuctf RSA5

```
e = 65537
========== n c ==========
n = 20474918894051778533305262345601880928088284471121823754049725354072477155873778848055073843345820697886641086842612486541250183965966001591342031562953561793332341641334302847996108417466360688139866505179689516589305636902137210185624650854906780037204412206309949199080005576922775773722438863762117750429327585792093447423980002401200613302943834212820909269713876683465817369158585822294675056978970612202885426436071950214538262921077409076160417436699836138801162621314845608796870206834704116707763169847387223307828908570944984416973019427529790029089766264949078038669523465243837675263858062854739083634207
c = 97446390824333086572897876921359540078205339859689774131627572259641501891292950863739385091922496927176638871002519503989696195606289557006214694773634034292797499261667889337274426195417287349087880548324119634588172116407865115606711995781642276852444202568807946265675560598210417400163534587402213304540234401004596111172015199041203447775585180276906930906901873854185413018369220475876142712127998200299393974534369567190001529679063746488033737551153642479689099652668120063308684103632039584772593574475799301335280465057506813612929559130656921330015633365091079594680082006749414336488584289629112613732 0
n = 20918819960648891349438263046954902210959146407860980742165930253781318759285692492511475263234242002509419079545644051755251311392635763412553499744506421566074721268822337321637265942226790343839856182100575539845358877493718334237585821263388181126545189723429262149630651289446553402190531135520836104217160268349688525168375213462570213612845898989694324269410202496871688649978370284661017399056903931840656757330859626183773396574056413017367606446540199973155630466239453637232936904063706551160650295031273385619470740593510267285957905801566362502262757750629162937373721291789527659531499435235261620309759
c = 15819636201971185538694880505120469332582151856714070824521803121848292387556864177196229718923770810072104155432038682511434979353089791861087415144087855679134383396897817458726543883093567600325204596156649305930352575
```

52740394254708363550026911458644357553338211339692669515451580527459382525743013276968223471150536140524230288355325092206413787608006933515426338607022257726389305010215714159073481282696812241783002482726897053089112822086854596682005070571834206629591139560775847817379832547887030482756989214270298842825574683343996778499623421961408644039891621177382062461836658149387831229099300828020318551
n = 25033254625906757272369609119214202033162128625171246436639570615263949157363273213121556825878737923265290579551873824374870957467163989542063489416636713654642486717219231225074115269684119428086352535471683359486248203644461465935500517901513233739152882943010177276545128308412934555830087776128355125932914846459470221102007666912211992310538890654396487111705385730502843589727289829692152177134753098649781412247065660637826282055169991824099110916576856188876975621376606634258927784025787142263367152947108720757222446686415627479703666031871635656314282727051189190889008763055811680040315277078928068816491
c = 41853085294168740058312307810140924071984513859556773996685018339026234783956692794048839907251843327091524433725837010761987866352917393567708572867021071567300200043589556225110614106610589826220551997368208082038414467963052843946517144309186903894869205608346723161581464531837894121409390290293247560353580817544266451600332629243302486752161082709801570497054886202634851294809528147640028652800191851276624493183242793832777664162581422751439235321687984130110282715430852490290489974522125031117423023020654010514580665853953604684474606586729528516435471938227752183878536234536380254923891222045075559088621
n = 21206968097314131007183427944486801953583151151443627943113736996776787181111063957960698092696800555044199156765677935373149598221184792286812213294617749834607696302116136745662816658117055427803315230042700695125718401646810484873064775005221089174056824724922160855810527236751389605017579545235876864998419873065217294820244730785120525126565815560229001887622837549118168081685183371092395128598125004730268910276024806808565802081366898904032509920453785997056150497645234925528883879419642189109649009132381586673390027614766605038951015853086721168018787523459264932165046816881682774229243688581614306480751
c = 45210380110447584418911284684672330884938857508505889857085199111547780905971361261502890418934541266744681413934726623373503617122126948673116229704407077279411132638323571731417758552279737425710889745934763020841117706257642228383662775595608870429488598921385514726806545178149166092797483655806107122598566777405184770865315922331071754700682919036075057994329319896637074770179046114262137702383970057437303860800319556941584665584755997519402450391676291265767840244823484528683134174715429567782855677794359402671406799066865318624676272384010034591016371912972094224703881218025365697614144576182583435506 13
n = 22822039733049388110936778173014765663663303811791283234361230649775805923902173438553927805407463106104699773994158375704033093471761387799852168337898526980521753614307899669015931387819927421875316304591521901592823814417756447695701045846773508629371397013053684553042185725059996791532391626429712416994990889693732805181947970071429309599614973772736556299404246424791660679253884940021728846906344198854779191951739719342908761330661910477119933428550774242910420952496929605686154799487839923424336353747442153571678064520763149793294360787821751703543288696726923909670396821551053048035619499706391118145067
c = 15406498580761780108625891878008526815145372096234083936681442225155097299264808624358826686906535594853622687379268969468433072388149786607395396424104318820879443743112358706546753935215756078345959375299650718555759698887852318017597503074317356745122514481807843745626429797861463012940172797612589031686718185390345389295851075279278516147076602270178540690147808314172798987497259330037810328523464851895621851859027823681655934104713689539848047163088666896473665500158179046196538210778897730209572708430067658411755959866033531700460551556380993982706171848970460224304996455600503982223448904878212849412357
n = 21574139855341432908474064784318462018475296809327285532337706940126942575349507668289214078026102682252713757703081553093108823214063791518482289846780197329821139507974763780260290309600884920811959842925540583967085670848765317877441480914852329276375776405689784571404635852204097622600656222714808541872252335877037561388406257181715278766652824786376262249274960467193961956690974853679795249158751078422296580367506219719738762159965958877806187461070689071290948181949561254144310776943334859775121650186245846031720507944987838489723127897223416802436021278671237227993686791944711422345000479751187704426369
c = 20366856150710305124583065375297661819795242238376485264951185336996083744604593418983336285185491197426018595031444652123288461491879021096028203694136683203441692987069563513026001861435722117985559909692670907347563594578265880806540396777223906955491026286843168637367593400342814725694366078337030937104035993569672959361347287894143027186846856772983058328919716702982222142848848117768499996617588305301483085428547267337070998767412540225911508196842253134355901263861121500650240296746702967594224401650220168780537141654489215019142122284308116284129004257364769474080721001708734051264841350424152506027932
n = 25360227412666612490102161131174584819240931803196448481224305250583841439581008528535930814167338381983764991296575637231916547647970573758269411168219302370541684789125112505021148506809643081950237623703181025696585998044695691322012183660424636496897073045557400768745943787342548267386564625462143150176113656264450210023925571

