N1CTF2020crypto Easy RSA?

原创

前方是否可导？ 于 2020-10-23 20:30:00 发布 352 收藏 2

分类专栏： sage RSA

本文链接：https://blog.csdn.net/weixin_44110537/article/details/109221497

sage 同时被 2 个专栏收录

7 篇文章 1 订阅

订阅专栏

RSA

40 篇文章 7 订阅

订阅专栏

task.sage

```python
from Crypto.Util.number import *
import numpy as np

mark = 3**66

def get_random_prime():
    total = 0
    for i in range(5):
        total += mark**i * getRandomNBitInteger(32)
    fac = str(factor(total)).split(" * ")
    return int(fac[-1])

def get_B(size):
    x = np.random.normal(0, 16, size)
    return np.rint(x)

p = get_random_prime()
q = get_random_prime()
N = p * q
e = 127

flag = b"N1CTF{**********************************}"
secret = np.array(list(flag))

upper = 152989197224467
A = np.random.randint(281474976710655, size=(e, 43))
B = get_B(size=e).astype(np.int64)
linear = (A.dot(secret) + B) % upper

result = []
for l in linear:
    result.append(pow(l, e, N))

print(result)
print(N)
np.save("A.npy", A)
```

代码审计后发现首先要分解N然后还原linear.
从而得到一个LWE问题.(c=a*s+e mod p)
进而尝试解出secret
记第一次得到的随机值为gen_p 第二次得到的随机值为gen_q
易得:

$gen\_ = k1 *$

```
x=3**66
M=[]
N=32846178930381020200488205307866106934814063650420574397058108582359767867168248452804404660617617281772163916944703994111784849810233870504925762086155249810089376194662501332106637997915467797720063431587510189901
for i in range(9):
    temp=[0]*9
    temp[i]=1
    if i<8:
        temp[-1]=x**(8-i)
    else:
        temp[-1]=-N
    M.append(temp)
#print(M)
M=matrix(M)
res=M.LLL()
ans=res[0]
R.<x>=PolynomialRing(ZZ)
f=ans[0]*x^8+ans[1]*x^7+ans[2]*x^6+ans[3]*x^5+ans[4]*x^4+ans[5]*x^3+ans[6]*x^2+ans[7]*x-ans[8]
print(f.factor())
x=3**66
gen_p=2187594805*x^4 + 2330453070*x^3 + 2454571743*x^2 + 2172951063*x + 3997404950
p=gcd(N,gen_p)
print(p)
print(N//p)

#122286683590821384708927559261006610931573935494533014267913695701452160518376584698853935842772049170451497
#268599801432887942388349567231788231269064717981088022136662922349190872076740737541006100017108181256486533
```

得到p,q后,就可以还原linear了.
在还原linear后.会得到
linear=A*secret+B (mod upper)
即: A*secret=linear-B (mod upper)
可以得到的是,A*secret会是一个向量,而linear-B也是一个向量.我们可以在A*secret所在空间找到一个距离linear最近的向量,由于B比较小,同时这里的维度不是很大,所以A*secret很可能就是这个向量.这样的话,就可以还原secret了.转置一下为并简写为

$$S\ A = L - B\ (mod P)$$

```
from sage.modules.free_module_integer import IntegerLattice
def CVP(lattice, target):
    gram = lattice.gram_schmidt()[0]
    t = target
    for i in reversed(range(lattice.nrows())):
        c = ((t * gram[i]) /(gram[i] * gram[i])).round()
        t -= lattice[i] * c
    return target - t
p=122286683590821384708927559261006610931573935494533014267913695701452160518376584698853935842772049170451497
q=268599801432887942388349567231788231269064717981088022136662922349190872076740737541006100017108181256486533
import gmpy2
phi=(p-1)*(q-1)
e=127
n=p*q
d=gmpy2.invert(e,phi)
import numpy as np
A=matrix(np.load("A.npy"))
upper = 152989197224467
result=[102884774254035234857642849445646067933232338049413242002007822001582093973975319027932944390139060118022690205761991194178081652415377075586381358165709590644956764326599231148212400505766483132442131505026412566570, 60085672877069184881540258674658975759994351089625185485404543051225134400002086441141135036547807832712576968452393340137625427253106884740308863041844264555650240156451318576951838242366179146626453658121615312230, 12077110016
```

