20210814-InCTF&&RACTF&&SSTF-Crypto&&OSINT方向部分WP

原创

4XWi11 于 2021-08-21 16:29:24 发布 125 收藏

分类专栏： 树哥让我天天写之Crypto 文章标签： 算法

本文链接：https://blog.csdn.net/m0_49109277/article/details/119841199

InCTF

Crypto-Gold_digger

```
import random
from Crypto.Util.number import *

flag=open("flag","rb").read()

def encrypt(msg, N,x):
    msg, ciphertexts = bin(bytes_to_long(msg))[2:], []
    for i in msg:
        while True:
            r = random.randint(1, N)
            if gcd(r, N) == 1:
                bin_r = bin(r)[2:]
                c = (pow(x, int(bin_r + i, 2), N) * r ** 2) % N
                ciphertexts.append(c)
                break
    return ciphertexts

N = 764125918785890622182682952145881551138482145911596517066068990981488269917652449188458526546925212277962628053839546258267862697145372148511519661130 19

x = 727340352566582836503281881085588816277339003139455525720628453976822359966086864821923222846617340653985403198821826712870660894076815578872379044962 83

flag = (encrypt(flag,N,x))

open("handout.txt","w").write("ct:"+str(flag)+"\n\nN:"+str(N)+"\n\nx:"+str(x))
```

```
ct = [3266754124418328672247866726679755848701520371443746634280907120024788951726790644565764235065010905480462
052367779604906344974859812257431783971523801, 3910983850369346009480778834354740700744997092428714236904249742 2
306200337366274291411280952313828999136395230581507054250216188918084446025451499398 81, 2731781092076584134208 69
291110421935794973536216100314847800352990011319828784670156659829095485530247874887151332207299734095482845206 3
9203793990800234, 1904925382693528240392820554945438799336181158945590017639824263453364372865677438612148173559
940312961019478684249090129969383176734881188829557294476 7, 4680827155297659793071068280863950172508774598647851
243911022909410605426070060961165159213610810566809580379313538418738679814142445662724693405421220 4, 6466355666
388787644852182538917168197022617180333504711699460263106018477120891683890706132515722706571783620767768218179 1
737509930934478006410977305334, 7137098987890247372953807599261179383538109791619969185539284001313647125831466 6
533631139620910819776545627240136734304044689167904095661008959427867080, 5120760109829368119622569216249179916 6
622864938673303923018361607194831652967406571956932708259055309010010148314023788289892665531292769107992480111 0
7, 2524676220015576472567491511742826694635125222392035329284653714204312300410872684656054042741369434866217206
383753257380576855992359675791454257849170 2, 4984042003553856225981807727001423313543746758606320568394376962743
429301654701839348206039848243111828037038064140512892743084019853698563064985929880 9, 8423235641602881983156667
977959118729978704663699554344931491207684061426586672141058634694887718610174835334427733310708786293690307992 8
428665929615, 5625598934074718847299400172856582390514544908808060831201247395120943557252637264554599869163558 1
191431650844541918635345655144222239028951168850704422, 4578566274032845385989027850244545060689044532872045406 0
032120470673511251330845850132591950890320517787732079986810994883608872640852386167756195212718, 54029870403864
304285925769805259101311108719589466350768320792251083544066361265116520351278475192456130712826836166473186592 5
320027949919235085240646 20, 4662426837579393641741594072617249590286848829608553355947407871071589935042125618 09
297033755161330014597402556621214339005629069143694208767219690396 30, 1592121947996584880275001308592852247079 00
346799693247525035813853162757998365219011555623588523856027635997604096518289237291076362483593115325354123 86,
201905624754282507177927676080719657924280194056864143945157316000726350562175373041040198074744401305490500890 2
949995655414265219350291141178276090107 8, 4198305954803366327036794617423410335708321131913543472100324822079255
044958824878387766092918905322815714298862273613644129198924908044668951606539343 5, 7160953941141324019455621504
270915721226012858814908714149376011596239207526893595530931424073379974121380555492484068748612893928488639194 7
755983910372, 4838228472086585164843101694579718366026615549834362637203825647628729352876433028551466143535005 8
162782747986164808116116765643203666318480114386099343, 4673032063865661211088982191811422656480993466117959484 4
549753878327086621670111917286750423548271235812428733761683357631975738361840732519608444014971, 55158112951581
407023186496177304925445962183673199215662079568367093310059249411803313113095482726739394326470492736668839734 2
863126503437157679836103 63, 3711298020369887419649776322541441737452638013393796721384183126952037485661911046 06
065429114402281725339683627869317462914148345149977772852674031405 59, 6332208301773286960048425666410795256542 44
421642189428935028090969458273127459186162464997349907877423585519468310088091856246577873758198070195667561 70,
713149941955910488637698279057810246313923626423796449068390183739793222052537021809018603956141249753716206346 0
706345433646970829567561962759102801409, 5898794229544129500702766241341931624322062319707184621055033862249540 7
069803847200822547917184493216087823262589570286179930999452321610193662415873715, 4046306801781988229639797525 7
296430843199918804116579332129293544451758450871632123477648266871632208235745045407313414566869271527363707673 2
69415792748, 6303925560586059470623570180218246972257591834743721639178514181184494019019604700514399618036767 91
191012774083756351485366881804279460194024849872725 10, 7184751879548138140587031878670693091468359835075087640 02
192103327242192780965766865835233690960727414623596860183346076654157156218920124990466878263 81, 263372841237538
748283191863047912116209305665661201954956651558628538548595434756305451757743342879404188922886973242549945336 7
809809574437374941704 5163, 2176401417591252124482406117684302715994104392431515917582640272144592461012791617102
948322678257978289579667288852386178193836636397283025784540691097 5, 3435623095726196844062581172306260159832381
716480005885061523285318057788012070798019652466654719345533109449262217283547667486720590207050726788521007, 45
919770921828919777762020824998206274312663582623531457423945627938988437572523960733207639926323480092557203738 0
584491233375608109387101609063644476 20, 1031617653306075953351395033109326574862179796163402046459993547036342 97
990399094754633192530367879103006182318609697861555107378312066320503942100704 51, 5991732603411936933137180888 45
747918936637835516107208866055829406130805991422244667067275326905076064526964596270554922212621185967276751465 4
0248450673, 1084241916928330607503851935280601931883156894659281718284119755362834189402332519862537770196093268
367288692464159181448022496032311416285014983849900 7, 6674206403419281523569023800745131017722988261980241723005
741818259105385486399072943426923020354227606343548948723022861731329968644507211486193749552 0, 1733779950648909
881031164053679273315071861388089395063452876203189493125440583098633760967599976357715275089079851849443670113 3
617817677416137197595268, 1180535503977497341396027998135308948702654552478864197878296029731735002497091359297 0
423213016483957303390870999692309756230863161264738948268751555880, 5948988363473973597496887004585521781238122 9
180244297407474712914329781106395937678986012546789197922278383445284656100208400201934959073937202913889830, 11
401451000912707217036107785027425488005850574045702577420854119932133317734234141433888477046072783546143158822 1
153619065934238019474248557351381 80 6051, 1817996383026975232834701289218951810576052627298609687316687056936806 59
121596901711681533347623637868604817161956662697390569606191872851102362252258 86, 6250964070082659419799351297 89
708509742976189605977090716873705542587397379858412206152476658774151578056254805665855842122545222160958182262 9
```

9866438643, 5990222180228599266357925284831684381480268959200508366159555502046629155561009569578204543747284027
60512196275216756000155742274194300141550867736323 1, 33433077637882273687249451259081443266379398604904264246156
11848606007593545570187388465414079057820373250217084991244346994213996778920014442841724186 9, 67390195969105286
28459747325927332256834828128806880638199183217891741455875150841740453391851528263211391663399525124683497016263
39704436292989924347318, 51701910800009973400544456943096381774979876707129028438769990843089912852448841473885 5
56005345531439548870638966325407697691571465101340746897457585835, 64048417355580136172437626164825086735195128 2
81991270452716237192859126404734412422587916788587067007095933362505117338589065656344579539799999449469574, 110
24312233820256409788185405651410973909901139662527410532287633062222198961951836395718214894529860296406012036 22
16099524058282433294904395648559350 53, 45329081591634176909575079913822799290480598748734762443445536547105615 37
19375237890027287900515436350476275960201139655008499344603270431331588999375170, 50858826475819728877134521770 11
99971926682351116318422993518678158780829461608080437228699550559655549142460257502006194541153981121014516725 1
037970092, 35605374328853657972896594891951135620842006755668179374120075488686032129628717565054614577034983995
01362132699221485469465415446251274084348821046939 6, 31170348521031754418118681749590239915934031936796619456246
63405217895950940233172036068187754739535088532582485145635984657142355304099240591206545 7755, 59235278298913032
81591920384041520984294851811891568014728727561602883101131487865385779152257449191703306561388806457458621975 94
20566309846454002915944, 55319991676617828235828390538945693681702722602937980374183338775928431972606168528372 5
04847459436496193456215997930129475890947660295696626996070685399, 79468704574590599701095856291869284762419351 2
86370941433001107112349660484318958148535882519340036267944369382787212810175424680159076706591741260945 88, 6011
08915032724036640653941700038160118671165998931341077953603725651787768513741284294050065077187856846974721007 52
69973248848394680481880018778657864 9, 28279251639525643355877411167790163315397766491944901475131371705035937611
14791382368026334030488849278806687786569718278373060752050034217727327314796446 5, 66738333706969720355292207099365
17797053812916528936873626422295997956892073437608466673345610466591708954318522770521974566575022354974853539867
7139350, 58790418031245170318066302477198021884477251204428881108559075469565434718542814355069809687908203211 24
20172481161479879214487811665576489930762332013 6, 46864340634794085287213925222361157745729562024150128352765398
56759308840822109774132533653457958791436040152289099382668946960782675268065945976977143 1, 81944513140341216236
45292874953043868906899758451558731238739345182971126911643030327002247089719765234796367899874722374131450517 33
0794969184864265713, 54446936497825800023536609025402128927467216919569806105966992425350211112265310321871365 27
31940696121989657141468357924442787093663081420964122972650 32, 49664620584746459632512586261608724278384529510 56
10865228886270870594196415183914728597425164116908338789205554472890236075134398884010523158723955743 73, 3415689
86384958288623282769333432546354520632654852101774673376097973923158380787690114381301250847679669824547335342 59
50204032663205014947171034850866 6, 30492198670321094942861049272814891796315708599800847931912081071102611152253
09361797825907130166421603302742863069751045545858406640789891734541694198 4, 36137937841491922110097554886074288
77163935560348733114269389687951497165685491322762261041825459125734297171440959408110806113464512878353595621 35
4124, 12279705763694970673180436576088750272877526458037348371251591370848320075305832402846262804422841673867 16
51741982338558480530558681198476388723725253 95, 40877345239599080056832127332813108739794170402420519232059882 58
19633794076503487565959273225656025114879012014820807454819605127489792304285662919622 09, 50546970004760152402 74
11734850143990243684592669144251535868176609107173884843632468421974693863088509485697601871309219020623898969 18
698251273033571856, 64662267274327121405145824520139519983970096850456319521102019795323464547250680114959766238
01583806032478163289647770739137045839964197764812961280 9038, 74823756640316025618954831379580570287967795410041
95024572914739151104032776194865535763333838972915264431609855807085227694992789571514131184106814268 3, 76207544
02083724684579625184810327744850907650407843527346120090163631536254317118479417295115724409766158753674605470 15
73418199699548515726072566 2952, 64718051366850823837872791256009130717247018020738367732669264535095514823570679
00982905243729171482226221668609086737941523983244769909622762595365457 5, 14328318579478329070293281000390592890
07029591939278996708722558604803690197010239892192003425268078698302947550484632407745367096676671298570808611511
50, 47819508550033678412702853706889631101410669749660665471143943281512698676783617665357189652026699097954120 8
82414001154717918997258089353475775017452185, 59171670118704686249344597564660419162107665016912077910542211504 3
84790429978573953021496496415510350801778094287830315663802965138537955484496416286 6, 41372363122583466455014 08
36502274160260959619157746650025917109933594388765775128222893495968723527433676169202665342203228052021770081399
906934762996032, 28647102763694202026999872093656188436005177902763767153208315986253712316969712008918306397 79
19817337461117019710690498950570144848493553441632473116 9, 53461351058252039600406409020962287941814731855470754
78648433648070835183199369280607873125357336530762942983555825037604739507248934361819021517869651 6, 43211630519
98280825532505549643141656222240574139106514400674720749459051709496308932664622429421275001640249343885650090 82
15224317253710640894768430281, 84897089114605051859418166124552713389368110133790845671015502604565739454786490 3
84785061242941181973006694695527050171776558272709448444185786456991 52, 22739718474207416860681516907108136245 17
59081105797765992214238137807365212745098183178096410491367561261997539893112359432266231967750828490592577380 72
, 41216499670212294334651280812035668747548709105131700794545752519540336375321441907637985149672677540242864272
71349674058209425702935910957170900071382 5, 48436506165397582669698530270507359120085582624990229731099970062649
83400809523989851229002506717985980130737038140593520819480298999566478069615938968 9, 15853699467991311553041667
92386457012394172770118639384910000681642835771323532468563585207012194611439135457247277948695062359471337941 00
9175179750235, 86032881441196665119440033541682373034585234809255603700623885646359530616354227173896479400099 66