945961405709276631990731602198104287528528055650050486159837612279600415259486306154947514005408907590083747758953115481248654867206338205591350634409425280314029519585576308335037751120107156042781143255289937710812335352471184817658522732524049634307928989482195394733124629798491370
c = 198927725246514523410275956194827343562434356715923981726803799815027596957840879006690899199877056758999456586486238000902725991545901230821896450218009580768615183973254395211399956520263771323682325021086200334000513461277576986238861426217934232257492402865116665560917878516839780175069833100735243982872797376800917873335475382399206077610809882436395475708183637886732495827830154756821099847152931631373244398628385744601087937141726036724777668313564113044468819986747795011881636006644880329436396948286989847394922006996844627489228835500026529135182293229450408190641333503145363786945237047933961690651790
n = 227268552446323560291596917534518221633315192375476399387795177514964987131745889355665761673295764947902193607278771660741364961299272962969969700480828704888044565649866671293881365561370133462281189819368995106875895852865171513230482931502570368474754240443781091681794122878893405963947552577049380061626776565815093754711025462613557482518690480036005200346562645219318086510385241341857329295703847059185639820656841457664279625022615224819941919898201105759819069984315531075255420011876557035346832317779884192683382495476413357183933122958000447345347616927994034694979540628978562990312574547359458674911910
c = 604011979517585640754108236002353220461472385868863672482271271757275979396024634180030814973980987123431304962973293479756978105300068618566637483397840329052507259877400173135024474459077279570106512956189811657649998418592066127112366535613271919366547423559688423910803060588277768885612237822268114057051918032128697694714404227262241130398101130258622563085989273172464057465812547828711519840625384736797988376800081260539548295269868960447771947894759544218592148065263786833567323320066210062102506150089572960530566586469312295255736187152316530020607032566035309559277803776739536032923133132282361006000 6
n = 232973337914430532973630007868353360952522908184619500545426583274845074065946327857127674599589179430955225942282054234282073451288997458009273191472576697738126695427828392377443051800982765788419294963459639975122442193767017876160462353971393818948374355626625910607684769973335387480652940331416105022523252928018168122689341713619343999515486272677914010897039373890125865810802233130601594562388570807406995286664113030299348070112149539841697858447141596277920169264909552826978771416146388063976893067953283447784786920847542167534258425578188994679451026467763426551676553842248605040860831478412522327609416
c = 541812030120837871311588946557996425787181411451504609609096015973785907682925851692036157785390392595419840684375730368755784830230220022929591690243020573784360180670073823475669857570861242492848044086873912007588868167206220652915656642127661110780291741899362502969062719681383032636987424977761923960330060587686596751571907979711591057865356278789901931013994590495802488241783373630489476543348947623457535675527514725657738702287334890690014963494074710451385015411810699113707264330862028466310828305224575094522899538780343212884215225154929269894740766364389585343265002935209201837283445705427110281693 4
n = 288736679047156827229872342934932003069769478987112550641251159336669686787425988587224314262189144629035215963417711316956193822661942335616778243573798053038859938042664368106062630220979002669752504315756546869150496930914678648205127670707132677089938998990111561067661789067003361117128033621130396135486729370533978756631447940180870177319490877948949037376823839161732674214034081409677130710260018747334872950075010688710446491706157098914518567922323155266962201618427426647785812873213187482024314665089489027453143722997995616251869552346730120982109197458798822685126569317143267823352110895768973105914 91
c = 991988046378683668498795797909152747747144499639237524407552784186550916018166654301631763496351243751032419870241632284137748941702957238847445007580146299682524465753028610742818635417283671650281760907059029769261932324275353289939302536440310628698349244872064005700644520223727670950787924296004296883032978941200883362653993351638545860207179022472492671256630427228461852668118035317021428675954874947015197745916918197725121122236369382741533983023462255913924692806249387449016629865823316402366017657844166919846683497851842388058283856219900535567427103603869955066193425501385255322097901531402103883869
n = 223246859475396537224999324694096075330654191573478139619580756890476904652664043841994836839085947873124455281596355278339044758018903814556538072655012173287578713527312930003034382053158167926639175790666748423077438452617710323639285688446698957680925156583287562292458370252617442606148607469979315035487885099838680383497202253057309855762936752690737090223507008365100540676417537132129999543070225244958855833617073785137421625663390101343549078637332059218450389182244639037898418814008140745872617202838797601220709014665171182654228634203769215367348455021002514608724991222366868321895496980207373176683019
c = 149152705020329498988282924856039518480497727774712614310395721916462418752844104783735126358044068647476738046400554026462791012648312993066834409581454759211506105784347013149807506042039511100861902719903701992570123666016656306824568397578776280435952016470169169091648259102613858270555824686949616275978087843713796082300004398822730300387641050312137016330371160335943076453933759786686250845152815828510325181005874187968787521838416028

25061727066133594776572154207348160493933395937554892185887966070602618979052334532686714116106310473404594893747951193345036946221379573893301900147180315760779173853846 7

n = 27646746423759020111007828653264027999257847645666129907789026054594393648800236117046769112762641778865620892443423100189619327585811384883515424918752749559627553637785037359639801125213256163008431942593727931931898199727552768626775618479833029101249692573716030706695702510982283555740851047022672485743432464647772882314215176114732257497240284164016914018689044557218920300262234652840632406067273375269301008409860193180822366735877288205783314326102263756503786736122321348320031950012144905869556204017430593656052867939493633163499580242224763404338807022510136217187779084917996171602737036564991036724299

c = 21991524128957260536043771284854920393105808126700128222125856775506885721971193109361315961129190814674647136464887087893990660894961612838205086401018885457667488911898654270235561980111174603323721280911197488286585269356849579263043456316319476495888696219344219866516861187654180509247881251251278919346267129904739277386289240394384575124331135655943513831009934023397457082184699737734388823763306805326430395849935770213817533387235486307008892410920611669932693018165569417445885810825749609388627231235840912644654685819620931663346297596334834498661789016450371769203650109994771872404185770230172934013971

n = 20545487405816928731738988374475012686827933709789784391855706835136270270933401203019329136937650878386117187776530639342572123237188053978622697282521473917978282830432161153221216194169879669541998840691383025487220850872075436064308499924958517979727954402965612196081404341651517326364041519250125036424822634354268773895465698920883439222996581226358595873993976604699830613932320720554130011671297944433515047180565484495191003887599891289037982010216357831078328159028953222056918189365840711588671093333013117454034313622855082795813122338562446223041211192277089225078324682108033843023903550172891959673551

c = 14227439188191029461250476692790539654619199888487319429114414557975376308688908028140817157205579804059783807641305577385724758530138514972962209062230576107406142402603484375626077345190883094097636019771377866339531511965136650567412363889183159616188449263752475328663245311059988337996047359263288837436305588848044572937759424466586870280512424336807064729894515840552404756879590698797046333336445465120445087587621743906624279621779634772378802959109714400516183718323267273824736540168545946444437586299214110424738159957388350785999348535171553569373088251552712391288365295267665691357719616011613628772175

n = 27359727711584277234897157724055852794019216845229798938655814269460046384353568138598567755392559653460949444557879120040796798142218939251844762461270251672399546774067275348291003962551964648742053215424620256999345448398805278592777049668281558312871773979931343097806878701114056030041506690476954254006592555275342579529625231194321357904668512121539514880704046969974898412095675082585315458267591016734924646294357666924293908418345508902112711071752320479987753036031753639640550485897693185621048836597549749555617256947797542796067263585888624791988159992768392349521420172105938873719506454184173559125679870

c = 37885297842482550270816745408770163728078482227768879204534888782471379305782967974376479224945104837676511504929333560932889659437415702689438619870242766107127174091399464095139630431144639331460884300042377471634228029592502966025706493630161515813640067958942265995847080725826969967405188876067854607758510298142803593857630910789023019572264846204285136046305851315111670157631905912258842027728404565636431595078057110041139014175037511810508236382078035331114295109116161608513917547544347648195680548508238109011598212978497900056461021293540357353501244768387866615420890455096569103486767428449570088574570

n = 27545937603751737248785220891735796468973329738076209144079921449967292572349424539010502287564030116831261268197384650511043068738911429169730640135947800885987171539267214611907687570587001933829208655100828045651391618089603288456570334500533178695238407684702251252671579371018651675054368606282524673369983034682330578308769886456335818733827237294570476853673552685361689144261552895758266522393004116017849397346259119221063821663280935820440671825601452417487330105280889520007917979115568067161590058277418371493228631232457972494285014767469893647892888681433965857496916110704944758070268626897045014782837

c = 14069112970608895732417039977542732665796601893762401500878786871680645798754783315693511261740059725171342404186571066972546332813667711135661176659424619936101038903439144294886379322591635766682645179888058617577572409307484708171144488708410543462972008179994594087473935638026612679389759756811490524127195628741262871304427908481214992471182859308828778119005750928935764927967212343526503410515793717201360360437981322576798056276657140363337007147322248483468089639923024090377060945889641702395211935894700708397904045972529908185837178691402298117122950057105404763567433789066422670457236338740116492598421

n = 25746162075697911560263181791216433062574178572424600336856278176112733054431463253903433128232709054141607100891177804285813783247735063753406524678030561284491481221681954564804141454666928657549670266775659862814924386584148785453647316864935942772919140563506305666207816897601862713092809234429096584753263707828899780979223118181009293655563146526792388913462557306433664296966331469906428665127438829399703002867800269947855869262036714256550075520193125987011945192273531732276641728008406855871598678936585324782438668746810516660152018244253008091