7507103615308965954497700848637047185897213169811420954574028535993259319908011987659857552889069347276260284855
15459385285948978327190995149566652870795034130529018785797647118734723046605772519331279730, 7389313281825513530
3141036681956909835744340069520835496959725518092759347794424324053131414415786913182958291870485070034852573789
20473632445521021667536732869373513125507923359405810054919686690389603066930301975, 1072936904760391451784022637
4468391903294874291534302197445023809394235464749950452651157502399695242979556233732973657417215215539522477839
337904741946623476747304944452454042412038128184644747708443175205707513929, 219134122751100100444659223572562538
5790352999984678782929448097848078942232978270488813434743709743706622345729114875875558823339127353146128406108
6447508597320450213978481681541380383662771332661455056480161893110, 51874963823939953864324745835949310041923322
7169011574949683429098116234490364968146933107849124571611687677055547460576818932852643065641942884071844552570
2380018135498444181161596204954417669702620639870271315714, 38547253349686051155093029363415626706363242820950219
7050533920977506534355369945487378058314752893724058546074155480555667155863994928341882229756530243957773632368
1629390362416040300962967336578737241968508194622, 31992950003597355018507676089121630852144072864760243643221871
9424278074769569300470608087242363855838052238484939275831498554152379253386307907549835464929602750767874624239
60739889523663905861923759915204826434254, 2527482235052981674439924251119533830936363280746293402795177780704631
4661965632355692599416024094696391113072124828734858170701497375788670686582207694302991627701339649377844007202
181304640190749965046575636916464, 992124257957506931668967453533399745393238603975650633162799796490826098740327
9790768310766586220195079797477942795615423763764068800487032933469748674168491068115793357586152642244881397742
333467011936146126178726, 327962741672536639540658257321654029821683823358475564451396534888830447053876798126910
2112209205060703614008562159310556759248318813419362904704101359090685277436596996658197722476735437797085363408
2383152529845069, 26420075175810982250843138759497875863437200398400217382205856762645400687177535779719247269987
6931243309918993812729989212757973184486852614976776659391380854746543416867191057137520359300582329091374297320
62178119, 2140920469926086671636137889829754826891342986807192961718938273560999197183112266611138082553724005628
4316962060089791177286322723056378163364916212011013258517898818809936966816854970125645088959487022798080538324
, 243868008692695899526107282628077536022563625612445765636560813479235770200841435699595043804087463958736013246
13603031294139347238025102893045806354381129937740558622461243125471959735920766065526598675543194342392, 1142255
2671008481701371830020382307162478514636107662749165647382845802313862169526316114854920094904140230710271530512
068821363911924373138913107206944533517640367634369066861173606190006161032180585448745775032342, 219439292763003
2414325758193339713465508649935956269163084592382007205093955991550537857024471710323709971044569548477000791804
4611458743396533434933292513573107644105378585709321552310292959297898322419259520011660, 59870965995043033594836
7829260972486821939497810159447512301600867288875803186601456777390619220869566705027795931891366251093259099777