345557089758149833309897265764908036946377403726618906, 641012226200876115923093247094868513726565861386488916231355382587699060880251679418845074378698983455913735455512631837718524608656864659090229279228231, 16527144583489800339074589267622703740391892670414596775572362839811603852353263595287933280097926247287643050855717192439454800012237185587025342258030, 436672766808170828568342676362921218069818337776054581192099122997277813740127359509428476819760146506504051154170736556522573304503194059159285655376177, 391409514497013441665156882443744288867908774365022331802910729551279271010127341508691775699841360372723452220782164976844244100821729799208516977739751553793104270025452258761117625200445341235957755822041607486709551337816898474015470938916896911036711958763594391182588434474991050279590491356522717, 57584115592473254303228454322525041631785171154103151093178874729079883455704358742586133432524956311883692239859557427834314150568077783639133527406561, 1590223798003480950297114396591035838081608040013918472912576447499825948326480189436946693926399567607325777127331554498851208122524899904682289056497, 508594325078768712589270447761483637314064836175543618713243325793653923778649992240298803639762434136565090520398147216185576777968974078294811425017160, 500607981735796424601062763652593950206881795518588303248269936126696233959293488652011047831850272639591310073217160385388767288159165116325334755087872109340145607923423586331713677786104465541172981737137447624509711934748165966351698815134174114130389317601227179315560084049221076977811387383235630021, 508712644701346441496420938286134076687613841640100182556431035217063127986072614740067893189361132299512547692465736516045248695413909402311046846878281, 658385557028141802965025652564449433407891461556584901303357010862974756194021775763743801693266647267364943686353459192970772699821606437357720300139293, 241837229117739248919639950016413315995943005387304948762391252584405551125511303463740413522936864848652957115160040795425597165983705063552523887313500, 706069837982298637702508389189615856302065153263948209985159054655016172319787344622197773386191990830518257309178902886613351812776097808662478557290481, 11574928020551879788627561129470863705564562907388661456838163800143145198992173457723644287037869966419076396134774957477432556478226898353190935778723, 610296016923814790536635874919352189892308116325582643006013088773548512840489324247303792851158981549598893782426750704080779165485695907451614940206740, 34604770125285800302365085079448294275594244440799617063053747652130859109690225689984871840665734961588683955127558201536801499336385265078556174141724, 11825597588617747085813837160017740648061802450778741359221519197975620769557373411105506691743139890711450252799721855339832409870791189985511619821148, 342211428046888846127872344762104889665848174787405996084468614795565011843082495176677963164338250134958867744266195019380428833183539491690736223227440, 18626654830829475933724422229531521260247749630282640788454897823986815196267646960322528599768563257608682140163517447300417938175281593596472310333259, 157090749951556665367935994383726535996737350721880457743626695124515800135916114144073836050835446867382327076532914854717504005093461937024076648833318070312927302658521613689204714764496937122522183479326616441032518784470408537206595298873402664366666028335804777378715412285901615379046498740410095606705388808078973507358398160040266718217946420, 23577772402384557801596886168597789666554549003021929356323719604133665153262595199156069065965213041706956579810596768294392894560876103128919580119, 71699058026409903383591705758367140642656320715564592776562414985231704111130111268636522681868943716260492033121836183918600499109157978582867307435478, 59373402817414091738677154486174228500560835052522998356116272078684779029616860677959134494037046168050957703569140611482176556315215450035663111632864978970050684346645753410765937802248505636168494626578887182023273794960033653433460563394458144307982586048416865603229619651223215132716189029755965020, 28870151994623151917023631120163925496751172862446820796983669340074436826020543852010174031614232391623084724927387919132365749617232754179670252501288, 69316076200432522853422621078078479151899079890475362712069060151657101527879255706785128065088204453815353722430442067537036693490873329815183509775, 36560516051914018985239899519554502497534865446638941789887125772466230063679465257307719235068303888721137471297120062356395485372053837452558786194732705383745255878619479582636945897341257214132582557363092131208020658278233018010960000772115403361978048198292226385649907403671206899150419230608185369698453033360481520948564634856890061396617573026325499682957433376693691992474718806773199560189824785196805497315571286020183516630241334112212777785882656481533200963457355599444553542918636294818393448981258140805854896344771404494641486313994489712061017959934634948723074739252828514224659794230711270273986941151181246, 5004440478258797544235861132141858589914031090802136033131586314105761655234066901124380114339529981508025488479425995907761905431560001456871867826258848, 185581863132864348273423931308576883819812405225405696529737403169249065207005548282902164615035343613289213966132291144360610296452837269320962109283651, 68121379646664377662543670223776546293099986219464564654888075357435343435295885243745380118444351548491552692045476944398276755320279785851733710778053, 69676172471015297584764278648519463973205605601973973954462659583351488700599697084095357354579852852975382605861180382202167440159214607938057506594888, 39868944884482077091789165603089328814636077812394209556130445270433071989411476864469152420597572325645830729366730705237597203343357461240500600362535, 23984225124526499163679989394300108542505969311640364168939273256169801709960904670771326948340213899233512604169808182913494660805720194941581797486789, 35140762457338703522439666809223184036794921565129617900381351263704514634805278362132497435

138148263120289598367498165241519353320876411527172006380453, 24710691291453760841127687544504422972359827070499
809049833293022746980471322200519845199709962567026745924106667690801956717451739332740526036551644785, 42582526
200077717150143034364406179825370961007062721122124035466123261273825712581697916024437162094418224246572238536 8
603922602363913920472716535315 24, 678574831943399544827085192858799710580571703314480363019586217159167521080652
1083985679636075166632064244739410963790478504253916209411107280204733549 7, 25996584368879485101464281211431222 7
0311474436315255066097573906424588555325614896291500818473644752988078154748378704726917749596783076943413881775
398, 6241751146278383939817976706065988078356709668731578239685723301923876413747474064539988235882964261647382 6
4494276548137002823138797468641450854816969 94, 2504681517463220688691553232463861275223504674605239655618137337 1
4089590079803749649470169926677283558792801890354564441402029569191680843309211758667 99, 2674608724500327101909 3
2420661869601184453598860888544493671230735057257000643702707715412018303837899789222996690350823894922272825118
56195439127986603, 1289994133082157896936795512637751894237439646121209998014827291367080841345682270073990820 05
34046934604705454192034690229329311450091796802978183417118, 347594550783374667136875708377592993911458881341022
7755196235802462075868817118780191166784457785454891426310045430544983230175124467705080832676557393 5, 626415685
0983371371157099704238016523566483541788004783488711994110653394683862516548530954206287451355858093783781140177
5554996056276012858548810747347, 541940196641344415773063660788214492697794384592430018962660571826344027374475 1
462958881125176125112961115386019500347264296298778205161110370896148527 2, 96767199756057275895765675948062841 75
6545114633469167585605170208809516894320812691003956256758181969251279977342159471767633033271331070637286528650
92, 635667494897277726203921732413546901914799962085150131408996094823230180898912746285879453480537328504027773
7561648821913473247502116753661418374912423 4, 41389623900588800459370336537971008333777146975023702675438708757 7
49752963555785484099714125932669585301871871129676831310055260650788211828337348491635, 479170751289107213365249
1150647753830816696383567603323987900567938892209945301370849260238478933357108303729023469862321618421527911346
482373028946763 1, 420783969659237962921975671739861463905991800347263054039809895443009244885948535006701352972 5
12277595679494530843876238245891725750283236723473747919 41, 26303467325603478409681425746270561760458104487375 75
0208136288587139525406524153947947748518132616711483856699835473508339705278736292600540239815382909, 7021090394
3912719585335197681971161149552376713285943471513533016171830587948389001752097220135466501852133147457131249134
740746493652843424857558685008, 10982176703594503335099043190281003439554172817765519010960096427582643358491587
99901389411671727258361434884336133936935212604030249801251334017362017 9, 1537529601432254247751207979336545183 5
2945486327292391772982436083124960552069832090517852078163560147068274646821181038028484587652310225305765266016
10, 6074128165704494972527910109791671840875997800288842722570108204437505070840424348577242428606175392758229 68
60956198565404203687044663002010199141883054, 51453860908549486935732242355904656953839434743576398315040968465 0
957095543023789907888448345644790905762267046241936136512093061745018762608821755126 00, 4212142984323563416500 35
935662538127132261654316031179219554026856337414292698685216800132864328156565105845979405436126661072584257759 3
579078679001204 1, 758473365229957085988595074819881944860141773056609971898427283364329515130697075894879511841 6
18811192600903433242856189317584054131080751583395679259 03, 6575834181722262145788510891659615875509830665822092
1631792142654742204146490776266664280599781759820995333825069037428985525987702654906233411792587673, 1575221386
76017165478752930018661131638875824110520239852660753510563843154645359357352512393019739732332868360622555077 77
2606747318955306000573339946 65, 1115150600942561644824474773959125092350068870070915680282602841096124775011151 3
1671625573467768250442497321476040632965089815930091089610675516263954 68, 24988307810903416422223700059042860807
1885078653788992132176299744811508320357975968506224185740877997718652008410877173350836394926110119689195849869
91, 1918898399906814521148573084088730210703599556098890832582255574778872714229690994342099173073640723265776 26
26482614632643567904876131676294106469080567, 491658071492916100787672632130119322293698900953749483391305839967
79251886618924483782989424700910216292003196618943704463960760836284727712556416138720, 208801208253147663134708
651253085727955776620084201471411895507905021019076569494390652730366010145258123073216954091420981534273504561 5
977992406599542 6, 313414827763855217293161538890996324326763144050015180167840873363367846046662558037249062385 5
5969103212778084178159865936956452281868375643597735452 08, 76027513376813747014021359611570577983815818102025816
6672586922961153854132272966198757747048566160687426974897579912645864467266408121859966195265008 68, 95763863002
1938345892190733670498714800225597665286175452767298904121349957377234446492734417016085413480116903029942471402
7104595802440175290118115467, 478463123438895359704160118402735594700231833386807465151011246584089613050184381 3
4079804670804491884363672682872663103910308908246260073683029778116394, 168360202258950412833998655702789525633 6
1372411312099179664436864693089583825672663104654006872379721154178277022850302378558639898531813871944866012688
, 2931255544386635311537528579702085893359381931771475384897405320775114479879048931660744270265159778667097242 4
27301557746572397118395431729063225551834 1, 45952399494660064838144555112298851928990690958591804048587523480566
85167938366938786666850743686382234895316942445848009673982183732680195330162292656 2, 683348765173218358712175 64
4463957175153551683049961498956527067270691471652819844112191621064815946080009957555151779899698717529318256390 7
90021401438718, 258610296416669725276343090139682745427994020098685716071866827118833475484732606956688317502520
788322749433536024642647201655688889257067285740873426 28, 685517750886881841997719421953554269116680326742294300
629974037265383795370674909785773291784979212916865612178436485660109185934399058105986123189052 17, 377650255056
825834643622111823987576034233825090259475218731123437266947023005731348907945272890028517670370291901718159998 1
1136695377397688834815605025, 4249505767147772196031020651289585799937480050894276528897542147646240685440344617
119239879135528543262687454500110733454342336571756916026373576137223, 1221189774655219068425213537503819357122 4