c =

24700665556872771389372987479519295762310362513162706025134 51
c = 1734428486027548947749152581992285532679227512871970940129254560812285982982746208839004461223496755168287995430145842584283199551383241035532806556209876366032616326203320034733877343909570994420225249455217258950391596593152432652366328977758315266472224192080053786733103062390667408185229623230633627154283272841080363117022964271752494233239084246703514363150440114072708327073246423744391526386588058030877611121971896174637884292464414212724357382497253381947907938102310358586209906338212975756012407467615062228870609411007556770640344292069647262779760769796287302611224052749830853590323266393902858703672451
n = 2328848693411712031503691941858813622702848549413793019632371533620884932783396569389467056721797172792124383912996912878385301576015544677059069603758268484593713279004736321636208727786133696476089021405973277938302034920480320572587022542998593957014150822004128685781004816469670701866375841680770891067147740736609888343081186193301497340939017994857771257974935229944031054368903565146539986790842888554123777614340437633344294939706324922370235505157179055515120386682186790853173378878497866747870767298453951243154955867246775271200451930031899920810207673250141258910490473498378989535875366407748689452949951
c = 1073825441811407654807144884496404646814162174060321438498635418910523697707100142927156063642807597045989095827494176252811644517116104004083335787613468974984694005261939275039468350481608119343235066945244611328563898255176258665632910900721401994497581643482776888270463046000120945223916289657619187632466233315383553395660029525515837702519842695094404064323543021101106358603246772432973578594737205175904213817105416585484247299058380089998489323254909276640051030008358551301417122042310345229289149614180695630039654068238166836756456942781309206405399310353763599431114301070881485186723970649257720389902451
n = 1959144138395852943559872911393634665700135257835790934765725723977754042481174981778306123323581791656068913834404149773274901151973630303898627739403671879097137465683274105454705641777150123449476850978036907544355090784729824627571742056237511440605573362025877790522216970203649404508601738108427249616277025995581117444049012651474787666131775064948877499234800504438908110168601644621926406997137064631954642978290481006302032470413849560876153256331069975332244487106038369304448193226580150581964699853519208303687255168340576612396848790764898090071211805234617453351397800913175716754759585755237058635397351
c = 3834917098887202931981968704659119341624432294759361919553937551053499607440333234018189141970246302299385742548278589896033282894981200353270637127213483172182529890495903425649116755901631101665876301799865612717750360089085179142750664603454193642053016384714515855868368723508922271767190285521137785688075622832924829248362774476456232826885801046969384519549385428259591566716890844604696258783639390854153039329480726205147199247183621535172450825979047132495439603840806501254997167051142427157381799890725323765558803808030109468048682252028720241357478614704610089120810367192414352034177484688502364022887
n = 1925424257158843017130819175787126107535852115862474570274405755605465233249596119679536963048478293029200323873026739646249173355771537995696969423826790898525169983470773440077531145286892433086650242957695193427922323467665474927293276910739097632120860551629953256005408130182944068879690463544698608169115684227126805997076200425921903675317490994234320443279507637743210763020362175455280412440879235822007186236944320158415571189338887735013802323862456661655124680405472049281622665146701780250409407061489255644442591592026948586179953247338330462206449322362755255834408883986017829458948189920631886331060 3
c = 6790553533991297205804561991225493105312398825187682250780197510784765226429663284220400480563039341938599783346724051076211265663468643826430109013245014035811178295081939958687087477312867720289964506097819762095244479129359998867671811819738196687884696680463458661374310994610760009474264115750204920875527434486437536623589684519411519100170291423367424938566820315486507444202022408003879118465761273916755290898112991525546114191064022991329724370064632569903856189236177894007766690782630247443895358939837358228242434871818510987872712702567808910944051219476310887299173983176523204977651017901326791718893
n = 2680970025117127910297496294918441113645937226762053519842144983329844809258049748530195379661918533931606438779809222029863042820755648280573980342027905619119436004965176741257260918768050807307465329135099825393879326921423045711719443485388876530340338582478623185945035121244940487077632029741971248657480479432560276034730643292728171616036883018794494012890797102783851007951946684617610656516473096398889240024006308939772041492139893639999279482351950852021712647288161845326511382218622409696551855966282858140570824483217495679439462737761846576981044650627492443270925882379279964196201702544238378768066659
c = 3862135566084340137698647271238794120419912715289905285485074512106926189866528704246322194246016775242650110431467483097740678949850692880679525461394168194040396884547560448627846308828334960908225685805728590298006466713017489015281321537129133011792548798774413222859145449745197273073110023303505348578675164666124747697535778586600758305928914035518672460573978396883291725301771870422290286858620361407790657710619335281374230194073114735818324058990897092517470027880320020944953796146865446729690732493097034825563860246228147310157678100429698137525486174649749157144255953519402660770216724098586454273 46

```
import gmpy2

e=65537
n1 = 20474918894051778533305262345601880928088284471121823754049725354072477155873778848055073843345820697886641
08684261248654125018396596600159134203156295356179333234164133430284799610841746636068813986650517968951658930563
69021372101856246508549067800372044122063099491990800055769227757737224388637621177504293275857920934474239800 0
24012006133029438342128209092697138766834658173691585858222946750569789706122028854264360719502145382629210774090
07616041743669983613880116262131484560879687020683470411670776316984738722330782890857094498441697301942752979000
29089766264949078038669523465243837675263858062854739083634207
c1 = 97446390824333086572897876921359540078205339859689774131627572259641501891292950863739385091922496927176638
87100251950398969619560628955700621469477363403429279749926166788933727442619541728734908788054832411963458817211
64078651156067119957816422768524442025688079462656755605982104174001635345874022133045402344010045961111720151 9
90412034477755851802769069309069018738541854130183692204758761427121279982002993939745343695671900015296790637466
48803373755115364247968909965266812006330868410363203958477259357447579930133528046505750681361292955913065692133
00156333650910795946800820067494143364885842896291126137320

n2= 20918819960648891349438263046954902210959146407860980742165930253781318759285692492511475263234242002509419 0
79545644051755251311392635763412553499744506421566074721268822337321637265942226790343839856182100575539845358877
49371833423758582126338818112654518972342926214963065128944655340219053113552083610421716026834968852516837521 3
46257021361284589898969432426941020249687168864997837028466101739905690393184065675733085962618377339657405641300
17367606446540199973155630466239453637232936904063706551160650295031273385619470740593510267285957905801566362500
22627577506291629373737212917895276595314994352352616203097591
c2 = 15819636201971185538694880505120469332582151856714070824521803121848292387556864177196229718923770810072104
15543203868251143497935308979186108741514408785567913438339689781745872654388309356760032520459615664930593035250
75274039425470836355002691145864435755333821133969266951545158052745938252574301327696822347115053614052423028830
55325092206413787608006933515426338607022257726389305010215714159073481282696812241783002482726897053089112822080
68545966820050705718342066295911395607758478173798325478870304827569892142702988428255746833439967784996234219610
40864403989162117738206246183665814938783122909930082802031855

n3= 25033254625906757272369609119214202033162128625171246436639570615263949157363273213121556825878737923265290 5
79551873824374870957467163989542063489416636713654642486717219231225074115269684119428086352535471683359486248200
36444614659355005179015132337391528829430101772765451283084129345558300877761283551259329148464594702211020076660
91221199231053889065439648711170538573050284358972728982969215217713475309864978141224706566063782628205516999180
24099110916576856188876975621376606634258927784025787142263367152947108720757222446686415627479703666031871635650
63142827270511891908890087630558116800403152770789280688164 91
c3= 41853085294168740058312307810140924071984513859556773996685018339026234783956692794048839907251843327091524 4
33725837010761987866352917393567708572867021071567300200043589556225110614106610589826220551997368208082038414466
79630528439465171443091869038948692056083467231615814645318378941214093902902932475603535808175442664516003326290
24330248675216108270980157049705488620263485129480952814764002865280019185127662449318324279383277766416258142270
51439235321687984130110282715430852490290489974522125031117423023020654010514580665853953604684474606586729528510
64354719382277521838785362345363802549238912220450755590886 2
c4= 45210380110447584418911284684672330884938857508505889857085199111547780905971361261502890418934541266744681 4
13934726623373503617122126948673116229704407072794111326383235717314177585522797374257108897459347630208411177 0
62576422283836627755956088704294885989213855147268065451781491660927974836558061071225985667774051847708653159220
33107175470068291903607505799432931989663707477017904611426213770238397005743730386080031955694158466558475599751
94024503916762912657678402448234845286831341747154295677828556777943594026714067990668653186246762723840100345 9
10163719129720942247038812180253656976141445761825834355061 3
```

```
n5= 22822039733049388110936778173014765663663303811791283234361230649775805923902173438553927805407463106104699 7
73994158375704033093471761387799852168337898526980521753614307899669015931387819927421875316304591521901592823814
41775644769570104584677350862937139701305368455304218572505999679153239162642971241699499088969373280518194797 0
07142930959961497377273655629940424642479166067925388494002172884690634419885477919195173971934290876133066191040
771199334285507744242914042095249692960568615479948783992342433635374744215357167806452076314979329436078782175170
```