9616288757104123716226146606951660943996247183692463077833323038613625335276879, 25854120161895608522885388404662
8840251731549068797771783859844770747505214179347102292827429871408072237278668867592864944255740705093500897832
48868819116666911518387280996577662620811086810546651234378090497042883, 1770330882435095879768102756729252761246
2778323135569705621019781224541648159033476743471230752556822105762903951506185947694793098695696488775525161175
25557979162776851944348144039603364092784125153169223159318146, 3014428710186953870106064578808918680643062903186
8744193668853637245492984469680712406741277354189678762703789381132779425689661514424209422905903475710662182173
514083284138755679065342736942562472400006244023145602, 184970722410486078615448332452316272752719492245481912564
1939130847971505334605677338948854891232345447959131046944140767792996237324245571959894813442260228289678563152
7402269927982134686647022871931991612736484151, 93657507251111988634259205312387209736119068364419923478828276581
4006344160716722931999938345537477429623060113079693858425048686060883127943159041465392900246142910440921213171
4140047193844755401215435131682451815, 17508084146402515547566337295069031497226250075631034428313468666540673755
7225230755464994729367881939861395954614230543352455880613490327879099460526579373118671832089165066651182833689
59810537374318161670434552114, 1206371445374823275851179608434053576190768467798891209249054070741894841414187583
6459950732680138577811351842940106649902561618353236241630928061126944638204024429235179446759466336911857207571
622747021021725744071, 819071239856256890949693520520011583051676795407727579400302888540638079014755885191447933
6460594848107557791843527683822930181641096266975204119690962541507388033367788196255327295315511221851142145423
603771588416, 799060291549941650780718826984618254437630697942042145502326846104262796258930905637715829871932717
8718879512271479645475488759685941116138755737785027450239219250757544068040735765177247478197722234987042670778
019, 193586711439269035621606597344051321605787685269958202456807683841715569198790779512813911314243348034161725
27913742743406248275267395837102903609807250739581440424012016655356361481742296525587153005884113980646786, 9399
5011132712563374690413725036671967311849094814613589997061166369045234743458136353175624248092108909544887790762
56514113611337054265631451934711497570993416389448564321095024347269447076928827056122775492537885, 7047719301319
0881571090119619443957071998057304431066920749959848798726014641781085527211442918132872490810229112206405535291
45732996653073946592681011650300703529698765329003317261627649979300325336038537223764841, 1313217809454117859922
0043623508374378293166017219494844928345596155648519015703478029167686648451725422735381869002166845710213207175
290908245363168895232777141606787995915485278514149225498543634441451970567924437, 213322586590300789514121389257
5590719608587967693362524761881406702583382620247469618594738987889290258381156303010454482433528640903667553640
0434873198516883369123579998367174988460419092030808043124848747167293321, 32613075578615383125177906417093796900
3109906625335220559055508505594535999178129846158731402829933146751776344995817856751814334197246084247172134007
68899361881897671327120818536583804992185519287510699529193528526, 8788479101255093451970038450840736454819608595