731278828097646293011671737319460987527595630272305866452394238518927533887961137804982383129793243658322073814,
636721599258317020846085937708713788328406347652542425809227938782627806573032153000653431997450826173263643015
679881882475442906584123237083091285211112, 591615240009758025904380119154286921946102200982657161253129472365481
484474238831310120073467700762091176505689096370650770873685438893895426109063681 6, 143171199887716368105669620 7
898266750468047221273101556016325894979113617531550770988223435737560803856784246755828448586232390686576078294 6
330956519430, 734254264987636003633984776328460271875949938745075845211479272600637312774466228594804544906555 97
092173511066199697647323557539421105251159917461116448, 512916710086978122639543163539588182453580498015150134 02
923829127778604245127923912127853869137576703271789663513404617700625997281587078815337810294446, 167645525178 38
375964591874922821157969132749425046056275194064910709033826102499972685485237677710147299249213993545772193666 7
192027177773044365251382 30, 592955570126527447722080904979265087636668613801905719692432455014114541183875169632
621881761322186396856097914229286949493626619892984054123868949593 64, 656802392453068562983451116058063594970398
620136029212888017622803645061364947772410633969491845337930430228575391476148169752386092437336047425590304 17,
723754578891485767898110456757637177438133267829177923913775467026175985195873572387162639437848392910856901925 2
633764848697932516224490767411929050317 9, 532340779920072079689846299079559238071938646607715716650778715054227 1
896606530101531820042941788671303553308120684970129414452497060715701872788101142 1, 158864839317929742030504247 0
089649446902263275039256601794089609211302001130144711545227904720070284164680940887412128600691534099308464494 1
811925011891, 400002621160118550210666364176201170872543070373467192098007313189191828529508175254917 6309539210
781833933753231318484114385042186535101430855179243 54, 103196496245567319040394474258250696671833473604302563301
424177107662545622236867340711097439561448034181549428732867291257099538171807156255015891625 45, 295912729907009
114211658497010131409849825920902337312211353416448956172383461659775435745782671225981182472196801904263740146 0
259286073863020743546081, 269669631878740685496153339738021587998750482696475616393195828739861610933366383739 47
258726531714616272425009280351155372607494769526061426271185799776, 604803796869403045043442109348042478838445 03
527104600258142856523953218645216216990403655911740533083627163777976245336274909972984546880202034729883312, 27
261558287522575971851824442111090365144022873658966480485633047176320843612473205407488091205599851003730101551 2
139294200571070393130522165221971989 78, 592488950996841205564181291305319996695359567860591072340438314081699562
114523283028876624338711999952120686770190047065872320415823373153118995756475 8, 234531567966554502471161413073 6
662375841807756576707376020845438242954618665426554867786777535406756084081639189663175944108343566049500115902 5
898492686, 761505034043585357463222033108611133405365456232774647716974765867986900773248765843989281625932187 98
780607052161166996099801460843556940059525992786824, 377273158761728475913932750922267351971312164157627713774 1
373327831827247473435512306043337156965991700136410696885151255831157825105690279082625332709, 340634466555756 84
287153287784734254171212485972386063875998727605151998698499957152558118780955043931859154057516779473847326673 7
862332940779868596176 90, 474834705907822053330784964394585251386097291223820727339993547562468201630156602013726
720524762278118480011510062062164432417315731558884245353671767 08, 392184209072331523493375039977500163727015240
445693182594990480637486715318814749593516785694308099881193172108581141170535510939653930112433813784929 98, 346
813155305357896000101560296376715878805746572198412084124073507251650659757384260350199082220679479346402180280 6
560076775375056030120729565673792 00, 452203373501441372494560971665947875923368417352742986853717119940023524068
865791270214446697221434162111349159680646540270969053383005920931070537085 12, 546001210449437703376280335366867
291091093287216792323561703284089798633465438578355561499931308622424295038874284084401113602785737526087939667 7
603020, 370236461444233211749947171179080193186500724602882629388752731289866721141851075894329720313042902115 65
654988060691997961153590815964538144365251181775, 631774772234459100492013842796900789300198192842643060675008 75
252847796215965700799007341759196250450491593055470958720571995993265879745352512656382848, 170058301295164959 06
117290349812861003427215885581428809645825667999107875142200662686820669814282295582269441610135180562290078121 7
6089692828860741392, 172460387651730673132498782153593309575275873266625026459852916352460534700159157285373307 4
077230368672190645542691321453453026107990160719293403993806 0, 459874341473999961974967820269932985579589545704 7
673278384876060979354963587142962027706959116023942669911684287795552943573941865886283566909841182631 6, 2111149
054730315298794485410803630322328164352239615065397256970437915669730191051672783018477014466277008010791354013 7
717531007645289253745952440414926, 106982328790341068012603537591162578845330089498485027541623809926414378943 67
605208136298588395112435423177990947470598835570681171317007264887720823778, 542936430788511723646878369349908 21
579687484157127703064858191752204436487026179374856533544917557799042002597904530828982489891703237561281336459 5
90518, 477970055800772738344831095917547938069859499613173988467694835056685687556033942845651649126468401496457
638019034934687556062225099792888854360397972 14, 373865066281532603848401509941247011818362008908090740834277852
988158504679040262089906228294082071129686032739956556473511726911306591098696229415133 99, 130572057119340464671
180087396526126757580527582905524361051797649034484691999579257820893421000344358116180768568980391253848468737 1
8510721165423899617, 180161419078084331459610252844675897889002847499429235164573104687094370017889661787510791 9
806778383167355946358535685181141381489693980706747555542737 4, 281852145414990791048992990967058444765087979186 7
488972421891835949153862704676806073926726264156308597839554730272621351167775406598814447400642166991 9, 8541173
904106443905299905768662395072832935944800738204096451433781271007344649650999312461498262780266939438629628997 3
605035246099876940558715407978 22, 555838569389658788517277725320126155911070087341795992138497311441397503329907
749630544967288706269559600235487374882415522315328769108959707179807236 26, 731268788817014897116845281702872009