354328869672692390967039682155105304803561949970639111814506 7

c5= 154064985807617801086258918780085268151453720962340839366814422251550972992648086243588266869065355948536226
873792689694684330723881497866073953964241043188208794437431123587065467539352157560783459593752996507185557596 9
888785231801759750307431735674512251448180784374562642979786146301294017279761258903168671818539034538929585107 5
279278516147076602270178540690147808314172798987497259330037810328523464851895621851859027823681655934104713689 5
398480471630886668964736655001581790461965382107788977302095727084300676584117555959866033531700460551556380993 98
27061718489704602243049964556005039822234489048782128494123 57

n6= 215741398553414329084740647843184620184752968093272855323377069401269425753495076682892140780261026822527137
577030815530931088232140637915184822898467801973298211395079747637802602903096008849208119598429255405839670856 7
084876531787744148091485232927637577640568978457140463585220409762260065622271480854187225233587703756138840625 7
181715278766652824786376262224927496046719396195669097485367979524915875107842229658036750621971973876215996595 88
778061874610706890712909481819495612541443107769433348597751216501862458460317205079449878384897231278972234168 0
2436021278671237227993686791944711422345000479751187704426369
c6= 203668561507103051245830653752976618197952422383764852649511853369960837446045934189833362851854911974260185
950314446521232884614918790210960282036941366832034416929870695635130260018614357221179855599096926709073475635 9
457826588080654039677722390695549102628684316863736759340034281472569436607833703093710403599356967295936134728 7
894143027186846856772983058328919716702982222142848848117768499996617588305301483085428547267337070998767412540 2
259115081968422531343559012638611215006502402967467029675942244016502201687805371416544892150191421222843081162 8
4129004257364769474080721001708734051264841350424152506027932

n7= 253602274126666124901021611311745848192409318031964484812243052505838414395810085285359308141673383819837649
912965756372319165476479705737582694111682193023705416847891251125050211485068096430819502376237031810256965859 9
804469569132201218366042463649689707304555740076874594378734254826738656462546214315017611365626445021002392557 1
945961405709276631990731602198104287528528055650050486159837612279600415259486306154947514005408907590083747758 9
531154861248654867206338205591350634409425280314029519585576308335037751120107156042781143255289937710812335352 4
711848176585227325240496343079289894821953947331246297984913 7
c7= 198927725246514523410275956194827343562434356715923981726803799815027596957840879006690899199877056758999456
586486238000902725991545901230821896450218009580768615183973254395211399956520263771323682325021086200334000513 4
612775769862388614262179342322574924028651166655609178785168397801750698331007352439828727973768009178733354753 8
239920607761080988243639547570818363788673249582783015475682109984715293163137324439862838574460108793714172603 6
724777668313564113044468819986747795011881636006644880329436396948286989847394922006996844627489228835500026529 1
351822932294504081906413335031453637869452370479339616906517 9

n8= 227268552446323560291596917534518221633315192375476399387795177514964987131745889355665761673295764947902193
607278771660741364961299272962969969700480828704888044565649866671293881365561370133462281189819368995106875895 8
528651715132304829315025703684747542404437810916817941228788934059639475525770493800616267765658150937547110254 6
261355748251869048003600520034656264521931808651038524134185732929570384705918563982065684145766427962502261522 4
819941919898201105759819069984315531075255420011876557035346832317779884192683382495476413357183933122958000447 3
453476169279940346949795406289785629903125745473594586749119 1
c8= 604011979517585640754108236002353220461472385868863672482271271757275979396024634180030814973980987123431304
962973293479756978105300068618566637483397840329052507259877400173135024474459077279570106512956189811657649998 4
185920661271123665356132719193665474235596884239108030605882777868856122378222681140570519180321286976947154042 2
726224113039810113025862256308598927317246405746581254782871151984062538473679798837680008126053954829526986896 0
447771947894759544218592148065263786833567323320066210062102506150089572960530566586469312295255736187152316530 0
20607032566035309559277803776739536032923133132282361006000 6

n9= 232973337914430532973630007868353360952522908184619500545426583274845074065946327857127674599589179430955225
942282054234282073451288997458009273191472576697738126695427828392377443051800982765788419294963459639975122442 1
937670178761604623539713938189483743556266259106076847699733353874806529403314161050225232529280181681226893417 1
361934399951548627267791401089703937389012586581080223313060159456238857080740699528666411303029934807011214953 9
841697858447141596277920169264909552826978771416146388063976893067953283447784786920847542167534258425578188994 6
79451026467763426551676553842248605040860831478412522327609 41
c9= 541812030120837871311588946557996425787181411451504609609096015973785907682925851692036157785390392595419840
684375730368755784830230220022929591690243020573784360180670073823475669857570861242492848044086873912007588868 1
672062206529156566421276611107802917418993625029690627196813830326369874249777619239603300605876865967515719079 7
971159105786535627878990193101399459049580248824178337363048947654334894762345753567552751472565773870228733489 0
690014963494074710451385015411810699113707264330862028466310828305224575094522899538780343212884215222515492926 98
9474076636438958534326500293520920183728344570542711028169 34

n10= 288736679047156827229872342934932003069769478987112550641251159336669686787425988587224314262189144629035215963417711316956193822661942335616778243573798053038859938042664368106062630220979002669752504315756546869150496930914678648205127670707132677089938998990111561067661789067003361117128033621130396135486729370533978756631447940180870177319490877948949037376823839161732674214034081409677130710260018747334872950075010688710446491706157098914518567922323155266962201618427426647785812873213187482024314665089489027453143722997995616251869552346730120982109197458798822685126569317143267823352110895768973105914915c10= 991988046378683668498795797909152747747144499639237524407552784186550916018166654301631763496351243751032419870241632284137748941702957238847445007580146299682524465753028610742818635417283671650281760907059092976926193232427535328993930253644031062869834924487206400570064452022372767095078792429600429688303297894120088336236299335163854586020717902247249267125663042722846185266811803531702142867595487494701519774591691819772512112223636938274153398302346225591392469280624938744901662986582331640236601765784416691984668349785184238805828385621990053556742710360386995506619342550138525532209790153140210388386955c11= 14915270502032949898828292485603951848049772777471261431039572191646241875284410478373512635804406864747673804640055402646279101264831299306683440958145475921150610578434701314980750604203951110086190271990370199257012366601665630682456839757877628043595201647016916909164825910261385827055582468694961627597808784371379608230000439882273030038764105031213701633037116033594307645393375978668625084515281582851032518100587418796878752183841602825061727066133594776572154207348160493933395937554892185887966070602618979052334532686714116106310473404594879374795119334503694622137957389330190014718031576077917385384675c12= 27646746423759020111007828653264027999257847645666129907789026054594393648800236117046769112762641778865620892443423100189619327585811384883515424918752749559627553637785037359639801125213256163008431942593727931931898199727552768626775618479833029101249692573716030706695702510982283555740851047022672485743432464647772882314215176114732257497240284164016914018689044557218920300262234652840632406067273375269301008409860193180822366735877288205783314326102263756503786736122321348320031950012144905869556204017430593656052867939493633163499580242224763404338807022510136217187779084917996171602737036564991036724299c12= 219915241289572605360437712848549203931058081267001282221258567755068857219711931093613159611291908146746471364648870878939906608949616128382050864010188854576674889118986542702355619801111746033237212809111974882865852693568495792630434563163194764958886962193442198665168611876541805092478812512512789193462671299047392773862892403943845751243311356559435138310099340233974570821846997377343888237633068053264303958499357702138175333872354863070088924109206116699326930181655694174458858108257496093886272312358409126446546858196209316633462975963348344986617890164503717692036501099947718724041857702301729340139715c13= 1422743918819102946125047669279053965461919988848731942911441455797537630868890802814081715720557980405978380764130557738572475853013851497296220906223057610740614240260348437562607734519088309409763601977137786633953151196513665056741236388918315961618844926375247532866324531105998833799604735926328883743630558884804457293775942446658687028051242433680706472989451584055240475687959069879704633333644546512044508758762174390662427962177963477237880295910971440051618371832326727382473654016854594644443758629921411042473815995738835078599934853517155356937308825155271239128836529526766569135771961601161362872217 5n14= 27359727711584277234897157724055852794019216845229798938655814269460046384353568138598567755392559653460949444557879120040796798142218939251844762461270251672399546774067275348291003962551964648742053215424620256999345448398805278592777049668281558312871773979931343097806878701114056030041506690476954254006592555275342579529625231194321357904668512121539514880704046969974898412095675082585315458267591016734924646294357666924293908418345508902112711075232047998775303603175363964055048589769318562104883659754974955561725694779754279606726358588862479198815999276839234952142017210593887371950645418417355912567987

