

HGAME 2021 Week2 WriteUp

HGAME 2021 Week2 WriteUp

Crypto

LikiPrime

HappyNewYear!!

附件

代码1

代码2

Crypto

LikiPrime

题目显然为 RSA 解密题。

观察题目，给出了 n, e, c 。发现 n 较大，尝试上周的解密方法，

在 <http://factordb.com/> 分解出 n 为

$$(2^{4253} - 1) * (2^{2203} - 1)$$

分别填入 p, q 。

运行脚本（代码1）后得到flag。

HappyNewYear!!

打开题给的“output”文件，发现有7组 n, e, c 数值，其中 n 均为3。

结合题目描述群发了多个相同信息，猜测应采用“低加密指数广播攻击”

3个一组进行遍历（脚本见代码2），检查输出，

发现flag分散在两个信息中，拼合即可。

资料网站：<https://err0rzz.github.io/2017/11/14/CTF%E4%B8%ADRSA%E5%A5%97%E8%B7%AF/#%E4%BD%8E%E5%8A%A0%E5%AF%86%E6%8C%87%E6%95%B0%E5%B9%BF%E6%92%AD%E6%94%BB%E5%87%BB>

脚本来自：<https://github.com/Zui-Qing-Feng/RSA>

附件

代码1

```
# python3
import libnum
from Crypto.Util.number import long_to_bytes

c =
12231968712157544957565674332358785900531694075992478687431091563154403661555167
74000965786544846680686873170919356773757699779814109222718660445478204668252050
43077280358128463715123321231323317755611765664370114207654676588367848076158525
27516855241397388900702687598543471369387267121827006630935505632008749310127713
70507277336743387324515587398699577397963429903965008464793320227955146777474716
25632382380000705977268785288223182374483479237381406664972669036492230350639806
40918231139026750428239519314497225563165288724113423577821441493985108733490979
63365660273483833177075792617323313108963771166478400130642269793752600798491488
20466574558943617007574932595548101935532184148804601708855923976851909716737684
60616632551881280403915254448436478606860705202982263789153183370505651984575985
6907439649236503599976452250598977118499482643321752349471170684109416185164942
47462405521890357265097213752876090784263584819935239855346021255332750375195112
25846637108433897112086989162322440287459483742713277996080634525761443536160332
52705422484283868276079374157481310735656358762200165166744301102251267195294109
74410012225308332555627739100901283086493666541113323835087112629668896341123755
64460598151035552459061360133987186153044013473848226195822479897759433377262863
90250520524210126723919378003114269879148821233587199759502636217155157153568358
66634761030214285603880113785205685967627669219210746933251583811742396260041947
68303533010586976662957963832959354815373169981257991639940739472677138957961831
55488137067691105907424478335950928110830706569557563067742860002913840722745498
90311822751480589458577098016037412311099612382925289369108798377455033183731325
6537771349484796474749416675509782729

n =
29719074182040300936670415295070601820058002191399366592777898061956875000411772
65495588264559348082637142765979243258127249946113947282297554010288792666357058
51027038183208721131970311897953845143262009291905402470958948625319075400252165
01472741890726831429077005774250599685354264780182210904292527042769986171940585
98351993469264041797024489887680774535153209471977482371196471365944484597982222
60588870499920933264454029437951956564858308075751593204424432247909435046490780
58098593868983635071615324139697393893870001424342981801370268016901546680696032
61724749611911540527227679245909339244048360898718905735863014712647061757253305
25590503479666489869468842112891150185688367433120719570222809318581761803074896
15167784667106895358258688296088269485128231034055611113315290724500466968103870
84587155305819783219851468961590607274547352011059265051423195951523748310703876
40595229878751974872470024331948516224751835003579718133508606655038566841790401
66019438906670753994371111138429929890833094866981245100824542407978293187750656
61671938965826403172848771934804708246757785208756452136134839999409615409436425
20801301748917564618106054055642282784411426960273387021894339244586353444369269
63846429122153282427873946233558610559122443510382546164806181182489609087751257
1728145894861163732801883809465918726156374666882030554880834498124445727589730
36227098520184255711084263671420773720930560938333438298574609811258289099226150
51166828500771492598482216552790667232057263654054719918495240319122625666597102
4342219463601081585085423674412283556140519562502143962754863260888871227867615
95205416653064077088787655442716512915331926868877768175122583721210873527989527
8509433459029960725990332445185015809

#n = int("",16)
e = 65537
#e = int("",16)
```

```

q = pow(2,1279)-1
# print(q)
p = pow(2,4423)-1
# print(p)

d = libnum.invmmod(e, (p - 1) * (q - 1))
m = pow(c, d, n)
print(m)
string = long_to_bytes(m)
print(string)