411638944646776678903576976238030692828924729399452025110683490410640127662730204563315955822397186077155800589967921, 703544011732342038170946038588617285393506104389613869965863239863049566263090696284956466849068503094424262293005862361372868685187418874229683921625 48, 89142842277590751666698438006061128542694650083367567019641198370787326985377912202765203580042945022317881679632981365373794425776582296091669914356631, 71679986255547965813146878140040664201073433340974131720089263707910307438689531571321153842267530643245284971416280923014280802420073531897677737784480, 12700447152069741878296970568845043035888752941098126195431952022535521184822464642258479573298459505834137899501751562570215414736024639835136989283837, 63430047396616680273326897822250360164971580245513601412603695624092981100621104180917765229446547097304591859166387676613423085949453183530782609273496396433749210813022953410436640360654942950942583889361076233368360278656037518887474462656107535235848206921449873711446386468822404009414369597332197967331564851630274889744575564877053915024320348750381733860879963760029288286952415043130610380611202287853110449108590432736764101996881476127456612908, 53280882069162605530191514443798777810028687362597894103548425458220909107156582202503516464523795628658208894147158134959433009893999958404472326887421, 33987412638079761735126555460021225568819079582348419476130572631524190951142125555279430092745231216914642104268144970982726216308555881726629242470610, 13682406178752200853488921722342196537145987369704113476544421137346145516814433815172365070204243148827801660590665538792993163703633151871356444406959, 59463989125735016166555373271475329218895751331847622880739844997590477284788570075116983616019629056762256994818763091149753839468824722562416533043843, 67281682017361977913152739570150548267207777610917492408365814330418488902058223459045634717266171571439824557859718739925029610690419177548771060547694, 39405781498711220413739963695737002658793585701279503786490288662610492817823621117021234029885675098802400891723678776479565707731211683846374263316873, 5303480741935887476635043237631574239529698874402253078511746248484692551334468886634906800587182473967353291398744523746147146840024118692722285737183 4, 68305629722812234698423066134000790386970292527553321835797323301872488612831063496859128755927745930236100965836720379665554220277417403641562506589739, 15838477469714165090920618367681569358742354857430493842822696358423656464701334055269093431007279544256458871593017800573626348214105467971882806009973, 24406667934205773393486573213298175430629511700972743156092216312470305819697796258655710647669449052724920514990995515510027140733652668755162210879284, 68460243344752374579091832429666515661775987782765587913153602252111100470593112703724890209241836723350279279958880258422671884541542173747990780407761 1, 63808325950210035810812291635020630613732453561277058010602422073363230632345954950950233595453773160105621255639806986604615621453822332892789828462090, 35920729037346907063152399926080706264554331849560440381191227037937910244659464632447084476697840313861056020706495596126485303699013742182912707172975, 70315041903670157336851359766913844259670523706324294379204277248685999742047453561977925733597786796424146533733873673211660303409007875211743693703450, 3930053112686031995539834584776101060383422532553536492597318967388358901970488313064816317976714133750730006766103069825352822191659252591862434060753 7, 15496845894895615630021254140566466646250515307806313944390059489493636414202320808813409873352911875321240477276777125460299625425443517127346136060402, 691893199133421404943230293321403887766425269831254380649881056826554053074593802010635658700655987931755615413109180148551682315063977146206855249045 8, 13284319826136226129231185037901985819553434334436034136363422696599972727231112997735289148332196516271619405264890626985179077260440615779761000533675, 47141354451986229521055621338816842478003758611988390046169176610982917702117914199406800715608779829266151978859414114993007913651989935003014956276172, 62006071231519162075067533854248673825540723340885150250907087023728863043449786611822047715700318722376817127112362733271740625676783440798426908449101, 63893521915695074076473015870298955838191664815517808757499000857893428891197252747360448837407785054229725838898014349928665255821170162098307539344307, 53724997828497244329408633732485843721280646497077186636538276560039817034467049143979659252524650609122526779152238242200009648428459318191364710668758, 595600268438674496012762637409331125761821292397528974478577854822669688068508636756399747416238093066758915101900999782991256635686210658335486363645 30, 40908904103345585788262408080445592912077785202466130402193215696781356453887694866479723318713262095397682184771025397015406424244516593134998423540293, 21520846393831470685610096190168502256530920634386412660925756889910811879936477244071180593183278964080595838026896057947192168361175044065775753001472, 71994121934100897695373777005150806654834175335935905432800180220212844161938577456202364343367762384804519329089155317640274999082541777992495590496300, 59953753983754938792876611451670073996692753691715543251991783348339718600355783975827174588450532410169935268798235267585856807755052641657216121321 8, 32018619708338154045357870379406367509414130390075786097563998491238705394761106321287493739342215745501191759206980684126857845949108887540197973688400, 19753200456167466465779432336842541030557413397596794468519345155114986012441764419115444925556673818310817249150486960437725537702448521078373504867565, 73424848582132502354626088892133860800647268600468530817168492064944153668156198440200761080102551286167572164740862528620529517512729205573332520104317, 476989668771596788933648131020329084051271275699953293089100078278793252842827038272434326744123983623489910485051244582982648570980226659325652729753 8, 74355004258607576571833753840053548463378928267424658977196161874473156579212738683557688699040100682847094105589799689843205305201454653584801640872249, 66908920165518145321100820147882571798061670584729418574791655417431204551470372008704732238693301913737163218098157907136070692790760316537616614981522092923134974902977450704347491365638429511473355432249333310332023978934414277369039338417668185812956854961133448630326009193412099111506806575709930 4, 17153283710807583417797086518064762512344132499163280505223698478090291002458606163847203257279411593037898263419480619904785414327965511942845045917778, 22050651142736213565244963818664170172032916896662073301155387192243089695489247087391670138735276225579775431936391388626697441900275744645

141428022189, 509378199651321538114445655189649278604757240532991295577220506391989080744295894606670051918384293061966353735708252966813530034272204261302869715859391, 589132844626041877001723931581003101686354738352809834849056325227076275789568767282903927550440234674068253162307068212384362726389217142375567708591041, 176818901529468962259728044418811075079039841318788712893742131399066630309587739693390536826240673469019917141690680869968582713620825891390871150542921, 390911246830724329332475800090117655587164212326684952959469807799854590577591622035260457731558965229706822890604047406359605191871076132969028622793321, 266593579969124323624407428952226372742763901734963782529808026676645329314180235474699635580518693686700357281445950394736290428317131131761575379650851, 171792267675284855222348971813778185199830804143401109976189439938017387686950176774852737250109279511888299592935495971223478140932518027981501604844841, 198444337370830547374969982875970169865122763798276879992231002656645930485562122700243099743442831542370559121054375308845880655588569066020961958082421, 473487105511140465560193313067943347568082753567618883944617580292434826690943518261527784671233200681236017383669450296088236211206717768707099063751171, 97001175555411479571625392367999292993046709979963595852300767077239642099820898215639322933965638321798799991903570451993473913249794690597737765886271, 134670028736266368889495232710319272131593466089650948176463024012886612826107914780797367712593215661552378192090654358981486517591896225691015074857151, 6303796123581749707020007626278575847737160268856166415291644149472210600443703190905369903562359731905928556718274218364116758412806547528922772977763242187607911895416869027246603819970664313506455920488148791215602497569336950361142384744880154632841827794749450034276833675991153288511197242689683, 47942263513439392830167504616104953960109996199015457630131745546068423701013642403323839156160826426619128873229034532556824671458723559069019818844664, 6874274622182563249219749720388662956433689017106697510006439927726538907944533506432387677351240369908865156490610628224604208935896518456792275951386, 52212644024277302202964993748543423030284246877586585223549426038195599560460361521694871178577347471545868137719848759593471592105056983977953734420504, 70264906652847626089535377366020004277383733482787527044642946126390256017682990657039167855937818529538070303778612928791738038128780113446546585027768 9, 70338735306991917918870792762895693400859231411804513011341248280823069527131025167916532212139891844804984508688078627963308722454289725189496741592783, 11202943024812091871968653090774694646166527588230230055019610642288376456094708642854597051283662781541220199344624011347563372208585467149576852176942, 4546528777207981119440303136383806096626466078443539158628632391516207171097840834864160671551704752584152769260359153446683348461777671929690225445180 9, 15169623996435078849216247400427343363968733516560810866651811037320678250903315110528158438221622688297331087485255287010416118126711779737721856328337, 28852475740061878372356478463808810042887244041514447822647154314012875742232208435189321135142249111535515768003337785061252044994754401654492928310569, 596483040572635584586891868278303001119553263572267507370755778727212027489337736392717046648137369189343627520172703003184695095514475939818426978 5, 342400002708644775320751024509684508394703555282227200940687016170055257472202295700794327659682616264459965768595539320620828071889471221102051215415 73, 360668470093812787502622676431606829914902662907882662794546407588986539717003455769374229874729075716384240551381914485031213112060684031523589037279 31, 111700910072349758527111361745766407642016435846730422098249046223331494791497436896212560912732124608527112413257879769353469401109326565209850224562 80, 582581269455487649507977177827987006247798119592093968143235485093961260113916469538855807424372084842604004779259046868593144978374617517956424401237 37, 19967926920673152856400786885696878947102629857831808775813998592829014590263345080292013471735185782309661488552163583034160303360394712031300560258 47, 23595548276608645278366664833783341231551328905679099443768564892841143279319379101358803895431983463285466294746298308657854039318187145804362431897564, 28934743709613354864565258241746631680813108094971296762113580762338343987458594028223238734444880747190525806972142538811064505340654254617382918695589078290344250340603160706475356554596155501099824193225547562516641550346645186692765332359548753145780024775457891546302235424149662919260477919 6, 27788566883685737903481747231933802166299928088919432671260904020088637407292302594730412087020004041723078159004193447947542516090218561430792231480922, 20532093112179185521013377866112742417812622082022290708449532178388359732865119787523382224112648787182208662206608003197496180647105678758158192400715, 53650577218203110600410729325998398766865814136267255360061172788801435890073996725463408842308335996720339673250282900111659334006005865543492882410994, 27945606735686322555814229684881151888663150442470178076013292048060839982203053567640973752973606459118462199368045579874974993094749585683152306114353, 78301112579278595735177414789427711005542160346479431187348815083857665889050672722188739180080915469996629054971642888212786857463782095745577145494 6, 25025808677568131096842775102792540807686366181393166426022508716670220871341079639434019763537052343485081027257058743353860070591961282205809544500182, 57275545082992817348531435083795200415028483426365916402393970309933619370110077943540129137832238789381871925850416308939738775665281482345475161905493412529795522197341685742117972708665799891046629126028557802376330060219345750557343852699753918800541682917612510175637149121587292834253431715256063 2, 32748794215539175827451064809169640707872656691637312790248785369034804895807371648792467471366168858175551862032815723885968389112394766296982682443669, 19316062337601046084359756740917069089224659580679757830844402882574641776835008814717493659219551992308545704093654161563862554123430967564362043544475, 16698150154757920977809280429499684949586664950572392192530208431996083807110717281687762672769576510155761079366746466550237192996169124113339334886230, 44572056955848609010373092439149356067260311771322096152721745227413956103682879244155534554941522431647827072846297085468860260003046353502705163208246, 27628575438344418993708339803452443890754069104828236665940305554239599902121186251891130374253429078333471004275298197440209461188110

```
8994332259999120164, 619196525620449725864384927852124279806435946732224542607233870396101921243962731877016587922339767643417516025431270603844070446893760486088485198179660, 461097641896883291010045084711714506284962649553743149804520861149359402845344250973451375537923179909512856159616277982480253713852285301047331248074660, 468173879097910351174006198775316010855934309734927098990237388845335657170567029437073837503988786948544566682386619074908937427912901789587470416816610, 590562249206097922045655688300613907453554885653483336169392297082895188251788851051329732962751889416657284005368261083495569340374835238028697929697160, 666049849215007416654789267231434201464380080685093895007281738533595027140915402387303248367245258093825816283604343541028484489241560472150019215553370, 3141958243077946284026531348126325080751279493120314107141625052546957608584947984494774988027671989564710926931667209626629435789878637907200652987686430, 391838327309730617552016473307536169481342261157903204433633382942194517707536943482591673246548881199713828510942863576679639282308449064038862832896030, 3283255784320516413168899839829830028094602407822730101434806505467144706365783146560674309642101764920423301535255518747699612103072011492758793346946, 3336883597499152526672502313128756213683935611321300307463997732320800729880341428956713548725712299724545635456410303516953109696877442970294630349700 5, 6984602500040257436496247059037211384086053542408605921048902503869997713986303549367720747440868029206277376655807722118007331791455770997775107027870 1, 342242326320023551343651346299360055981771406162388584983143059707808522154527889020321359774056188315734560539244728898395142214952163311587220162100 45, 656589809384691471932909953308024139528824159647939417007039380822187270235737825089736345404228195215007819643279194800121704558939809794527817274964 50, 966525034815453665420653013169451566517278948300264299661230459135898205488124309022334015089446476241643906480996619160189655275707471373858910103894 5, 828421576460121798154478599942248822985906181439019719504261337649183677436391633927214996439369644157281923795632710889124836514845055471790257900888 5, 538392107612753841228126781553756242362131809950836378490908355961085323237791519523292620563170644480031668829649788360177730034558317665196158497343 09, 887906695008593729571342637514516896259938961374588184469128868108404775521960594951565492925591645646371516067575936543389930717306194845139609308130 0, 448465229548909320534521705483847379610907002752096423786856620359571051577614374515962177470934018444789886317292303183833279813537123622734243034555125, 431581630029802681768594700969067750427522523257569032675331866541495034389970669320816383619979135542335877614522222466072354276196953395835608544539891212127949412305299557469240851099800784379573409693234444619841081780056117325707423228680768458974203389464304624497967276221837748729943472 2, 789755037438490488751396711321677500077376411395276540762504399568347430869135735710254877011351439903075733491173832003841617308308455840015212821859 7, 167155921769109789204447096547004026740877294038545030836200964815915690676092911057809944017537042556707857254981332695607631934503809537266544340983777, 139972957154510712537472391244286391996176191562312473267298362334171985435041182629388479896493487785008483145556876070529154386951919300138936286900615, 472295997944886130981240563494738231552803929983547657586706868622165063315177232324540165316843226647506443608478789352548001630604076040168618807914792, 352582136943200467016542000108843125883123215721055447770042800465913443544207061199158932054306645005935884186552041028739845001485245188933967016269 55]
```