c14= 37885297842482550270816745408770163728078482227768879204534888782471379305782967974376479224945104837676511
50492933356093288965943741570268943861987024276610712717409139946409513963043114463933146088430004237747163422802
95925029660257064936301615158136400679589422659958470807258269699674051888760678546077585102981428035938576309107
07890230195722648462042851360463058513151116701576319059122588420277284045656364315950780571100411390141750375111
81050823638207803533111429510911616160851391754754434764819568054850823810901159821297849790005646102129354035735
35012447683878666154208904550965691034867674284495700885745 7

n15= 27545937603751737248785220891735796468973329738076209144079921449967292572349424539010502287564030116831261
26819738465051104306873891142916973064013594780088598717153926721461190768757058700193382920865510082804565139161
80896032884565703345005331786952384076847022512526715793710186516750543686062825246733699830346823305783087698864
64563358187338272372945704768536735526853616891442615528957582665223930041160178493973462591192210638216632809351
82044067182560145241748733010528088952000791797911556806716159005827741837149322863123245797249428501476746989364
78928886814339658574969161107049447580702686268970450147828 37
c15= 14069112970608895732417039977542732665796601893762401500878786871680645798754783315693511261740059725171342
40418657106697254633281366771113566117665942461993610103890343914429488637932259163576668264517988805861757757240
93074847081711444887084105434629720081799945940874739356380266126793897597568114905241271956287412628713044279084
84812149924711828593088287781190057509289357649279672123435265034105157937172013603604379813225767980562766571403
63333270071473222484834680896399230240903770609458896417023952119358947007083979040459725299081858371786914022981
17122950057105404763567433789066422670457236338740116492598 42
c16= 17344284860275489477491525819922855326792275128719709401292545608122859829827462088390044612234967551682879
95430145842584283199551383241035532806556209876366032616326203320034733877343909570994420225249455217258950391596
59315243265236632897775831526647222419208005378673310306239066740818522962323063362715428327284108036311702296427
17175249423323908424670351436315044011407270832707324642374439152638658805803087761112197189617463788429246441421
27243573824972533819479079381023103585862099063382129757560124074676150622288706094110075567706403442920696472627
77976076979628730261122405274983085359032326639390285870367 24

n17= 23288486934117120315036919418588136227028485494137930196323715336208849327833965693894670567217971727921243
83912996912878385301576015544677059069603758268484593713279004736321636208727786133696476089021405973277938302034
92048032057258702254299859395701415082200412868578100481646967070186637584168077089106714774073660988834308118 6
19330149734093901799485777125797493522994403105436890356514653998679084288855412377761434043763334429493970632492
23702355051571790555151203866821867908531733788784978667478707672984539512431549558672467752712004519300318999208
08102076732501412589104904734983789895358753664077486894529499
c17= 10738254418114076548071448844964046468141621740603214384986354189105236977071001429271560636428075970459890
95827494176252811644517116104004083335787613468974984694005261939275039468350481608119343235066945244611328563898
25551762586656329109007214019944975816434827768882704630460001209452239162896576191876324662333153835533956600295
25551583770251984269509440406432354302110110635860324677243297357859473720517590421381710541658548424729905838008
89998489323254909276640051030008358551301417122042310345229289149614180695630039654068238166836756456942781309206
64053993103537635994311143010708814851867239706492577203899024

n18= 19591441383958529435598729113936346657001352578357909347657257239777540424811749817783061233235817916560689
13834404149773274901151973630303898627739403671879097137465683274105454705641777150123449476850978036907544355090
07847298246275717420562375114406055733620258777905222169702036494045086017381084272496162770259955811174440490126
51474787666131775064948877499234800504438908110168601644621926406997137064631954642978290481006302032470413849560
87615325633106997533224448710603836930444819322658015058196469985351920830368725516834057661239684879076489809007
12118052346174533513978009131757167547595857552370586353973
c18= 38349170988872029319819687046591193416244322947593619195539375510534996074403332340181891419702463022993857
42548278589896033282894981200353270637127213483172182529890495903425649116755901631101665876301799865612717750360
08908517914275066460345419364205301638471451585586836872350892227176719028552113778568807562283292482924836277447
64564623282688580104696938451954938542825959156671689084460469625878363939085415303932948072620514719924718362153
51724508259790471324954396038408065012549971670511424271573817998907253237655588038080301094680486822520287202413
57478614704610089120810367192414352034177484688502364022887

n19= 19254242571588430171308191757871261075358521158624745702744057556054652332495961196795369630484782930292003

```
238730267396462491733557715379956969694238267908985251699834707734400775311452868924330866502429576951934279223234676654749272932769107390976321208605516299532560054081301829440688796904635446986081691156842271268059970762004259219036753174909942343204432795076377432107630203621754552804124408792358220071862369443201584155711893388773501380232386245666165512468040547204928162266514670178025040940706148925564444259159202694858617995324733833046220644932236275525583440888398601782945894818992063188633106030c19= 679055353399129720580456199122549310531239882518768225078019751078476522642966328422040048056303934193859978334672405107621126566346864382643010901324501403581117829508193995868708747731286772028996450609781976209524447912935999886767181181973819668788469668046345866137431099461076000947426411575020492087552743448643753662358968451941151910017029142336742493856682031548650744420202240800387911846576127391675529089811299152554611419106402299132972437006463256990385618923617789400776669078263024744389535889398373582282424348718185109878727127025678089109440512194763108872991739831765232049776510179013267917188910944051219476310887299173983176523204977651017901326791718891094405121947631088729917398317652320497765101790132679171889n20= 268097002511712791029749629491844111364593722676205351984214498332984480925804974853019537966191853393160643877980922202986304282075564828057398034202790561911943600496517674125726091876805080730746532913509982539387932692142304571171944348538887653034033858247862318594503512124494048707763202974197124865748047943256027603473064329272817161603688301879449401289079710278385100795194668461761065651647309639888924002400630893977204149213989363999279482351950852021712647288161845326511382218622409696551855966282858140570824483217495679439462737761846576981044650627492443270925882379279964196201702544238378768066591c20= 38621355660843401376986472712387941204199127152899052854850745121069261898665287042463221942460167752426501104314674830977406789498506928806795254613941681940403968845475604486278463088283349609082256858057285902980064667130174890152813215371291330117925487987744132228591454497451972730731100233035053485786751646661247476975357785866007583059289140355186724605739783968832917253017718704222902868586203614077906577106193352813742301940731147358183240589908970925174700278803200209449537961468654467296907324930970348255638602462281473101576781004296981375254861746497491571442559535194026607702167240985864542734 6n=[]c=[]p=[]for i in range(1,20): n.append(eval('n'+str(i))) c.append(eval('c'+str(i)))data=list(zip(n,c))for i in range(len(n)): for j in range(i+1,len(n)): if gmpy2.gcd(n[i],n[j])!=1: print i,j#i=4,j=17p=gmpy2.gcd(n[4],n[17])q=n[4]/pphi=(p-1)*(q-1)d=gmpy2.invert(e,phi)m=pow(c[4],d,n[4])print hex(m)[2:].decode('hex')
```

e与φ(n)不互素

场景描述：

发现e与φ(n)有公约数，模逆直接报错

例如题目：

```
n1=0xcfc59d54b4b2e9ab1b5d90920ae88f430d39fee60d18dddbc623d15aae645e4e50db1c07a02d472b2eebb075a547618e1154a15b1657fbf66ed7e714d23ac70bdfba4c809bbb1e27687163cb09258a07ab2533568192e29a3b8e31a5de886050b28b3ed58e81952487714dd7ae012708db30eaf007620cdeb34f150836a4b723L
e1=0xfae3aL
c1=0x81523a330fb15125b6184e4461dadac7601340960840c5213b67a788c84aecfcdc3caf0bf3e27e4c95bb3c154db7055376981972b1565c22c100c47f3fa1dd2994e56090067b4e66f1c3905f9f780145cdf8d0fea88a45bae5113da37c8879c9cdb8ee9a55892bac3bae11fbbabcba0626163d0e2e12c04d99f4eeba5071cbeaL
n2=0xd45304b186dc82e40bd387afc831c32a4c7ba514a64ae051b62f483f27951065a6a04a030d285bdc1cb457b24c2f8701f574094d46d8de37b5a6d55356d1d368b89e16fa71b6603bd037c7f329a3096ce903937bb0c4f112a678c88fd5d84016f745b8281aea8fd5bcc28b68c293e4ef4a62a62e478a8b6cd46f3da73fa34c63L
e2=0x1f9eaeL
c2=0x4d7ceaadf5e662ab2e0149a8d18a4777b4cd4a7712ab825cf913206c325e6abb88954ebc37b2bda19aed16c5938ac43f43966e96a86913129e38c853ecd4ebc89e806f823ffb802e3ddef0ac6c5ba078d3983393a91cd7a1b59660d47d2045c03ff529c341f3ed994235a68c57f8195f75d61fc8cac37e936d9a6b75c4bd2347L
```