8222681109035076005446741171862828192612107628163328733972030170918747787494544658148113202108870868512905324672
99421975771432737420118004746885312219838692353610197412, 1328455012568605637892057938692521084141527687344094361
7579944969205063044500030050947770396588619427319563631577936557855698258184232000060886885679553208819722127264
547155085068937838203017220289983016473406278947, 209188401245480658966427129960715798438939271672776362878660618
4354748273211263282480538607986607673354012242365439966195763796522502842844615739356668514104563232699652245396
6326424906124666654878772779229743619951, 14480927249754932402734895471397045399161243325698535103512424279838259
4218077865005393614850555591315616395048019502603295686179797906805791244236712453540554567700748862005009813990
16893127322858575169044974318199, 1355252799519558793041648676220332544168563864805350006683276991540801165335955
7121708018603795101604826453588699101268466707552208636403709046955744107649468756849058384132042142069811899343
531345241389300829138261, 246592109738879672250667464676487296170878859260193976968273200169900158791700032156647
9894941966231585067148515200451079608758512278695556628050382136524539867818826444894650942751696000686158676962
7992649944250422, 16071792543605613856607103218718775032658413402168430358742579484052262095056030514626574056825
7344807838093167976328686429902255095118813958748202910626967673318893365942409157199103504508243410945787649962
86911304, 1257665377555480494595618243166192235707416128690277153871893157401043953128001913037906096496074717569
3192143814250903064023817674997576419853346155182797958152235767256180714159771938530562230842887209540611848842
, 244210100465766845756393302089697778280365252410932395841839044028968258343720693671058147209409185945736549389
81664551215993962658271675479173472324293326854036999128550504182097607949677366331227094096244253904168, 3959909
0423517065471714363689426870102485359786842588307659655001112602552661653660089660304003996996318026834725337677
36025319764756449579244926173821099303504957098846973342970084657754991061516990535729255753821, 2383796085366063
9818122356796338444274934399381540842790068319888411756455519704721623099729013928364063020776290255990065827011
469480186948662554074901428245785687673388637649700165977905709450885918143857854579410, 146567589838930483619372
8239987125045112297892354496846169016008096961872157765358361181860481089406806350970727763266471415101787515842
3454326933471191395916478283516599959610103645193257430568588484586204219581568, 22015140795246767624674114120952
2155698525920498952276175377699446467039938256264065465444847420311553032752333188227350037428392548759032956347
50690159308721656273966373411523675500052262760836896038757112859355729, 1896334934534446931753880110289151350712
5057391476230901317085750286623443063686628565544279595620519200606841020737016508394060312770384540288456347012
117493173401410415709072164521026520208255878803508619430245711, 122383019143314630029901267755899221016316444293
1143079562890833738173051639572755127043700947929397454756326762676487064533938562912603465942869266723639951218
3442689086667672992127081921275934392899940081357213927, 22536986979049938410959907342087128692812256739448892754
6947849743318496666086734939902331944565582618415291971388816493005422775837311756117089836672663363440241387364