ctftime上有原题，但是略有不同，更简单了；它提供了私钥可以分解n

https://ctftime.org/writeup/16120

顺着知道这是Goldwasser-Micali加密系统，也就是同态加密；然后在la佬的博客上找到了脚本

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-
from Crypto.Util.number import long_to_bytes
import gmpy2
N = 764125918785890622182682952145881551138482145911596517066068990981488269917652449188458526546925212277962628053839546258267862697145372148511519661130 19

ct = [326675412441832867224786672667975584870152037144374663428090712002478895172679064456576423506501090548046205236777960490634497485981225743178397152380 1, 391098385036934600948077883435474070074499709242871423690424974223062003373662742914112809523138289991363952305815070542502161889180844460254514993988 1, 273178109207658413420869291110421935794973536216100314847800352990011319828784670156659829095485530247874887151332207299734095482845206392037939908002 34, 190492538269352824039282055494543879933618115894559001763982426345336437286567743861211481735599403129610194786842490901299693831767348811888295572944767, 468082715529765979307106828086395017250877459864785124391102290941060542607006096116515921361081056680958037931353841873867981414244566272469340542122 04, 6466355666388787644852182538917168197022617180333504711699460263106018477120891683890706132515722706571783620767768218179173750993093447800641097730533 4, 713709898789024737295380759926117938353810979161996918553928400131364712583146665336311396209108197765456272401367343040446891679040956610089594278670 80, 512076010982936811962256921624917991666228643986733039230183616071948316529674065719569327082590553090100101483140237882898266553129276910799248011107, 252467622001557647256749151174282669463512522239203532928465371420431230041087268465605404274136943486621720 6
```

38375325738057685599235967579145425784917 02, 49840420035538562259818077270014233135437467586063205683943769627434293016547018393482060398482431118280370380641405128927430840198536985630649859298809, 84232356416028819831566679779591187299787046636995543449314912076840614265866721410586346948877186101748353344277333107087862936903079928428665929615, 56255989340747188472994001728565823905145449088080608312012473951209435572526372645545998691635581191431650844541918635345655144222239028951168850704422, 45785662740328453859890278502445450606890445328720454060032120470673511251330845850132591950890320517787732079986810994883608872640852386167756195212718, 54029870403864304285925769805259101311108719589466350768320792251083544066361265116520351278475192456130712826836166473186592532002794991923508524064620, 46624268375793936417415940726172495902868488296085533559474078710715899350421256180929703375516133001459740255662121433900562906914369420876721969039630, 15921219479965848802750013085928522470790034679969324752503581385316275799836521901155562358852385602763599760409651828923729107636248359311532535412386, 20190562475428250717792767608071965792428019405686414394515731600072635056217537304104019807474440130549050089029499956554142652193502911411782760901078, 41983059548033663270367946174234103357083211319135434721003248220792550449588248783877660929189053228157142988622736136441291989249080446689516065393435, 71609539411413240194556215042709157212260128588149087141493760115962392075268935955309314240733799741213805554924840687486128939284886391947755983910372, 48382284720865851648431016945797183660266155498343626372038256476287293528764330285514661435350058162782747986164808116116765643203666318480114386099343, 46730320638656612110889821918114226564809934661179594844549753878327086621670111917286750423548271235812428733761683357631975738361840732519608444014971, 55158112951581407023186496177304925445962183673199215662079568367093310059249411803313113095482726739394326470492736668839734286312650343715767983610363, 37112980203698874196497763225414417374526380133937967213841831269520374856619110460606542911440228172533968362786931746291414834514997777285267403140559, 63322083017732869600484256664107952565424442164218942893502809096945827312745918616246499734990787742358551946831008809185624657787375819807019566756170, 71314994195591048863769827905781024631392362642379644906839018373979322205253702180901860395614124975371620634607063454336469708295675619627591028014091, 58987942295441295007027662413419316243220623197071846210550338622495407069803847200822547917184493216087823262589570286179930999452321610193662415873715, 40463068017819882296397975257296430843199918804116579332129293544451758450871632123477648266871632208235745045407313414566869271527363707673269415792748, 63039255605860594706235701802182469722575918347437216391785141811844940190196047005143996180367679119101277408375635148536688180427946019402484987272510, 71847518795481381405870318786706930914683598350750876400219210332724219278096576686583523369096072741462359686018334607665415715621892012499046687826381, 263372841237538748283191863047912116209305665661201954956651558628538548595434756305451757743342879404188922886973242549945336780980957443737494170451631, 21764014175912521244824061176843027159941043924315159175826402721445924610127916171029483226782579782895796672888523861781938366363972830257845406910975, 34356230957261968440625811723062601598323817164800058850615232853180577880120707980196524666547193455331094492622172835476674867205902070507267885210071, 4591977092182891977776202082499820627431266358262353145742394562793898843757252396073320763992632348009255720373805844912333756081093871016090636447620, 10316176533060759533513950331093265748621797961634020464599935470363429799039909475463319253036787910300618231860969786155510737831206632050394210070451, 59917326034119369331371808884574791893663783551610720886605582940613080599142224466706727532690507606452696459627055492221262118596727675146540248450673, 10842419169283306075038519352806019318831568946592817182841197553628341894023325198625377701960932683672886924641591814480224960323114162850149838499007, 66742064034192815235690238007451310177229882619802417230057418182591053854863990729434269230203542276063435489487230228617313299686445072114861937495520, 1733779950648909881031164053679273315071861388089395063452876203189493125440583098633760967599976357715275089079851849443670113361781767741613719759526 8, 11805355039774973413960279981353089487026545524788641978782960297317350024970913592970423213016483957303390870999692309756230863161264738948268751555880, 59489883634739735974968870045855217812381229180244297407474712914329781106395937678986012546789197922278383445284656100208400201934959073937202913889830, 1140145100091270721703610778502742548800585057404570257742085411993213331773423414143388847704607278354614315882211536190659342380194742485573513880605 1, 18179963830269752328347012892189518105760526272986096873166870569368065912159690171168153334762363786860481716195666269739056960619187285110236225225886, 62509640700826594197993512978970850974297618960597709071687370554258739737985841220615247665877415157805625480566585584212254522216095818226299866458643, 59902221802285992663579252848316843814802689592005085661593355020466291555610095695782045437472840276051219627521675600015574227419430014155086773632 31, 33433077637882273687249451259081443266379398604904264246156118486060075935455701873884654140790578203732502170849912443469942139967789200144428417241869, 67390195969105286284597473259273322568348281288068806381991832178917414558751508417404533918515282632113916633995251246834970162639704436292989924347318, 51701910800000997340054445694309638177497987670712902843876999084308991285244884147388555600534553143954887063896632540769769157146510134074689745758583 5, 64048417355580136172437626164825086735195128281991270452716237192859126404734412422587916788587067007095933362505117338589065656344579539799999449469574, 1102431223382025640978818540565141097390990113966252741053228763306222219896195183639571821489452986029640601203622160995240582824332949043956485593505 3, 45329081591634176909575079913822799290480598748734762443445536547105615371937523789002728790051543635047627596020113965500849934460327043133518899375170, 50858826475819728877134521770119997192668235111631842299351867815878082946160808043722869955055965555491424602575020061945411539811210145167251037970092, 35605374328853657972896594891951135620842006755668179374120075488686032129628717565054614577034983995

0136213269922148546946541544625127408434882104693960, 3117034852103175441811868174959023991593403193679661945624663405217895950940233172036068187754739535088532582485145635984657142355304099240591206545775 5, 59235278298913032815919203840415209842948518118915680147287275616028831011314878653857791522574491917033065613888064574586219759420566309846454002915944, 553199916766178282358283905389456936817027226029379803741833387759284319726061685283725048474594364961934562159979301294758909476602956966269960706853990, 794687045745905997010958562918692847624193512863709414330011071123496604843189581485358825193400362679443693827872128101754246801590767065917412609458 8, 6011089150327240366406539417000381601186711659989313410779536037256517877685137412842940500650771878568469747210075269973248848394680481880018778657864 9, 28279251639525643355877411167790163315397766491944901475131371705035937611147913823680263340304888492788066877865697182783730607520500342177273147964465, 667383337006967203552922070993651779705381291652893687362642229599795689207343760846667334561046659170895431852277052197456657502235497485353986713935 0, 587904180312451703180663024771980218844772512044288811085590754695654347185428143550698096879082032112420172481161479879214487811665576489930762332013 6, 468643406347940852872139252223611577457295620241501283527653985675930884082210977413253365345795879143604015228909938266894696078267526806594597697714 31, 81944513140341216236452928749530438689068997584515587312387393451829711269116430303270022470897197652347963678998747223741314505173307949691848642657 13, 5444693649782580002353660902540212892746721691956980610596699242535021111226531032187136527319406961219896571414683579244427870936630814209641229726503 2, 49664620584746459632512586261608724278384529510561086522888627087059419641518391472859742516411690833878920555447289023607513439888401052315872395574373, 3415689863849582886232827693334325463545206326548521017746733760979739231583807876901143813012508476796698245473353425950204032663205014947171034850866 6, 304921986703210949428610492728148917963157085998008479319120810711026111522530936179782590713016642160330274286306975104554585840664078989173454164919 84, 36137937841491922110097554886074288771639355603487331142693896879514971656854913227622610418254591257342971714409594081108061134645128783535956213541124, 122797057636949706731804365760887502728775264580373483712515913708483200753058324028462628044228416738671651741982338558480530558681198476388723725253 95, 40877345239599080056832127332813108739794170402420519232059882581963379407650348756595927322565602511487901201482080745481960512748979230428566291962209, 50546970004760152402741173485014399024368459266914425153586817660910717388484363246842197469386308850948569760187130921902062389896918698251273033571856, 64662267274327121405145824520139519983970096850456319521102019795323464547250680114959766238015838060324781632896477707391370458399641977648129612809038, 74823756640316025618954831379580570287967795410041950245729147391511040327761948655357633338389729152644316098558070852276949927895715141311841068142683, 76207544020837246845796251848103277448509076504078435273461200901636315362543171184794172951157244097661587536746054701573418199699548515726072566295 2, 64718051366850823837872791256009130717247018020738367732669264535095514823570679009829052437291714822262216686090867379415239832447699096227625953654575, 14328318579478329070293281000390592890070295919392789967087225586048036901970102398921920034252680786983029475504846324077453670966766712985708086115150, 47819508550033678412702853706889631101410669749660665471143943281512698676783617665357189652026699097954120882414001154717918997258089353475775017452185, 59171670118704686249344597564660419162107665016912077910542211504384790429978573953021496496415510350801778094287830315663802965138537955484496416285 86, 41372363122583466455014083650227416026095961915774665002591710993359438876577512822289349596872352743367616920266534220322805021770081399906934762996032, 