首先发现

```
gmpy2.gcd(n1,n2)=12120327527644543811107783655014863098833219936714394976342507913322405566177432644931575840816861543106701611662013978324877080018872656490603706071067111
```

那么可以分解出p和q1,q2

```
p = gcd(n1,n2)
q1 = n1/p
q2 = n2/p
```

得到结果：

```
p=12120327527644543811107783655014863098833219936714394976342507913322405566177432644931575840816861543106701611662013978324877080018872656490603706071067111
q1=12037827528067911684278967221392433256129944002157200272548317200308481572950474775891360447285969682243206009995242277136633522897723532096467191105943909
q2=12301580698247665838432962460247894405698817646605188562297985838079356879336309758823376086396761749681729993573203954506346863479448531269351981555913253
```

但是很快就发现了得到的e1与φ(n1)，e2与φ(n2)都不互素，求模逆无法完成，私钥d就无法得到
这时候我们推导：

```
gcd(e,ϕ(n))= b
ed≡1 modϕ (n)
e=a*b
a*b*d≡1 mod ϕ(n)
有
m^ab≡c mod n
c^bd=m^abcd≡m^ϕ(n)b mod n ≡m^b mod n
```

b我们求得是14，b*d我们可以用gmpy2.invert(a,phi)得到，所以我们可以直接$c^{bd} \bmod n = m^b \bmod n$,c我们知道，bd也知道，但是对一个大数开出14次方基本不可能，但是要是二次方或者三次方估计可行。

这时候发现了题目给了两个n,c,这里就找到了突破口
重新写一遍两个式子

```
res1 ≡ m^14 mod n1
res2 ≡ m^14 mod n2
```

进一步推导

```
res1≡ m^14 mod q1
res2≡ m^14 mod q2
```

由中国剩余定理得到

res=m^14 mod q1*q2

这里的res是上面两个式子的剩余定理的特解

```
我们可以把他当做一个新的RSA题目：

密文等于中国剩余定理求出的m特解
公钥等于14
模数已经分解为q1和q2
```

```
那么这样一看，就是一个非常简单的RSA题目了
res=c=11579189536560514527843556999236092385780870855303567302573787161860564164487269977405189773639052973932717556410994489718832123064810099564543418212811321056755271792756089424966227286905484742099862047302788442207507825486128071734126324865333135850943601987989358682570317512099546914461834470441650772334016103789019369451711310384021478033949674287133392765835965238541396568611168674772435329395131141049624649192677163789059657314916981928836150680333135 79
q1=12037827528067911684278967221392433256129944002157200272548317200308481572950474775891360447285969682243206009995242277136633522897723532096467191105943909
q2=12301580698247665838432962460247894405698817646605188562297985838079356879336309758823376086396761749681729993573203954506346863479448531269351981555913253
e=14
```

这里的e和phi又不是互素的，有公约数2，乍一看非常头疼

实际上，这里的公约数2和14比实在太小了，所以我们可以直接破解：

按照之前的思路

```
c^bd=m^abcd≡m^ϕ(n)b mod n ≡m^b mod n
```

2d可以通过7的逆元求得，由于2次方太小，所以直接对m开方即可

完整脚本

```
n1=0xcfc59d54b4b2e9ab1b5d90920ae88f430d39fee60d18dddbc623d15aae645e4e50db1c07a02d472b2eebb075a547618e1154a15b1657fbf66ed7e714d23ac70bdfba4c809bbb1e27687163cb09258a07ab2533568192e29a3b8e31a5de886050b28b3ed58e81952487714dd7ae012708db30eaf007620cdeb34f150836a4b723L
e1=0xfae3aL
c1=0x81523a330fb15125b6184e4461dadac7601340960840c5213b67a788c84aecfcdc3caf0bf3e27e4c95bb3c154db7055376981972b1565c22c100c47f3fa1dd2994e56090067b4e66f1c3905f9f780145cdf8d0fea88a45bae5113da37c8879c9cdb8ee9a55892bac3bae11fbbabcba0626163d0e2e12c04d99f4eeba5071cbeaL
n2=0xd45304b186dc82e40bd387afc831c32a4c7ba514a64ae051b62f483f27951065a6a04a030d285bdc1cb457b24c2f8701f574094d46d8de37b5a6d55356d1d368b89e16fa71b6603bd037c7f329a3096ce903937bb0c4f112a678c88fd5d84016f745b8281aea8fd5bcc28b68c293e4ef4a62a62e478a8b6cd46f3da73fa34c63L
e2=0x1f9eaeL
c2=0x4d7ceaadf5e662ab2e0149a8d18a4777b4cd4a7712ab825cf913206c325e6abb88954ebc37b2bda19aed16c5938ac43f43966e96a86913129e38c853ecd4ebc89e806f823ffb802e3ddef0ac6c5ba078d3983393a91cd7a1b59660d47d2045c03ff529c341f3ed994235a68c57f8195f75d61fc8cac37e936d9a6b75c4bd2347L
from libnum import *
import gmpy2
p=gcd(n1,n2)
q1=n1/p
q2=n2/p
assert(p*q1==n1)
assert(p*q2==n2)
f1=(p-1)*(q1-1)
f2=(p-1)*(q2-1)
tmp=gcd(e1,e2)

e1=e1/tmp
e2=e2/tmp
d1=invmod(e1,f1)
d2=invmod(e2,f2)

m1=pow(c1,d1,n1)
m2=pow(c2,d2,n2)
m3=m1%p
m2=m2%q2
m1=m1%q1

m=solve_crt([m1,m2,m3], [q1,q2,p])
print m
n=q1*q2
f=(q1-1)*(q2-1)
m=m%n
d=invmod(7,f)
m=pow(m,d,n)
print n2s(gmpy2.iroot(m, 2)[0])
```

buuuctf RSA部分题目wp

buuctf RSA3

共模攻击，解密推导和解密脚本参考

记几类RSA攻击

buuctf RSA

从公钥信息中提取出n,e,c

n可以直接分解，用yafu,或者在线分解网站都可以

yafu安装

1. windows安装

windows下安装yafu

现在最新版本是1.34版本，下载后解压即可。

解压后有yafu-Win32.exe和yafu-x64.exe，推荐使用64位的

2.yafu使用方法
把yafu的环境变量配好，在cmd下输入

```
yafu-x64
```

```
factor(n)
```

3.使用yafu的时候遇到mismatched parens

这是因为在命令行里不支持过长的位数，所以我们只要把n的值从文件中去读取即可。

新建一个文件n.txt,文件最后一行换行，避免报错

```
yafu-x64 "factor(@)" -batchfile n.txt
```

4.在线分解网站
factor
sage
Mesieve
解密脚本

```
import Crypto
import binascii
from Crypto.PublicKey import RSA
from Crypto.Util.number import long_to_bytes,bytes_to_long
import gmpy2
r=open('pub.key').read()
pub=RSA.importKey(r)
p=285960468890451637935629440372639283459
q=304008741604601924494328155975272418463
n=pub.n
e=pub.e
phi=(p-1)*(q-1)
d=gmpy2.invert(e,phi)
print(d)
c=open('flag.enc','rb').read()
c=bytes_to_long(c)
#print(type(c))
#print(c)
m=pow(c,d,n)
print(long_to_bytes(m))
#print(binascii.unhexlify(hex(m)[2:]))
```