```

代码2

```

#!/usr/bin/python
#coding:utf-8

import gmpy2
import time
from Crypto.Util.number import long_to_bytes
def CRT(items): #中国剩余定理
    N = reduce(lambda x, y: x * y, (i[1] for i in items))
    result = 0
    for a, n in items:
        m = N / n
        d, r, s = gmpy2.gcdext(n, m)
        if d != 1: raise Exception("Input not pairwise co-prime")
        result += a * s * m
    return result % N, N
# 读入 e, n, c
e = 3
a = [
76873128450632794411340623602726745315317850448196047416384941357295990190078194
14710601206646150366677215682364861042125439416260936836118200519568889999904095
35944068510533828285247642295156383062225121123397420863524500301605790432399020
45390530506713150949793191421443103315749838684001023448248417789819160867344569
05420419590914454188783758774351646742037769317387086248043016461796530198175966
12876848617302959482364008286148292002918372774353441375602500755004724814787928
35659407934436159683648252502143461627198292066231325653000788301872058504723212
12897216569631326836820236256832299405879593155835397208575574516814022281680965
59968476948263356605729649774017109848808425693506724312264272613164411551780892
43425574921312869212245436455998601825137916733142532180376045402694503985686049
10386699743956838098547903654638406363439809623762055400130156293073899344887255
37142983815565534720739509012176887290320329127809218230756596181528831774086891
63329034139915363117802217165515357679332404630234926742155622006326426173996810
39534604440180663814879413051907307216085130481814501276285627707021726580888365
81698332318905758721984778545449145728049393279394785952324627362503706190204128
637631213405674863660425389313259L,

```

52495554982270110882024944834154947178954297037429722071964414446704612099970843
50272698097174917083845915027478438118585992565780061524098615216248004142210494
34790169883523654257416906811451131195855586244598374880878692418389200238536952
25867743865481809623600166554087873399391607096943930960066905821653238128513122
00908543846964797023331905476908129907148845261227240652112947332528633530536126
62498096532976972273019631446622835704720241172866721075241553118399444619649756
06754648294891444603452719702904329686722646739014026236117546593267312968549766
66621670821142593685917136700444697809558104200607143890435075707070611291500718
85165680539302629323340904857078380746639406842784054066196290404127562974351550
47073295688905770106824153346966526970804033779297479283967160906462427373448826
44099080373279635827499391311192852996185659550384490800471851429080910992862220
71106259434530841587125509988124634728986309920606439740930811537598857558982632
23786873485766385364541112262111717598341716281879186918035073770903424360239968
60048081331160462608475138631005602859620531102785795748957549289609435065843724
24062481234806423574610837438057911596190771344568064718882123247708570545980147
637910744997312960997877114875563L,
53181671505106791162920056725464060840789515112032191593422355041608405594181005
72756471243653721646917998156543248431528356216572191439715107945652824387191321
89708357084269561390602533348667210778967547331570345307713271797500472800693615
89773838635732276021378260728867263915877164348051945569914453588575457063197281
47516492110265841469635697486600715193994590766948057872165331501495799055531015
55997182221446716574345192297201707280470099673168021522276021573255431147391095
90744465430396636836261830727789045043164668041708286690654355965583599208183516
83190975764187994424726340414397811109158145278606268400358845889538379437233024
97813966476632638781785524454419556109443369209786353302330932241171298568309190
08120663634772021426868810066167085694513717907623275381425967491310280638933695
03630473389444204682922487198565876410145691947522778296846198039187222457246771
29232358305719548783148527753735258295780607510739074337299037254055287750082818
92196408813191030718076093978452002157939946565766563496036568071173631123221922
17047525023610477806448388289475789628333677517739435132949607230818456747007141
14613905708967183234219078662548527491691822238226973730089750314606177285702898
595711912716069746542235493085749L,
49377225352002870122839407379111879689886064254629351716597634088018867150117075
79921579378358098643759576613803761491833622379607146245943013015788857241834906
78033704978135608268473206365825232902155458695063561942608980565675676060170247
58720383330020578148221030697861565621767525849323950453976221391998414647714635
29953494449042826480013385410918944231678049842563567836230929538921480620970761
94840351505254447228339051915162949343535017563167413299991340194548813782360554
77950772251059268381139850960747346860140458761756933715082477860088388461620474
62345753495499062877414631026750961183860622314921634586680215117510224391910805
07345540921839703382290445797046739813648289321292589201149955672085687445193343
36410549234361129334854059858728690949900023441695520161229945828268851565859660
06564175541618958120469943164232412452897353274507046420003409294598135009712664
36908790234452643087694195334024560701562917342963860276789458845939794177422833
05905167348322733237290596986874055641278284312876106067033418829394442101913151
41196960080658506318805881239295810978442556255935309352293417741893419097829796
67383762706038731196861300615117475933625813147094849135055190312732335084507955
724604696171453417718094964090327L,