28647102763694202026999877209365618843600517790276376715320831598625371231696971200891830639779198173374611170197106904989505701448484935534416324731169, 53461351058252039600406409020962287941814731855470754786484336480708351831993692806078731253573365307629429835558250376047395072489343618190215178696516, 43211630519982808255325055496431416562222405741391065144006747207494590517094963089326646224294212750016402493438856500908215224317253710640894768430281, 84897089114605051859418166124552713389368110133790845671015502604565739454786490384785061242941181973006694695527050171776558272709448444185786456991 52, 22739718474207416860681516907108136245175908110579776599221423813780736521274509818317809641049136756126199753989311235943226623196775082849059257738072, 41216499670212294334651280812035668747548709105131700794545752519540336375321441907637985149672677540242864272713496740582094257029359109571709000713825, 48436506165397582669698530270507359120085582624990229731099970062649834008095239898512290025067179859801307370381405935208194802989995664780696159389689, 15853699467991311553041667923864570123941727701186393849100006816428357713235324685635852070121946114391354572472779486950623594713379410091751795, 86032881441196665119440033541682373034585234809255603700623885646359530616354227173896479400099663455570897581498333098972657649080369463774037266189 06, 64101222620087611592309324709486851372656586138648891623135538258769906088025167941884507437869898345591373545551263183771852460865686465909022927922823, 16527144583489800339074589267622703740391892670414596775572362839811603852353263595287933280097926247287643050855717192439454800012237185587025342258030, 43667276680817082856834267636292121806981833777605458119209912299727781374012735950942847681976014650650405115417073655652257330450319405915928655376177, 39140951449701344166515688244374428886790877436502233180291072955127927101012734150869177569984136037272345222078216497684424410082172979920851697773975, 15537931042700254522587611176252004453412359577558220416074867095513378168984740154709389168969110367119587635943911825884344749910502795904913565227171, 57584115592473254303228454322525041631785171154103151093178874729079883455704358742586133432524956311883692239859557427834314150568077783639133527406561, 15902237980034809502971143965910358380816080400139184729125764474998259483264801894369466939263995676073257771273315544988512081225248999046822890564977, 50859432507876871258927044776148363731406483617554361871324332579365392377864999224029880363976243413656509052039814721618557677796897407829481142501716, 50060798173579642460106276365259395020688179551858830324

826993612669623395929348865201104783185027263959131007321716038538876728815916511632533475508787, 21093401456079
234258633171367778610446554117298173713744762450971193474816596635169881513417411413038931760122717931556008404 9
221076977811387383235630 02, 508712644701346441496420938286134076687613841640100182556431035217063127986072614740
067893189361132299512547692465736516045248695413909402311046846878 28, 658385557028141802965025652564449433407891
461556584901303357010862974756194021775763743801693266647267364943686353459192970772699821606437357720301392 93,
241837229117739248919639950016413315995943005387304948762391252584405551125511303463740413522936864848652957115 1
600407954255971659837050635525238873135 0, 706069837982298637702508389189615856302065153263948209985159054655016 1
172319787344622197773386191990830518257309178902886613351812776097808662478557290 4, 115749280205518797886275611 2
947086370556456290738866145683816380014314519899217345772364428703786996641907639613477495747743255647822689835 3
190935778723, 610296016923814790536635874919352189892308116325582643006013088773548512840489324247303792851158 98
154959889378242675070408077916548569590745161494020674, 346047701252858003023650850794482942755942444407996170 63
053747652130859109690225689984871840665734961588683955127558201536801499336385265078556174141724, 11825597588617
747085813837160017740648061802450778741359221519197975620769557373411105506691743139890711450252799721855339832 4
098707911899855116198211 48, 342211428046888846127872344762104889665848174787405996084468614795565011843082495176
677963164338250134958867744266195019380428833183539491690736229327 44, 186266548308294759337244222295315212602477
496302826407884548978239868151962676469603225285997685632576086821401635174473004179381752815935964723103332 59,
157090749951556665367935994383726535996737350721880457743626695124515800135916114144073836050835446867382327076
532914854717504005093461937024076648833 3, 180712075593285410416277299335297597776036863803085751064219235577089 6
237772277641435107116319434482498433810059226241520094868716474796133993906931214, 371758755916219373196208240 75
660098532446211618393274891254086565846020184454461310691428746518208846269028512685632952791283499316042277840 0
66268195129, 146529384444156501461084267273687749113155693903567252366690740386623709023538544306022992859956713
881217972709241849891388328959277154326245218266013 9, 475030544114966130941741861599728834773431491613939925193
684369924175608141755285972853952547007101112730383212927302658521613689204714764496937122522 18, 347932661644103
751878447040853732065952988734026643666660283358047773787154122859016153790464987404100956067053888080789735073 5
839816004026671821794642 0, 235777724023845578015968861685977896665545490030219293563237196041336651532625951991 5
606906496552130417069565798105967682943928945608761031289195801 19, 716990580264099033835917057583671406426563207
155645927765624149852317041111301112686365226818689437162604920331218361839186004991091579785828673074354 78, 593
734028174140917386771544861742285005608350525229983561162720786847790296168606779591344940370461680509577035691 4
061148217655631521545003566311163286, 649700506843466457534107659378022485056361684946265788871820232737949600 33
653433460563394458144307982586048416865603229619651223215132716189029755965020, 288701519946231519170236311201 63
925496751172862446820796983669340074436826020543852010174031614232391623084724927387919132365749617232754179670 2
52501288, 693160762004325228534226210780784791518990798904753627120690601516571015278792557067851280650882044538
153537224304420675370366934908733298151835097 75, 365605160519140189852398995195545024975348654466389417898871257
727466230063679465257307719235068303888721137471297120062356395485372053837452558786 1947, 595863769963459458993 2
125721325825573630921312080206582782330180109600007721154033619780481982922263856499074036712068991504192306081 8
536969845303336048, 152094856463485689006139661757302632549968295743337669369199247471880677319956018982478519 68
054973155712860201835166302413341122127777858826564815332009, 657559446553542918636294818393448981258140805854 89
634477140449461486313994489712061017959934634948723074739252828514224659794230711270273986941151181246, 50044404
782587975442358611321418585899140310908021360331315863141057616552340669011243801143395299815080254884794259990 8
776190543156000145687186782625 88, 185581863132864348273423931308576883819812405225405696529737403169249065207005
548282902164615035343613289213966132291144360610296452837269320962109283 65, 681213796466643776625436702237765462
930999862194645646548880753574353434352958852437453801184443515484915526920454769443982767553202797858517337107 7
8053, 696761724710152975847642786485194639732056056019739739544626595833514887005996970840953573545798528529753 8
260586118038220216744015921460793805750659488 8, 398689448844820770917891656030893288146360778123942095561304452 7
043307198941147686446915242059757232564583072936673070523759720334335746124050060036253 5, 239842251245264991636 7
998939430010854250596931164036416893927325616980170996090467077132694834021389923351260416980818291349466080572 0
194941581797486789, 351407624573387035224396668092231840367949215651296179003813512637045146348052783621324974 35
138148263120289598367498165241519353320876411527172006380453, 247106912914537608411276875445044229723598270704 99
809049833293022746980471322200519845199709962567026745924106667690801956717451739332740526036551644785, 42582526
200077717150143034364406179825370961007062721122124035466123261273825712581697916024437162094418224246572238536 8
603922602363913920472716535315 24, 678574831943399544827085192858799710580571703314480363019586217159167521080652
108398567963607516663206424473941096379047850425391620941110728020473354 97, 259965843688794851014642812114312227
031147443631525506609757390642458855532561489629150081847364475298807815474837870472691774959678307694341388177 5
398, 624175114627838393981797670606598807835670966873157823968572330192387641374747406453998823588296426164738 26
449427654813700282313879746864145085481696994, 250468151746322068869155323246386127522350467460523965561813733 71
408959007980374964947016992667728355879280189035456444140202956919168084330921175866799, 267460872450032710190 93
242066186960118445359886088854449367123073505725700064370270771541201830383789978922299669035082389492227282511 8
56195439127986603, 128999413308215789693679551263775189423743964612120999801482729136708084134568227007399082005
340469346047054541920346902293293114500917968029781834171 8, 347594550783374667136875708377592993911458881341022

77551962358024620758688171187801911667844577854548914263100454305449832301751244677050808326765573935, 626415685098337137115709970423801652356648354178800478348871199411065339468386251654853095420628745135585809378378114017755549960562760128585488107473 47, 541940196641344415773063660788214492697794384592430018962660571826344027374475146295888112517612511296111538601950034726429629877820516111037089614852721, 967671997560572758957656759480628417565451146334691675856051702088095168943208126910039562567581819692512799773421594717676330332713310706372865286509292, 635667494897277726203921732413546901914799962085150131408996094823230180898912746285879453480537328504027773756164882191347324750211675366141837491242341, 413896239005888004593703365379710083337771469750237026754387087577497529635557854840997141259326695853018718711296768313100552606507882118283373484916351, 479170751289107213652491150647753830816696383567603323987900567938892209945301370849260238478933357108303729023469862321618421527911346482373028946763 1, 420783969659237962921975671739861463905991800347263054039809895443009244885948535006701352972512277595679494530843876238245891725750283236723473747919 41, 263034673256034784096814257462705617604581044873757502081362885871395254065241539479477485181326167114838566998354735083397052787362926005402398153829 09, 702109039439127195853351976819711611495523767132859434715135330161718305879483890017520972201354665018521331474571312491347407464936528434248575586850 08, 109821767035945033350990431902810034395541728177655190109600964275826433584915879990138941167172725836143488433613393693521260403024980125133401736201 79, 153752960143225424775120797933654518352945486327292391772982436083124960552069832090517852078163560147068274646821181038028484587652310225305765266016 10, 607412816570449497252791010979167184087599780028884272257010820443750507084042434857724242860617539275822968609561985654042036870446630020101991411830 54, 514538609085494869357322423559046569538394347435763983150409684650957095543023789907888448345644790905762267046241936136512093061745018762608822175512600, 421214298432356341650035935662538127132261654316031179219554026856337414292698685216800132864328156565105845979405436126661072584257759357907867900124 1, 758473365229957085988595074819881944860141773056609971898427283364329515130697075894879511841618811926009034332428561893175840541310807515833956792590 3, 657583418172226214578851089165961587550983066582209216317921426547422041464907762666642805997817598209953338250690374289855259877026549062334117925876 73, 157522138676017165478752930018661131638875824110520239852660753510563843154645359357352512393019739732332868360622555077772606747318955306000573339946 65, 111515060094256164482447477395912509235006887007091568028260284109612477501115131671625573467768250442497321476040632965089815930091089610675516263954 68, 249883078109034164222237000590428608071885078653788992132176299744811508320357975968506224185740877997718652008410877173350836394926110119689195849869 91, 