或者使用openssl提取信息，参考
https://blog.csdn.net/Yu_csdnstory/article/details/90759717

buuctf RSA&what
共模攻击，得到的密文为base64隐写，解密得到flag
解密脚本

```
import gmpy2
from Crypto.Util.number import bytes_to_long,long_to_bytes
import base64
```

```
import base64
from libnum import n2s,s2n
n=785095419718268286865082143048169854470772937668193987280464111669178108204847593142910289764982236612293950094740631737051626270376109935396177519054430392782275835046048082519310838189094676132775878745457610743644275499665555193719138598753135772822430531500562746677980496946957036603135329331654493129497255817089654172730555822162959945876009759701248114962700808969770769460001027010302609905981814664472080547133915263137006813410939222403174281735990316241251551882164894768256061915211820349691203432876911813003996835154148092627004575258766918081802577303517076736603806989738846423068988100006336848787154028231435491398507329828974596980896495611907468506981302994580802555823126968731492100282408981378228884925599576650679365733563675897845931190166240724338727445374320059116684944557333306893851412146530918880177820490434348626203067834361698565641759298711006699134389808992195793298977532334509347701939154347914277286365862180498746172317053080037200662693127291357641756986110688084040541255815401149564636032402224979193846917187440140025542016023959693129999941595995360263598790602180564963457454574939197713376011774498990665798576300363508710904526498307750296954885755749850784285600542531808637253641476e1=1697e2=599#print(gmpy2.gcd(e1,e2))c1=[41262952616315074861932809130674226767574057801180006247717418978215127397078353122757975854036497048535015794432157910823222107239713593403406448149788707964113180883824274381151145135502443698305057202092506564435556643462561813320302421594153492611389293798852091893906144160691555651624605734958992149435138316003628082602460535187840805618090775997380411726300255492304175058754881974634681396667303418291332550782621996192393210052630528989496521660825425218839858013954518968187582408945619504498458582493838452190533428990642245415297683486730469329246667635576017323240775325625631754619017199527625892461353317989846768335893475199965519679016843834319822918374709110826298877659858609744709324571850262293294975336628234767258858873839342596887193772615000676401522431518310648303975593582965021189182246986957349253156736526071639973844039068996404290548474640668851856078201093335425412842295604919065487301340901573809617549185106072798799159726375235125260509158832996701927878713084753334549129580912412168594170659605421750204835970231909591063407612779337478065175988365401590396247576709343727196106058477166945670117868989025903023998142850338956985816131805349549059377047477131270847579095628384569645636821650,4946443479437105452246788319415890865727007924654595587707822135500697094585683496869986605418101668720340415847674871501401111517882214600278971932482734616074110278159848839693962206263586250417815582778049302126542967040558906837969413277127587977708200066232891469900001149152935396397668469102740342456077462307408519381583905622860570022231776096063763290076768454501425379307981482584287014664154832326706598157910646813844064943882377423307862255573039880254680368200829597120507330958605468604685758570846160691320510948829192537452347620297591247763480475877558971235751235069761409005652388407528418567136133682500719261718732138979147941154668907191232994699640194508992914107607621798369465709455552952881846981845550183686877084326122862484760737580671754817711990665815728701754600160171004144793464370342917848371322408913219316014944149089277132084489272210957458023800144418411398823913784104387648845979387738687718962523295174400686735324683728408305102185852554320006902652260165733135709779450838792149613940870655583761588269382576648405709522338328528693287855681754345162477203565202426022995103743174881827387327000788796657459096037664821001380014170236806477178243231433888578175957661721528834842747182483,1529422835997283071681441373701272126726118940720387321260410981026288310530009867592602712106719220705559480236885965754158229840261590105744043594746704286785182621750338805139843729097489927278283816944167767409810217305453740029740378965349445671245432727376183806467710718048787965859837833605537618283258178202602048200044219798818710272555626909523349006166756065249335574402636482335147572002635214995083739750034313068474530467140276871083969457198034444449540793084049471262163955265512921047220478781783720788603307185727785799793225525131598283789216442129820207394591918777985678589271725174670453731500377136973785489659517048515259101367694241813427853403765446784063352891681227526723015535207773658313099258767094165469538228702397126152998738452084382969577802931178643122740918901920581835191157275714555699360664346433619680235020461605628649724601680010500314304612060867349619675872055277677279660967053705633199689432277926763528147248155981983904242401717171830321405972056848493923937014403816154135425418276997977194875941310293398777340164450693020516489177382651316178373638660478348444634574495711946979923179636832492757069449667945331392756234565669024041462443130464624859922604652470236413109596433579717988936247951265489157583697956031893477858854186991051529161879478488281744062318600470906120960002282886511477294555606503083169449335174864424180701080203993329996226566203834693869525797695969610065991941396723959032680019082506816443041598300477625793433080664346470586416385854692124426348587211026568667694805849554780794033764714016521711467557284846737236374990121316809833819996821592832639024026411520407330206281265390130763948165694574512140518775603040182029818771866749548761938870605590174330887949847420877829240131490902432602005681085180807294176837646062568094875766945890382971790015490163385088144673549085079635083262975154206269679142412897438231719704933258660779310737302680265445437771977749959110744959368586293082016067927548564967400845992380076107521
```

```
27555665317606288233745197187637403782955855355917528873392229473971841163267067999215154311856367408257077827423737834757810526742572929102138439861329874668100272750524167746933634461845189018992025028286703094526223475329326788749908099306825757386538762893841514968071941463086143688210066606268709897846970451602310694284589611077512077710937773946168563052933356038921783275207565543333659751142359811734513681316804048508327731473330137169203,12311135365040115855663998345987066305729787199292705388697122477352963652511062818371574879598752511317754009281411992870827229037033653711038102313463775974071614096966218326937067663032558338528499494316469239745910319543496805737747461050021680137539470378124903935136881695822740965793409174150935715232838296068451509394555247946138228191396195674515426068602999782756507576870377489575056157515514360629711639166638570589913808569391324631377803362721031226895973739455351089472009916519398133377590753110723255690947815644145789979751569434881696176279670344350285610107943058554799749600109892660049972838911386289483378966921363033298869366988934048243061329149061380320448475147067668604100277255611721361215232260673715085811612293653913179511126351311456979453280588664308729991819663511303777713866691429698604054927455983521450530061825610550876402646151887657938715988198354466725853706495461609775039983966106579788310373169431485230184827209238863711495005921692296984208264852703553809005409389036564767611974899524341633780566655750134523405696847614260849183043806540121975168868737370939005752191094273663212672971160625615839996368299088147317821606082702137377659890128195852765554331841366427792149272318598,36869806815936046911848195817405817350259890871483063184373728397968909458432625046025376290214729914038387534731762237978339011724858818860181178811639468996206294711495853807311240013786226884265118119546377272154555615363105236192878292703331473547623021744317034819416624562896226194523639793573028006666236271812390759036235867495803255905843636447252225413871038762657801345647584493917576263471587347202664391908570140389126903204602391093990827188675090199750617303773574821926387194478875191828814971296674530519321530805302667925998711835019806761133078403281404889374663875077339168901297819436499920958268483684335998301056068380228873524800383911402490807139268964095165069610454677558808756444381542173782815227920906224931028457073652453777424387873533280455944646592996920617956675786286711447540353883400282402551158169958389450168079568459656526911857835375748015814860506707921852997096156275804955989964215077733621769938075413007804223217091604613132253046399456747595300404564172224333936405545921819654435437072133387523533568472443532200069133022979195685683508297337961701169394794966256415112246587706103819620428258245999539040721929317130088874161577093962579487428358736401687123174207198251449851429295]

c2=[59216907937209372730610021601139585782564632393428948097607362903754392290209812090113845446217715999637665417624823897913252872832759030109896613998315798061232056349654612864496773100071669770510407903915627671487214746335081130339326062270702495254350989169224624627796582341446032681124004806054365658868860445235389977906882512091028216700471533976318773479718032697613221332505469716532047916635656251802980592774165660517480972639756577227156206607807610549174590398659787740037020671895497528872107204833367860905500813580908930422901536434849092497409740373462726529763717181884946176652369159524161387870986550643658826899916334294507049533815360052053749853945739658280469295929661271575257314029613578493320614609143661797959974977433069994663759140635628940971608403445104909471520219620348608836879174410762927164732027325983691531279429724658950100866629916571772250770286603345421578324002550435615766445486175528628577776358517775179625265500820638302470788307751374586331207934979027509408070750239286694632579691445060226446258872205229743082768175082734909432396833767031127293378583850649376115667223821665435911506351891489985627506615492005617098615432522564204152887767244129985681083657783356557756654335186,37394064641683274087873325570756775303371658344840200078920276751192021038283034395555365411148672833398055731979936251496062787901679749138981200776883273097991623064764187275900190684674797763167570431017944885712816038570118589291452305366936653440886373430563522262559098600642048609255042730108698456312648081498702498059461354297831012924767882669141833530057757752795162369642643549783522816708473800775091427025100192132952147904766284865080898999608560019730936141086323852680212787752376726292151515098499856013664715486579116331650307328522396621644102563745222904351009732372438105697630228813684326016392270669291303522244549671600888894658153500454635574421168039073125730994190258730335313995110224486527029541447448879833540463045848970663980518657387481458673674623235884967747753367196834415424296328941556948757989591066099904357873746130040693782892481800265829276988218166878450143925413199684894812078156215886149588382784813942586224957645468913368100954936131446081865899595909822899570220226864963536310554997593239533507652113760428852008204012128661492298655465270005614896651417893595236303696321761987989967138360463841656795042135054620443490211315672000628272088959128885027107607494192771567830605717652763092646062293657138564984175821445341684903941240108744344431710185709090471148553810705882305608584053907334592079287136823235547539457109838059683546850999734050560433373054779956099882298974747378030777971771552278772447172476649409078397103059467101316820971768672044857958261837845956797902782227191865316962242815385619890781004022434027036241343249502967212326137540092715983153776070997477870816058325261378435823485858317454477797924288793882757360483776680199838137999907641644468389107809388968605548270983866835612091604035212301901925508451376
```

```
960380381494777455402871781463895141629127469677151547408635148210795315025361692278726239845037624912699644026
382478413080973933173079111305142716133389111399235545279259017424722601848670061556859163943895466553927946412 5
237501665827340057333783284682505689449459122384958779297171017223146781201722284937879649040725839057210747667 1
173221581556101296039453719575783295926860377511293286210594572085395928518752176355791535642811387689327687977 5
603217718981852114599706699524551973934242045743122744146361596971245034059345915315495232135483464496114770357 5
365762005114909224132081781498693478029887865134514864114098871645160650620849175561207124650742064358314981136 05,
878643717869894032287788980700995761677735184497986972696235655324405091128398428096066576164931089523045507297 74314151020539877359693265539789948531624830515446568732945551160099955920431830702087062581648405405995770720971 04139505857517663273929851202628854185356185647194933800084230503413037858893307713037149307477830536758283681093 51761782016918142079610533868158223078831810842813205179376101495283733045626227282862735570146474057819796633 61312730703725564728682349635591764235332791244001962183887038809182474862963742575912521463988513016318375237893 08729773517053259212525494555880921052679512582051516604297098204363525081039382358483926727008679327719083138866 59692919118636303820971602309607380435755593302640182127744245277191532485638767600679314990293842289932538625019 39333775851437747201193327927318114483038116984938789379939075505209306917960557948571034365557002859259588243663 32426527654452895431758715126580164902410286422637215098476316042367916779431052267545769495994723721129943616294 87964230554589491291463298045503175587908740157531069976540847360616672713793422451599841662512221305620880009509 07793310315069927265011615167470243846306273447271400492610366837850680400274004554796471669353634944766085058O, 20531496220451150035285837225413253316754996082549894961851484157070319926486743158075467427599055447814063704144 27842111391746883257447120035947621456863890934062044010795443059281736346976175772415034838334682726635263432655 55378529421773348880252837486115761715342514618473495665056282905872241508696403864376233712497431652603966752206 68330214280564636890693057514062861000391913199929585550121511139329481821879998270328930459698907047500008117551 00854322902645020237368991047463168307422269463950270298208257918318708573826472213227346050262100730939183312474 94943075556003355509423405265362813720366121387138810988663031694255019989784000088298730809655920093711762086682 90074288903681417933657472279670688597862835627506340169978450918788539270346340385928840299573889292189531738082 16640873404638142351646769432897138542190731481428348932261938657004618355657238398077727717334920933068342434365 81797810150722593785761304422229849630711662076425855898220615972824678508680507379577264237137616942318794970 37175627546427449730638216214828463003483408928375620315193290871300316930139260521382533279767663839278693750409 41949328075336845150880265827222076762476639063928530843360725525328270238376214975593551892207558463751249481 9,
271453634732502613378948161256470991260052778799128789839624515809143527363206813219580098196957510291648493698144 44975673920652512448440749927346694902962939973861983592803166559046916393674822032100518091259044104315069252383 74843856343243276508280641059690938930957474434518308646618959004216831130099873532714372402117796666560677624822 50915928767543241301647894859464087209168848214900442636394604851748005290630629012624286603424947804040635194 00882310814561091957994429967996416471675526895646133464152479068520555884983056659284508287561521030966292747606 01528737639415361467941349982213641454967962723875032638267311935042334584913897338553953961877439389588793074211 50259723846554288933536355905236818021201320617271256122135283389164065902025352758470646520548640899076275923 08421920283810485634377245284091747900227525575127957827131251661583298807027307699571854285220114301448402322564 19113631679343171680631630775266488738173707357123139368825087043785842169049943237537188129367275730984789479 90910339793711383782457513702101233346155217668757001044574426837384074289929997737283404192510285371896483122525 04072795784650085375426596736856862427733791319048908651106991904515344454345339191276589768747210295861681062007]

fm=[]
#c=list(zip(c1,c2))
c3=[]
c4=[]

k,s1,s2=(gmpy2.gcdext(e1,e2))
if s1<0:
    s1=-s1
    for i in c1:
        a=gmpy2.invert(i,n)
        c3.append(a)
else:
    s2=-s2
    for j in c2:
        b=gmpy2.invert(j,n)
        c4.append(b)
#print(c3)
```

```
c=list(zip(c3,c2))
for f,h in c:
    m=(pow(f,s1,n)*pow(h,s2,n))%n
    fm.append(m)
res=''
for k in fm:
    #print(k)
    res=hex(k)[2:]
    print res.decode('hex')
    print '\n'
```