40081471399915005333720299817724579718515331810858266128757989859631074650129197
46663477855766730460018635008789592078309177445562745461589198156009361149533146
00540036576429657582500764669413652252770861966417840099061248948771555745832102
92403885517261167504829026420287279133771086521307794559213079585179571860806581
27579687805786747010634113775385974241777225588675877811418976763001535232096759
96201871155481412772845570976807158049274849081684209479884845355028703657648486
31847597771607567024376621291003994255095728918994662826136003756535442309497291
73715720962035371861085969797227128192135545506450587172865501104653431004998457
61528635976859006285823914211739843983972560292482778326983903018873698437828016
66882151658122058883678209426158289939370402981985148433159226966447985521505676
48397795824174863661825244839863730984896363344126713581303895799728380292026099
36524996601129648191606117951616875200119129837212604760319073283133589692257497
99485588281965501872736844136131778827885772117908584735285303855320863983643305
90977751354526111143517662298002683212818561402466104382467833643207863906572424
14430601000831387967976691362673290089725234013924339500819390840062916754623424
132621350706544122257464089409619L,
44121983210232911394186283866094323357921544109134633693452802347530410996559667
61634403948132725583209184204803867490919478024554234028571252339082068671325990
69595323243154174569298961794344623241293553421864069389535348543832297805982907
65036714272156680331510773385245360811124605798106416424718764048071231206023416
92925990960874229403808744358517958476738839461343989432822976739227857861346689
39454715179979246505182510338437251221569074780060511794395438999419581907256239
69423923667460472740468876444735299402206799084317413024066928988828986226858830
77780292834932653486674159105530644575139261343775220996412091084485593734223059
01757344324758407462166774699512993336120173336911210734744313930970281023299709
77800608393317411345643696515043238777860763921789452277075620915773520309179054
52898138738862443350319127347052304341795830232351991533002633997674685866799720
93973609985111254951924071949408463935260725701129931726900345186925871556853670
57076282612238376200686910998100318080585151971618650637124290118723043309649481
20635689362790125573222197822844611403612256503408070953286220165654432742563101
94921729305097890315074292153303546235677671541793456589738387043928232044507842
169173330728718482770626654501523L,
32086995756378842703527799852361826570562597341703690120356947234203023744762501
18709791415781281369601294675469145233292600710504710088963986069881711896420599
0851795602091545146531398568928777861360309556861849062064900403692083060786557
29059123196294194210077171370313601888984826174914084034754697782359555680243025
48038370303445916460128571222132271152156744703885486521403812967057725004455722
24924018905225174265663584819356114341255408979866800339484643585303306817447453
00068477051809357766110254421210937882871178507351486340244287026435530037151668
39126710075733200592612578976518996975668045133197749542947083031687882920378571
34628186553450976637858562675039807897112079750384830264618639239956765667388939
33130331419181312625425491492638427949411557699777308025660090003456343495959367
71485314011602819605260617234791617545551939797266569615153740192121537265948071
42456303698775715290518062768887156433902187122160641097916121097179118289646514
21769631495647447262642086848615242101328478486365329993087525337198232736799113
91268282867295390333826506878594128681375793097754406985028482411223944231297714
42338402870863767769545005951064956498742874485207824630520777152431261010818838
138655082911865834699807375008861L