191889839990681452114857308408873021070359955609889083258225557477887271422969099434209917307364072326577626264826146326435679048761316762941064690805 67, 491658071492916100787672632130119322293698900953749483391305839967792518866189244837829894247009102162920031966189437044639607608362847277125564161387 20, 208801208253147663134708651253085727955776620084201471411895507905021019076569494390652730366010145258123073216954091420981534273504561597799240659954 26, 313414827763855217293161538890996324326763144050015180167840873363367846046662558037249062385559691032127780841781598659369564522818683756435977354520 8, 760275133768137470140213596115705779838158181020258166672586922961153854132272966198757747048566160687426974897579912645864467266408121859966195265008 68, 95763863002193834589219073367049871480022559766528617545276729890412134995737723444649273441701608541348011690302994247140271045958024401752901181154 67, 478463123438895359704160118402735594700231833386807465151011246584089613050184381340798046708044918843636726828726631039103089082462600736830297781163 94, 168360202258950412833998655702789525633613724113120991796644368646930895838256726631046540068723797211541782770228503023785586398985318138719448660126882, 293125554438663531153752857970208589335938193177147538489740532077511447987904893166074427026515977866709724242730155774657239711839543172906322555183 41, 459523994946600648381445551122988519289906909585918040485875234805668516793836693878666685074368638223489531694244584800967398218373268019533016229265 62, 683348765173218358712175644463957175153551683049961498956527067270691471652819844112191621064815946080009957551517798996987175293182563907900214014387 18, 258610296416669725276343090139682745427994020098685716071866827118833475484732606956688317502520788322749433536024642647201655688892570672857408734262 8, 685517750886881841997719421953554269116680326742294300629974037265383795370674909785773291784979212916865612178436485660109185934399058105986123189052 17, 377650255056825834643622111823987576034233825090259475218731123437266947023005731348907945272890028517670370291901718159998111366953773976888348156050 25, 424950576714777219603102065128958579993748005089427652889754214764624068544034461711923987913552854326268745450011073345434233657175691602637357613722 3, 122118977465521906842521353750381935712247312781288097646293011671737319460987527595630272305866452394238518927533887961137804982383129793243658322073814, 636721599258317020846085937708713788328406347652542425809227938782627806573032153000653431997450826173263643015679881882475442906584123237083091285211 12, 591615240009758025904380119154286921946102200982657161253129472365481484474238831310120073467700762091176505689096370650770873685438893895426109063681 6, 143171199887716368105669620789266750468047221273101556016325894979113617531550770988223435737560803856784246755828448586232390686576078294633095651943 0, 73425426498763600363398477632846027187594993874507584521147927260063731277446622859480454490655970921735110661996976473235575394211052511599174611164 48, 51291671008697812263954316353958818245358049801515013402923829127778604245127923912127853869137576703271789663513404617700625997281587078815337810294446, 167645525178383759645918749228211579691327494250460562751940649107090338261024999726854852376777101472992492139935457721936667192027177773044365251382 30, 592955570126527447722080904979265087636668613801905719692432455014114541183875169632621881761322186396856097914229286949493626619892984054123868949593 64, 656802392453068562983451116058063594970398620136029212888017622803645061364947772410633969491845337930430228575391476148169752386092437336047425590304 17.

72375457889148576789811045675763717743813326782917792391377546702617598519587357238716263943784839291085690192526337648486979325162244907674119290503179, 532340779920072079689846299079559238071938646607715716650778715054227189660653010153182004294178867130355330812068497012941445249706071570187278810114211588648393179297420305042470089649446902263275039256601794089609211302001130144711545227904720070284164680940887412128600691534099308464494181192501189140000262116011855021066636417620117087254307037346719209800731318919182852950817525491376309539210781833933753231318484114385042186535101430855179243541030196496245567319040394474258250696671833473604302563301424177107662545622236867340711097439561448034181549428732867291257099538171807156255015891625452959120790091142116584970101314098498259209023373122113534164489561723834616597754357457826712259811824721968019042637401460259286073863020743546081, 269669631878740685496153339738021587998750482696475616393195828739861610933366383739472587265317146162724250092803511553726074947695260614262711857997764048037968694030450434421093480424788384450352710460025814285652395321864521621699040365591174053308362716377797624533627490997298454688020203472988331227261558287522575971851824442111090365144022873658966480485633047176320843612473205407488091205599851003730101551213929420057107039313052216522197198978, 592488950996841205564181291305319996695359567860591072340438314081699562114523283028876624338711999952120686770190047065872320415823373153118995756475823451567966554502471161413073666237584180775657670737602084543824295461866542655486778677753540675608408163918966317594410834356604950011590258984926867615050340435853574632220331086111334053654562327746477169747658679869007732487658439892816259321879878060705216116699609980146084355694005952599278682437727315876172847591393275092226735197131216415762771377741373327831827247473435512306043337156965991700136410696885151255831157825105690279082625332709, 340634466555756842871532877847342541712124859723860638759987276051519986984999571525581187809550439318591540575167794738473266737862332940779868596176904748347059078220533307849643945852513860972912238207273399935475624682016301566020137267205247622781184800115100620621644324173157315588842453536717670816, 392184209072331523493375039977500163727015240445693182594990480637486715318814749593516785694308099881193172108581141170535510939653930112433813784928998, 34681315530535789600010156029637671587880574657219841208412407350725165065975738426035019908222067947934640218028065600767753750560301207295656737920, 45220337350144137249456097166594787592336841735274298685371711994002352406886579127021444669722143416211134915968064654027096905338300592093107053708512, 54600121044943770337628033536686729101093287216792323561703284089798633465438578355561499931308622424295038874284084401113602785737526087939667760302036, 37023646144423321174994717117908019318650072460288262938875273128986672114185107589432972031304290211565654988060691997961153590815964538144365251181775, 63177477223445910049201384279690078930019819284264306067500875252847796215965700799007341759196250450491593055470958720571995993265879745352512656382848, 17005830129516495906117290349812861003427215885581428809645825667999107875142200662686820669814282295582269441610135180562290078121760896928288607413921724603876517306731324987821535933095752758732666250264598529163524605347001591572853733074077230368672190645542691321453453026107990160719293403993806045987434147399996197496782026993298557958954570476732783848760609793549635871429620277069591160239426699116842877955529435739418658862835669098411826316, 211114905473031529879448541080363032232816435223961506539725697043791566973019105167278301847701446627700801079135401377175310076452892537459524404149265, 10698232879034106801260353759116257884533008949848502754162380992641437894367605208136298588395112435423177990947470598835570681171317007264887720823778, 54293643078851172364687836934990821579687484157127703064858191752204436487026179374856533544917557799042002597904530828982489891703237561281336459590518, 47797005580077273834483109591754793806985949961317398846769483505668568755603394284565164912646840149645763801903493468755606222509979288885436039797214, 37386506628153260384840150994124701181836200890809074083427785298815850467904026208990622829408207112968603273995655647351172691130659109869622941513399, 130572057119340464671180087396526126757580527582905524361051797649034484691999579257820893421000344358116180768568980391253848468737185107211654238996171801614190780843314596102528446758978890028474994292351645731046870943700178896617875107919806778383167355946358356851811413814896939807067475555427374, 2818521454149907910489929909670584447650879791867488972421891835949153862704676806073926726264156308597839554730272621351167775406598814447400642166991985410644390529990576866239507283293594480073820409645143378127100734464965099312461498262780266939438629628997360503524609987694055871540797822, 5558385693896587885172777253201261559110700873417959921384973114413975033299077496305449672887062695596002354873748824155223153287691089597071798072362671, 7312687888170148971168452817028720094116389446467766789035769762380306928289247293994520251106834904106401276627302045633159558223971860771558005896792171, 70354401173234203817094603858861728539350610438961386996586323986304956626309069628495646684906850309442426229300586236137286868518741887422968392162548, 89142842277590751666698438006061128542694650083367567019641198370787326985377912202765203580042945022317881679632981365373794425776582296091669914356637167998625554796581314687814004066420107343334097413172008926370791030743868953157132115384226753064324528497141628092301428080242007353189767773778448012700447152069741878296970568845043035888752941098126195431952022535521184822464642258479573298459505834137899501751562570215414736024639835136989283837, 6343004739661668027332689782225036016497158024551360141260369562409298110062110418091776522944654709730459185916638767661342308594945318353078260927349, 6396433749210813022953410436640360654942950942583889361076233368360278656037518887474462656107535235848206921449873711446386468822404009414369597332197 9, 67331564851630274889744575564877053915024320348750381733860879963760029288286952415043130610380611202287853110449108590432736764101996881476127456612908, 532808820691626055301915144443798777810028687362597894103548425458220909107156582202503516464523795628658208894147158134959433009893999958404472326887 4

21, 339874126380797617351265554600212255688190795823484194761305726315241909511421255552794300927452312169146421
042681449709827262163085558817266292424706 10, 136824061787522008534889217223421965371459873697041134765444211373
461455168144338151723650702042431488278016605906655387929931637036331518713564444069 59, 594639891257350161665553
732714753292188957513318476228807398449975904772847885700751169836160196290567622569948187630911497538394688247 2
562416533043843, 672816820173619779131527395701505482672077776109174924083658143304184889020582234590456347172 6
617157143982455785971873992502961069041917754877106054769 4, 394057814987112204137399636957370026587935857012795 0
378649028866261049281782362111702123402988567509880240089172367877647956570773121168384637426331687 3, 5303480741
935887476635043237631574239529698874402253078511746248484692551334468886634906800587182473967353291398744523746 1
471468400241186927222857371834, 683056297228122346984230661340007903869702925275533218357973233018724886128310 63
496859128755927745930236100965836720379665554220277417403641562506589739, 158384774697141650909206183676815693 58
742354857430493842822269635842365646470133405526909343100727954425645887159301780057362634821410546797188280600 9
73, 244066679342057733934865732132981754306295117009727431560922163124703058196977962586557106476694490527249205
149909955155100271407336526685575516221087928 4, 684602433447523745790918324296665156617759877827655879131536022521
110047059311270372489020924183672335027927995888025842267188454154217374799078040776 11, 638083259502100358108122
916350206306137324535612770580106024220733632306323459549509502335954537731601056212556398069866046156214538223 3
2892789828462090, 359207290373469070631523999260807062645543318495604403811912270379379102446594646324470844766 9
784031386105602070649559612648530369901374218291270717297 5, 703150419036701573368513597669138442596705237063242 9
437920427724868599974204745356197792573359778679642414653373387367321166030340900787521174369370345 0, 3930053112
686031995539834584776101060383422532553536492597318967388358901970488313064816317976714133750730006766103069825 3
528221916592525918624340607537, 154968458948956156300212541405664666462505153078063139443900594894936364142023 20