37417188896335006114944305838151361031975630881, 2619396107033636372645814557595249316160746419874071084615542626
8538255981123481134440474078440296328709159706908474130195590513319345514084164100020559716409183058820290012560
66486288445447270821089052957926735716, 2837190286814415502654137238762842452188165510095245133217508030452358367
6902193702542076235028689638824585221901511275660662216530264680801182042840930874902632320962386533970630409577
860240401187412098658217204457, 110013751023200677021241185611723923067831927673912486858427221591597955409878548
1120510664980963779765557158359113241912534897842606385320873829931992581407819750364500666965941953218621681173
6251752250723392566389, 24937313108414568065177468036226659480640527939603523256887831627780404390158279980843339
4720058447483411412557650051720449526014607267672834708201328340639082485955096995397923320936101510415520286908
39893169893247, 1420008353742030436156345820279382440868028269627358905894278470760607638431039590279695028354058
0713525270268283586419277784445127922588445624344018853392610964147154766562351827628630630755937279466323257423
055656, 117315783689017381900252816130044211251686624447635513133164758930650658610648932829336219373395363538444
35620175572644350326477036279845412460676326485231149808466551325136225138841851487149058032993632374701506194, 2
4789782491136268756178316113647230578831091802770115290352366230949062450153843044054933635371261213878522104223
496078841478338831677137447821742741906238969598555691003373263581686146386721670742543356648750432802, 853652967
2905011387353949148058833239334218589564086840001873845844151291265323993426229485900929433630078407364254099143
745946852330651744073064215579965209348603895213615175370753288133627754094676128130046735844, 177869583497801351
5912875108852886520423036831809097690621760213229387349222251853949279747936303894538818264280693970300759893737
28735315319728347416378178902372761656269103378496891294577329760205336889312542365, 1582168605330437258675046193
4181562118709267170596063927412370164269428649111801430286811265853699600351638479138616780556293479339496982631
433097406929339962124869055470858870255319245479738212117896411243191657757, 100594039921115148029520941634588383
4948594096699968691777655314428563914583085291747617480569058735177469469259649298437804163552506228744761145988
9372317322994436111508103215386374341556579580051466993208569502403, 10586252822821836585950962996144158170579188
4086678834170570828817185815840890647032713231447840425896337886544243860662383743084136798715531065965461018002
14253653240902242336797007878165254953846984827986042852375, 2067452429400876319724427577736293213631006788277313
4884128354170509478198281713483925893886367976266052878159723814938571153806685148784595499326616211312079988497
450701010586622920382102721176477513904325786252365, 267658922140074957585068799124981287409230192556660509170604
5592995167835496532125155963500698550123501226446404650055635002739606044182621044490503007199148269964969543095
3105824297990282175675182721836568121671558, 18272477763459069312757332808415667414728804467606583087676583113661
2153552254076121599366915565330362312575599128938519293593606430624439678558614512025224993004192565768455369054