]

b = [

72272526757187780740231908182662830525254488388433524125870368892092975798481847
00730414798409214800771131838695607580291215655248194667787124811834882779054493
28223533043391590093655773827799575075615676500130199172201779452716348108026696
82832302299397517461020756757165155033388173114735681301925888955155818128352422
66405332482788540114925611349437981496618737067694827760611462986937139153931759
45083367889987571681776927122583376239974702806044792299381370488664195802017823
24081139418050944060996734514114165338974643128489397253073543895546434828096082
53257764835540085375275381063982073356882613442540171518899312141515089154809615
09920681364352778795068266724879364096996252272841617341643666522563974346452491
30296982248390147273690800217699524480828520264454294915192031093888243256510119
71747874224791974055995039439283757815805383748534713950030884675451280600291877
94431891563377967647568991772201040537299188867383732391802781253804314567562657
95150168471026227659709127971986182900662837757507387578108893994665112818309072
42906074385975601933211304962404822605735686469716581306953085852404049568020179
29673317521572608385674052894773447205932790060730005333539795323555614705817665
786476411351969424168366962370578L,
34110663690236462453762180393705968382950084773173721702447794722910211786884127
08163914625804241614214813232872795603447718377116801492514076215447327378921604
96443939357041950388493554496406007658435517211507967374859158779641371713073809
45935695766487038502250628399463988501260875434349774096358287747534652886575123
87858986416415626444196399948890399216624995127923979943266792970722883449883298
63729467521185656908541750681614296631331948235836697947639517519093825102735706
41836816208169331158072857926444044995188836106534712444787681467005167965228028
19654911502661159641286358488482656797434992569710165351954774168891441316001751
59747033626985115139696085153828051183257884668367446309997650590293659781294222
77778443598733438419442999319987306120656390315922736193690101399470204657567708
92632881159055407611472932227216963408195053054976910527669997982979053685766843
59681315851605714974267829409740228043899512270242579080482164570677517245195783
18850933896278549187137041441448756539265679481725774889901463268936692870601342
67319208658027141471141186730533538723564445668403364317847936866077630997639159
43769968162453433779091468653936247489610842351714130350853888962620401435016019
892000066519489369586647822582532L,
96655501480984228476843527875038148766862682735216531181731365068856421448884071
63442205054325701520183640900609856451294867136980499515910482733185370016755449
45480646553959477906190300276665535467079212755110500675525200159151897119198162
40838635843727117678456359153157042256845391879627204005136329626204082446757707
27502401893262091997957372146232949096299279631705729397535013869030100609390654
38259954420418819126684676390588157524499944596717123709055769367662847035937913
36731603543492278087975208438906947966054673189424532474872122585340933934837935
65039364621623931813126810934491865125092542801827866556958064511743945958743772
97350096695928160572010530749782833191498947963973339026728584751616132558145968
17201545193202169499144055305358584644635503323032680354835638327999633796089419
07374189783501030091760332512256373414190776581518890690901724523624285326997681
66967954398269258762396004490146627369192058406997871884664364975307598892718782
72675511804209502453822900397006767975864334707665149166220819464748535531766670
26305022300940208219446721943861227993571631930049886115349603033320280892800670
10194083544710557740905323307047437531909208156552326189818775290574464308259642
56948001465214314349394508264556L,