buuctf RSA4

低解密指数广播攻击，问题在于它的n，c，是5进制，转换为十进制，直接解密。

```
import gmpy2
import libnum
n1= 331310324212000030020214312244232222400142410423413104441140203003243002104333214202031202212403400220031202
142322434104143104244241214204444443323000244130122022422310201104411044030113302323014101331214303223312402430 4
024044130332431321010104222401331222114004340232222142314024034032000122210233413333400423431223021134102101102 2
123324130302443133000130340402010444244312013000033411004243201020340144040401000344200122304221144200141300 4
c1= 310020004234033304244200421414413320341301002123030311202340222410301423440312412440240244110200112141140201
224032402232131204213012303204422003300004011434102141321223311243242010014140422411342304322201241112402132203 1
011312212230040220031200021102300233411432014043113403111342301402314122013333331424024231343332113021024131111 1
142443003244012334003404431422340040122411132300024223442044124041102102310022200312321434303012203230104224 3

n2= 302240000040421410144422133334143140011011044322223144412002220243001141141111412322333133130442111302123120 4
322233120121444434210041232214144413244434424302311222143224402302432102242132244032010020113224011121043232143 2
212034242431340443140222120243431000423420024323311443002142124140334141200043442113302240203012230333432424403 1
204240122301242232011303211220044222411134403012132420311110302442344021122101224411230002203344140143044114 4
c2= 112200203404013430330214124004404423210041321043000303233141423344144222343401042200334033203124030011440014 4
210112103234440312134032123400444344144233020130110134042102220302002413321102022414130443041144240310121020100 3
101043342042344124114244203212111122320311213303103334144234333433220244001212003333304322234214333441220230124 4
001304140142320221012402443104001341431312112343342411311341442204333042200231414411113414204433340411224034 4

n3= 332200324410041111434222123043121331442103233332422341041340412034230003314420311333101344231212130200312041 0
443244311410330043331100210130201400200112220123000200413420400004002220210223122111314112124333211132230332124 0
224231412140313031444441344030244201114232444240300300033402130321213032133430204013042433300013140230301210341 1
333440444042124224011310320301334123133000433204030244001132400413032403432343014310240144013024232142402032 3
c3= 100134441201411303224332041240022422243323340111242100124402414023421004103311314413032420110021013230404033 1
111204213044222222003244022442433224224444140433421301111113300222132030303244221011330322120420422431014343422 0
320412104211321210421242333033113431131111414320001124000211131212223434000340331204040104302143311203133432432 2
123304112340014030132021432101130211241134422413442312013042141212003102211300321404043012124332013240431242
n=[]
c=[]
for i in range(1,4):
 n.append(eval('n'+str(i)))
 c.append(eval('c'+str(i)))
for i in range(len(n)):
 n[i]=int(str(n[i]),5)
 c[i]=int(str(c[i]),5)
#print(n)
def CRT(data):
 plian=0
 m=1
 for x in data:
  m=m*x[1]
 for z,n in data:
  mi=m/n
  mr=gmpy2.invert(mi,n)
  plian=plian+z*(mr*mi)
 return plian%m
data=list(zip(c,n))
f=CRT(data)
for e in range(2,97):
 m2,h=gmpy2.iroot(f,e)
 if(h==1):
  print m2
  print hex(m2)[2:].decode('hex')
```