97487648229363557176561026080025595, 164105616917964106212559627004590730419438127874334553880346332333119112136033982585689014358751431072107465627559465430303411671302462034375658778321550016522479939240815249247501190767666117153938204211337702753460, 285965320241108572881487715373484827531377746392773638473828356725796786443738088577351730609337646093176208268338322954822970177808090203584810429943853664889575863720811439475291182979773225585772752166604757661250, 264228023087094521369529621352467204391985973009648928519313482106670849370670593745057046724231013031363220738514394748800670339618156424280308391949124903905687247815831616863794236120092067436547793684903316732420, 124650351084072446396161292357876182150105049825096280173153332490684620380113945540005918476082778762955520288156898491573251192581571908588011801453737705222736554623588872279080314335376362055740718671309519722490, 196148346403077909512960383295933743064726998391982328192339471068025140385603605323423111408929510337006371768023869591319008353843674940723460569299031653791726600735862510447501156591224084047639130958685344120442834847092234076853089275568722517400235550038070783196806732798016484658698848716352677141484382930090018023329274417154276381323874977047802805114973206091747096547330672513697872256567036503553726751366678, 140723904488903287943427090477402803494900848479755393812857024518148014755056797011951741325473709580146413107976430721515360616296051658609874690670886878792693036854738315707645429148985328051477842729373078900300, 298937347126065661878703696485644769904927677071012254374857292875045185659022802321367551691151908965639669550652926676703646477395924811898262306256413418064956616243386925634792380231615165281774366426087906111990, 297929110184957074402684820242922601321463020929444169191899383981043210880936856028557144320731844576058128319970065024533714375455893551759708036962350457787867923119165290489032722459789283537901950287943832495701, 110217952930871904188792483330129165408298699914717402372383600172936023001643606584549262162617258007312117450225334382669902271935037510428662709532284580222069717563911789600246989007048623685387709218339030801, 143369991709326221799249301045804221140880865459494497785711977036951648398264575110167060963446587061816468164186256722996025581003420495112636985917742260687476108733387697214230348321079637767487197767890773482121, 325085317975964085700795482384126003466470763407439036669956614485733441884839141600409182087082211942525337751328521311353708273806329793553606811742458527876383721650994734684029220237971400027545646170342675555941, 291312037621171140241615778288149924337160161413452601065357248802970539366255296192789326731730928643157804996715789146745353107054958065646349402033221009855158473613290382611932240135991170043118178204225294233312, 268740416052565956466130473511812256831821454132436888232244571416540414695325774477490074271075405713756514079150032304941110103749078297008169965403192983448313818343337278215680871643587179244859813714948989964622, 286649687600119203544065190124859130265078069198240031090843665666077308212513640967587995812964180312552279118313121762077448923499542669265079911967470848480523859653882506220750151948484401338187003825096265508022446413107702745621490485534587579178643958566873276011061667137368463896478249135769153718743581908207258020771868623465285632962030527466856049027712466148265455037182464859137847836647343814327615063549729923036, 563695735032999454380349019269871119053388631101639025292485365993587216695437469524669119966427005279723443994485696459766464836508086268281171230551322254029764701413937195743976500870035911925274902624517923280, 289828967967540183796631613387912292951594842678435546741725762088741616503200058364269753636052868718719731406111475718688046051346815484887250813653408843406117461878451716005092542196194441828804414170479450853113092287329765069857555877403623297309435921788149106709294294787489054560438384602432150266864088828336844402744216256043821920889575541345040130897313776247885381880335198208468239655858604537084419626042164954231, 798910334818403471281578633368410588568300358124100520149720161047731904624771675607638906777346581431859790135339355237407000664286676596969293303442151657830733604495401027518232735781886004631349975376617709826 3, 17182361290475393546913531021548812396114394540771968114461013979225575858043418041903829060980939001090026186998867481408559346071150704725677045562277000617078719836723116109012598617164193339249955166243022537561, 29666197715141120746809800047568417339298519614035454019088545071037514245304036377118656305831890599751145616228542075322042904813100962476087519320142604574135800816306476038849461438180962671985103769201883597966, 30128447784046560709873374337493670082590385674722812546801078343093226453891542926917593964720864758391235268038949812664900495189001714861154080961131367544278192271756982299547445394245084691997879026232272035214, 16563809676356034270681481602267335418474843448375176315514069449455694143381979337597172939548249392824719584779325550783740568715947688875483900569118780987714300036782522153707625338714681532628360819961911010854, 27871660167728058178056691413848877033545975505468981376520399391080127572151442882312615482849069775075729427328394085073076676368402305200141075655248875907487428001549572754090892389259629087361137700452305517 18, 21493910616749845221385268770674380147800838450063015707016357273716911116245261372408337626345595584785412584405992597456076201648656240726064237114884617675632495374568497771565908967654521049674935265602520098998, 25027116756002281477012560577633459876088855685080982684829337039125436380776200858350031557160859884673944490495767129424684434228054497689438054025868674769807319958925448716569153807237793046533521434948883772644, 17933205821044871368163281990089533978762057620367981444868474466538109989272053507886303927444134771601160669906305884007483388770917869596589594190623234523254949456853308860040504225150399219468629801391426358 8, 27481768977297711398189605897412347820331888239116339735969001314938372111800573775056751086607179524780117113935671078984715040443417403104019826809943544144670153307305192843982289663500522682115239494497522066280, 13410428768450411118687089562126682300692696091850486340546898475287137036016126015450116652958644951868240922789125557056677068563711465952011637904569166141956611695335738454882374341355402135835121405057055451122, 33828166483942148994134486436021415151686852993766524646480633364468816380404428762699978990751847878867933290637146567133172340457296315994736726765456134229586854031807140680904530097141112788685371550906632 0