35710358667713319040027553560829830709675551791774399177992816594480815655514336
45626526583182574411617809667540824313467034202130474649058013479874295878665077
84835294289240703319363713980965945263022810877492245609589053923882000898807593
18084130898757326220912295393071180108826503162756010457158526090020687859336552
10480310568182417915134492704370555030028335942992870489955607424358862155477666
57105383700364572345248814440024509278757886084274494794572349604428103225636768
27863377347170047059272943859882171294480597563963742749495182299499113152106714
16115639259560376721802616400357165174216817415275074319811637049299520377471701
61617798150545493396732644456871805542270699764392127056902381387198947947443962
66759507277710456542949404282850958840605749845289660667207960031807662929183296
46114850777783349848175957477265268040763067038171600535165303706961722187437466
76413884784385108888108803420106818173901070897426014100110652172248635456173774
00949711156778284607933523333361727883752746718644491958416147404452978404391289
34065552090160566892272496149062211385359894466859261856436046988069094511199089
25728900998397084501277736148437741526619184826982588354997162924650747731826227
150677994598866694976617038952960L,
19637338310590229002094481524811517856509678988458529293062371694703520807102459
79490930152914604596880390449971413260971300718262938446146034643067425977644228
62382005497313400758917851620553757103374309501021075747571843057781165101330819
14244608811627909863311372157745138906220771333018417391381467908734945007830852
07037437126175607644195184211189243198937007954376442047333016271938731156333097
60620284510790535125035058821049861371456491148507101291075161477427293354824377
76512925677503989459194555951112016757565252244131575782406066073014497084297169
85027225884210315754956029891327635606318310546503128595758836077998794347348270
00150732042760623153837096529339041007718789464168455505957010471222861988485628
01299906807596464526282733244686507228466021354445308152903057236438918650610811
04843118644859004328857529337205054182336262864341775870413762628059204927408654
02092716512672643242061407641167432424410178764502786772854859640601859309316626
05063427975862322595575784281008654430549382655544512022389604774744575411053727
72362543077664474375869751570896853978275406718906076992894505881560138110911938
50313213188596446595791898264003078214830341703064110270245588623025485564465677
065014954050674151068209958156338L,
34355857702058871442931302004109329755060051100184015413755221657574894615796159
10995973097308758472496090670888955673570407525836787662296617610730291786679417
59812656095394713728367061506713413650132129245164858512061430944849306322427733
29703365415216151293113989552389144705578467477635633672119560289808226470341105
23962237064918356152398989639650393498675766281819469545850027052527962310164451
66027513456849060948360498081892030697906086173612576083651879166491789946438067
17966221965106227931700205078987112033385027275122487212953574268520183709857512
53613126113920503000734628840468225716428839496733217368378383795145408278602193
07938135197101094531402063240331559853201121385391076154875363696159228373299490
03540129776992862737272188548809111000039574296453644585536774622739578371658195
58846415311328390808477700521530209147405619156121094494172038524520845516798171
29684835596664222472806271699238429017096741164052056835664191547244480985004136
16258587472701524803870337627904287025336541096323093730999570279202034208011566
11501634349499422902757892276745595179572430600777418167369501248944661973732093
08598030218454826136754312091821659566499445097655483610010997986426784494466843
809743836689209926943448276851733L,


```
78140898568960172537532399957542065079754785608196175653725188831315142763849427
14447743310988119656018362202722708795467419918899185592914633678497976472049754
76858247357519486760731968690271994116689515784905995073318003280726991930163485
70092942269398714025948091737017548105562834031699831877517521836116912407428829
03772999434860357869418724119458765005396668261644375743036669381643882254157232
04268199626967900473447056172419894034829626425613403635531008612320839028288304
16053526478120239416765009622649261419311221132287115995483736302156498238644085
18280710315730775510877407983947437317167847987927077237691845975233141657205737
31040683155168262708200792076877781794431709791192725469749483988360209662959767
32842161084596604333609962435508857188202619164351406760248161996398928399808794
16575068825155033336052154527142487649693986580388062533434113744322188390630196
80506702193844642514704165818992467080553637621344595668598997152064351401889973
49196902765578570516978378759650864568014586614460583304460504318729333658817066
27212098487574281521872220059343264824204337543967092395049347782136392379622916
52317008526530026480506455615216407413567880878703059582152229798816620073095833
80284362915245390595921375463156L
]
```

简单粗暴的3层嵌套

```
for i1 in range(0,7):
    for i2 in range(i1+1,6):
        for i3 in range(i2+1,7):
            n = [a[i1],a[i2],a[i3]]
            c = [b[i1],b[i2],b[i3]]
            data = zip(c, n)
            x, n = CRT(data)
            m = gmpy2.iroot(gmpy2.mpz(x), e)[0].digits()
            print m
            string = long_to_bytes(m)
            print string
            print i1,i2,i3 # 标记, 方便寻找有效数据的位置
```