6089, 5406993056580762357216597504436388960777840330732036708095982563878233281584780477815282847919972159397340374458964147950700210855470566789114667570081666473362604305766256720458540441949080973791225971891769277573, 212336610570233474510341564645085324439593737486922575372910018122431439780695683091068897272927127304529760944235119482984924508278584991326789330765355201681569757040883208344386057105992432479215213378707021057265, 143976853785875046230650957789912352870140934673068365532921950696723803123526914656704070202110234949078219936977981809812232981578435479812480675401619156023584169839049069737312513077772808245632578878670988883560, 268657572104180923441919375259452301897993719615492502870749888891062984798749488463128602297694163686543157301485170704763677930506489282906835161034381542772788232365220392111999656163739908321549919584120802018020, 263034789849153667420867116410977145911829108302735751117743317084219802076534244431136119116772754949591716805001386241708816011823138620754743771740639730651245820761366389475593400541004722400673256717465824656200, 13856193112001898317704709144728127618299329916747060470435801824679913883890418656325826190815922010339267451603453448661138664849823180926669277503231329114216916643952490689615108526940574456016006512662310977563, 230783798495198113397228287937111510311740964877607185788738855495198389435282168426170815390070262704327374974937577297159299040132057950036420285598817843767516263388239749607283957246245692663206778976212903416620, 10241837331532491076944511490337055500300179384514563823768902251546880925000870414919268390074562830934140114634739131484604089343644798541562549142918509714166147696423871031805459630149322856596306289230096390986, 233504705655653819081799358764636243177549208106341440460072837752076374580282384511640586233200174899008504700740345060020423257126318909181371848748351485426923912628922343003419659598921506279654032553088696874784, 29754831400694183747354793141459076720864477690068425401002140730777995812809821435489852180197928101463999114900035450001770541729111644141489248195912892735334033338711573559916169900467940452301480542588993740514, 89131617850504164505213030409727509675740577160834983672190081679412550419040250746493027162865977826970831315847804375682772170340969743651698819086485065993983755514727427782795354161475954180272589989367819671 8, 11565227995211778061360803557056548564607068988900302538439896698074813760437713533437168580979315644519042477774925016750423116683651324506957514973212782388884991033707639483641560011894204073561809856317851187583, 14949458306165636974156946454411685177630548897973098556930888693560097034546938992583124935606351738614845265023297291043344730766643320781799901342631083150776685749181573286792265476725364082328665996588688292264, 848426005084339196818371122213945642819393153145709894815926591446002243358572955490154388416878716819701056718419284166028400276918488998488499931928325877678420626032275308550596036296785942313418442298901915363 3, 145464498236178025130717341254035439282052352833593557320512737359001665781645093985516974885265906146899953382468848959187973920758004535449664880007622993120458721408440918283227498302819131469030687116994063084272, 251227621466293874804167355403835507334979597082619657279407385263881076813290321110925195204870656022135573315514972916620741883001842537271062666544094432618288412949063129983431559173754666749294932295652256656 20, 171553580548204410282538172648424897008074576631826698987005332339225445162440292680173325637257679044638691170836328128188497114698827442869373858884614594282790618985380784914688888578695465860579749327344954788 25, 240655614397821174215151745524034421776163140170880493398582367534867812076528106689161123162524621073677335764656558611987197380541559598663222323034847486819220278722213994542044417983302308748933163513643311910 9, 213266386432821909358340717344625105401938436280968954468763959727115786821704154045117008473985379441929147142796614126937767795683917528333067463691726759910392434807104055003835943325670223115379492880839127287 91, 115334367375137268533426663196574273691829383767711606190405242081871710795306996022139719539284164017347544912087206004081964258388034756757717304588648036082152534873737713229391061417701271966961865213659930716341, 17413578205109047658771068072839740992406940681063893781583805499641454557243011256200324434130248631102059039422588994492717289498385207434846910479788035096366240558507577967719276745076314570329313325875973040412, 82344065782946275654338318349277074543726283884525113034816699833571866715474442016362524818594290818037274562466408796218290765123017160383429405352193397785134055993963118238901048843122678965405153976916871201536, 13459949999212470824214369634465815383981400799953114858877412049058917841564198625308323023359023043642281125191158381452405954408015851346675693315716299524318273130292670120927872318597664828264194523092204882495, 61414542933022691309419025532289260105016007512020199701283902363087314379949270363084555780344225617741712391823925792876311462254776370943651656979542618969707933320841324548442707550181492053695764088303020521 66, 23636067008429813254108112915881876688518793539128087922362577771246065511694094670428786068798740254162912853481657859420315325967804784438688960459593709033504544816117889783286983065113715253670046945322158942127, 23524864509988180632873990491229945730386323961764029527895002836823913633509065940631515621529321538014384315694576133326275986741377790785857862214510281677159653108851815774076719939787198476039077592481690948959, 19521520440073584337536440663830210329435017295149118444136203950967934826303762930268598795041630609271764989278372336374885203235022737358063297207167509168963818977306694298399130043515332073153193922213856850464, 24150101566625821704926138574476504927247732596963151983306425388175172049033218683141428257313609561097048786087087338638916887326534795707499553270876240959014327782246233109560159695519787395301103733536555815 1, 18729543866770046661952085256648452732739796715028411713680658699288715708251839140277014641582821290765422002087502899342213213544083361024785181043097593712014355963085709339731537193440836006628720252455552953 62, 702736712699134888963826738763109261166485688561673736739639290362204254539820264150475559773993156250783154405238992337254428557499628064385259498058322473807259225735572556608871102134991319333264637060185365887, 16650119322721685660080639811294132937645686368543549809557249786459137768793496810026360416045895027818782128552114155925583203227255

```
106164341033273856318935168044085375032440584373966248976820634104659827857298878, 152522807624801466530793565937021285639583680396145179994338183520095346823832975956713209384134529885423860512769389260108124593843773695313804461614862746909626651863275053771807656161865169753171251093142242123 00]
for i in range(len(result)):
    result[i]=gmpy2.powmod(result[i],d,n)
C=vector(ZZ,result)
A=A.transpose()
A=list(A)
temp_p=[[0]*127 for i in range(127)]
for i in range(127):
    #print(i)
    temp_p[i][i]=upper
#print(temp_p[1][1])
lattice=[]
for v in temp_p:
    lattice.append(v)
for v in A:
    lattice.append(v)
lattice=matrix(lattice)
lattice=IntegerLattice(lattice,lll_reduce=True)

ans=CVP(lattice.reduced_basis,C)
print(ans)
upper=IntegerModRing(upper)
ans=[31087157982797, 104407786039344, 137686226773297, 122706247879898, 3655653435805, 75939712496394, 23231038469245, 62275128959587, 106568566534989, 139979210268501, 79578952325015, 39814231664618, 136423111991450, 127591081894620, 137994322544573, 78604075943622, 114622235852551, 88755932103963, 106116650561108, 110708979497403, 13385264758440, 74235730861253, 100669691706952, 14891138382800, 125542116499610, 133221001164711, 128410414732011, 8591859221697, 100429843011847, 149288233436677, 118497336519202, 151300808743994, 94906614092869, 39866689255817, 102387722052464, 39836963925492, 87282800140967, 7022222126766, 129977203277254, 48759983962723, 63128134859626, 88570138802849, 6826269841999, 151504656089252, 93761934099357, 90593498845283, 73033798174727, 43387506205960, 47906851298708, 98248454178910, 60699627108226, 102052261408519, 26283939450845, 108411937946188, 137962137325525, 48964082685247, 109663630507518, 150859035456151, 114574205419288, 58781294385634, 116079144233649, 41851533914512, 115615624663629, 117345086133188, 13035149717493, 152219947031771, 54143063217021, 28063583119478, 12418419242524, 84997801980242, 76140535711341, 22782669917859, 994406120 67143, 107228647755933, 144139270604673, 85556086412900, 128905302611902, 92851087699852, 142117521891608, 119557654940775, 31943733104263, 78303883202308, 64649956954318, 3549522683129, 40014171078833, 13252757299284, 116045625664257, 14664948290035, 65694839686742, 29518525156129, 150705658696748, 143791484820110, 131475164047563, 62428301185416, 4829603681055, 110933884725039, 2018130983233, 7272655468956, 124815479662231, 56240879680809, 95377339254408, 122049458606077, 147635008188344, 31827700267547, 39321382259771, 20624189318562, 12666661347662, 39748156613371, 73341116342109, 120046631622871, 79299889815491, 55335907796247, 104004761239418, 22242893504659, 35814193716089, 69815844744348, 98813297486221, 52344903586945, 78832812920353, 2440395446187, 151978021667337, 16994146588665, 61036562530961, 75402800673509, 32270398644209, 69141116344105, 58412825281162]
ans=matrix(upper,ans)
A=matrix(upper,A)
flag_encode=A.solve_left(ans)
flag=""
for i in list(flag):
    flag+=chr(i)
print(flag)

#N1CTF{f55bfc7e-7955-412a-81a9-ed2650b50564}
```

有错误的地方还请批评指正