808813409873352911875321240477276777125460299625425443517127346136060402, 691893199133421404943230293321403887 76
642526983125438064988105682655405307459380201063565870065598793175561541310918014855168231506397714620685524904 5
8, 132843198261362261292311850379019858195534343344360341363634226965999727272311129977352891483321965162716194 0
526489062698517907726044061577976100053367 5, 471413544519862295210556213388168424780037586119883900461691766109 8
291770211791419940680071560877982926615197885941411499300791365198993500301495627617 2, 620060712315191620750675 3
385424867382554072334088515025090708702372886304344978661182204771570031872237681712711236273327174062567678344 0
798426908449101, 638935219156950740764730158702989558381916648155178087574990008578934288911972527473604488374 07
785054229725838898014349928665255821170162098307539344307, 537249978284972443294086337324858437212806464970771 86
636538276560039817034467049143979659252524650609122526779152238242200009648428459318191364710668758, 59560026843
867449601276263740933112576182129239752897447857785482266968806850863675639974741623809306675891510190099978299 1
256635686210658335486363645 30, 409089041033455857882624080804455929120777852024661304021932156967813564538876948
664797233187132620953976821847710253970154064242445165931349984235402 93, 215208463938314706856100961901685022565
309206343864126609257568899108118799364772440711805931832789640805958380268960579471921683611750440657757530014 7
2, 719941219341008976953737770051508066548341753359359054328001802202128441619385774562023643433677623848045193 2
908915531764027499908254177799249559049630 0, 599537539837549387928766114516700739966927536917155432519917833478 3
839718600355783975827174588450532410169935268798235267585856807755052641657216121321 8, 320186197083381540453578 7
037940636750941413039007578609756399849123870539476110632128749373934221574550119175920698068412685784594910888 7
540197973688400, 197532004561674664657794323368425410305574133975967944685193451551149860124417644191154449255 56
673818310817249150486960437725537702448521078373504867565, 734248485821325023546260888921338608006472686004685 30
817168492064944153668156198440200761080102551286167572164740862528620529517512729205573332520104 31, 476989668771
596788933648131020329084051271275699953293089100078278793252842827038272434326744123983623489910485051244582982 6
485709802266593256527297538, 743550042586075765718337538400535484633789282674246589771961618744731565792127386 83
557688699040100682847094105589799689843205305201454653584801640872249, 669089201655181453211008201478825717980 61
670584729418574791655417431204551470372008704732238693301913737163218098157907136070692790760316537616614981 52,
209292313497490297745070434749136563842951147335543224933331033202397893441427736903933841766818581295685496113 3
448630326009193412099111506806575709930 4, 171532837108075834177970865180647625123441324991632805052236984780902 9
100245860616384720325727941159303789826341948061990478541432796551194284504591777 8, 220506511427362135652449638 1
866417017203291689666207330115538719224308969548924708739167013873527622557977543193639138862669744190027574464 5
141428022189, 509378199651321538114445655189649278604757240532991295577220506391989080744295894606670051918384 29
306196635373570825296681353003427220426130286971585939, 589132844626041877001723931581003101686354738352809834 84
905632522707627578956876728290392755044023467406825316230706821238436272638921714237556770859104, 17681890152946
896225972804441881107507903984131878871289374213139906663030958773969339053682624067346901991714169068086996858 2
713620825891390871150542 92, 390911246830724329332475800090117655587164212326684952959469807799854590577591622035
260457731558965229706822890604047406359605191871076132969028622793 3, 266593579969124323624407428952226372742763 9
017349637825298080266766453293141802354746996355805186936867003572814459503947362904283171311317615753796508 5, 1
717922676752848552223489718137781851998308041434011099761894399380173876869501767748527372501092795118882995929 3
549597122347814093251802798150160484484, 198444337370830547374969982875970169865122763798276879992231002656645 93
048556212270024309974344283154237055912105437530884588065558856906602096195808242, 473487105511140465560193313 06
794334756808275356761888394461758029243482669094351826152778467123320068123601738366945029608823621120671776870 7
09906375117, 970011755554114795716253923679992929930467099799635958523007670772396420998208982156393229339656383

0990037917, 97001799994114799710299923079992939936487099799699998929007070772990420998208982190399229999030383
21798799991903570451993473913249794690597737765886627, 13467002873626636888949523271031927213159346608965094817646
30240128866128261079147807973677125932156615523781920906543589814865175918962256910150748571 5, 6303796123581749
70702000762627857584773716026885616641529164414947221060044370319090536990356235973190592855671827421836411675841
28065475289227729777632, 64218176089111895416869027246603819970664313506455920488148791215602497569336950361142
38474488015463284182779474945003427683367599115328851119724268968 3, 47942263513439392830167504616104953960109996
19901545763013174554606842370101364240332383915616082642661912887322903453255682467145872355906901981884466 4, 68
74274622218256324921974972038866295643368901710669751000643992772653890794453350643238767735124036990886515649061
06282246042089358965184567922759513 86, 52212644024277302202964993748543423030284246877586585223549426038195599 5
60460361521694871178577347471545868137719848759593471592105056983977953734420504, 70264906652847626089535377366 0
20042773837334827875270446429461263902560176829906570391678559378185295380703037786129287917380381287801134465465
5850277689, 70338735306991917918870792762895693400859231411804513011341248280823069527131025167916532212139891844
48049845086880786279633087224542897251894967415927 83, 11202943024812091871968653090774694646166527588230230055 1
96106422883764560947086428545970512836627815412201993446240113475633722085854671495768521769 42, 4546528777207981
11944030313638380609662646607844353915862863239151620717109784083486416067155170475258415276926035915344668334844
61777671929690225445 1809, 15169623996435078849216247400427343363968733516560810866651811037320678250903315110528
15843822162268829733108748525528701041611812671177937721856328337, 28852475740061878372356478463808810042887244
04151444782264715431401287574223220843518932113514224911153551576800333778506125204499475440165449292831056 9, 59
64830405726355845868918682783030011195532635722675073707557787272120274893377363927170466481373691893436275201 72
70300318469509551447593981842697857 91, 34240000270864477532075102450968450839470355528222720090406870161700552574
72202295700794327659682616264459965768595539320620828071889471221102051215415 73, 36066847009381278750262267643 16
06829914902662907882662794546407588986539717003455769374229874729075716384240551381914485031213112060684032 3582
903727931, 11170091007234975852711136174576640764201643584673042209824904622333149479149743689621256091273212460
85271124132578797693534694011093265652098502245628 0, 58258126945548764950797717782798700624779811959209396814323
54850939612601139164695388558074243720848426040047792590468685931449783746175179564244012373 7, 19967926920673152
85654007868856968789471026298578318087758139985928290145902633450802920134717351857823096614885521635830341603 03
36039471203130056025847, 23595548276608645278366664833783341231551328905679099443768564892841143279319379101358 8
03895431983463285466294746298308657854039318187145804362431897564, 28934743709613354864565258241746631680813108 0
94971296762113580762338343987458594028223238734444880747190525806972142538811064505340654254617382918695 58, 5958
90782903442503406031607064753565545961555010998241932255475625166415503466451866927653323595487531457800247754 57
78915463022354241496629192604779196, 27788566883685737903481747231933802166299928088919432671260904020088637407 2
92302594730412087020004041723078159004193447947542516090218561430792231480922, 20532093112179185521013377866112 7
42417812622082022290708449532178388359732865119787523382224112648787182208662206608003197496180647105678758158 19
2400715, 53650577218203110600410729325998398766865814136267255360061172788801435890073996725463408842308335996 72
03396732502829001116593340060058655434928824109 94, 27945606735686322555814229684881151888663150442470178076013 29
20480608399822030535676409737529736064591184621993680455798749749390947495856831523061143 53, 7830111257927859573
53177414789427711005542160346479431187348815083857665889050672722188739180080915469996629054971642888212786857 46
3782095745577145494 6, 25025808677568131096842775102792540807686366181393166426022508716670220871341079639434019 7
63537052343485081027257058743353860070591961282205809544500182, 57275545082992817348531435083795200415028483426 3
65916402393970309933619370110077943540129137832238789381871925850416308939738775665281482345475161905 49, 3412529
79552219734168574211797270866579989104662912602855780237633006021934575055734385269975391880054168291761251017 56
37149121587292834253431715256063 2, 32748794215539175827451064809169640707872656691637312790248785369034804895807
37164879246747136616885817555186203281572388596838911239476629698268244366 9, 19316062337601046084359756740917069
08922465958067975783084440288257464177683500881471749365921955199230854570409365416156386255412343096756436204 35
44475, 16698150154757920977809280429499684949586664950572392192530208431996083807110717281687762672769576510155 7
61079366746466550237192996169124113339334886230, 44572056955848609010373092439149356067260311771322096152721745 2
27413956103682879244155534554941522431647827072846297085468860260003046353502705163208246, 27628575438344418993 7
08339803452443890754069104828236665940305554239599902121186251891130374253429078333471004275298197440209461188 11
8994332259999120164, 61919652562044972586438492785212427980643594673222454260723387039610192124396273187701658 79
22339767643417516025431270603844070446893760486088485198179 66, 46109764189688329101004508471171450628496265495 37
43149804520861149359402845344250973451375537923179909512856159616277982480253713852285301047331248074 66, 4681738
79097910351174006198775316010855934309734927098990237388845335657170567029437073837503988786948544566682386619 07
49089374279129017895874704168166 1, 59056224920609792204565568830061390745355488565348333616939229708289518825178
88510513297329627518894166572840053682610834955693403748352380286979296971 6, 66604984921500741665478926723143420
14643800806850938950072817385335905271409154023873032483672452580938258162836043435410284844892415604721500192 15
55337, 31419582430779462840265313481263250807512794931203141071416250525469576085849479844947749880276719895647 1
09269316672096266294357898786379072006529876864, 39183832730973061755201647330753616948134226115790320443363338 2
94219451770753694348259167324654888119971382851094286357667963928230844906403886283289603, 32832557843205164131 6
88998398298300280946024078227301014348065054671447063657831465606743096421017649204233015352555187476996121030 72
011492758793346946, 33368835974991525266725023131287562136839356113213003074639977323208007298803414289567135487

```
257122997245456354564103035169531096968774429702946303497005, 69846025000402574364962470590372113840860535424086
059210489025038699977139863035493677207474408680292062773766558077221180073317914557709977751070278701, 34224232
63200235513436513462993600559817714061623885849831430597078085221545278890203213597740561883157345605392447288988
39514221495216331158722016210045, 65658980938469147193290995330802413952882415964793941700703938082218727023573 7
82508973634540422819521500781964327919480012170455893980979452781727496450, 96652503481545366542065301316945156 6
51727894830026429966123045913589820548812430902233401508944647624164390648099661916018965527570747137385891010 38
945, 82842157646012179815447859994224882298590618143901971950426133764918367743639163392721499643936964415728192
37956327108891284365148450554717902579008885, 53839210761275384122812678155375624236213180995083637849090835596 1
08532323779151952329262056317064448003166882964978836017773003455831766519615849734309, 88790669500859372957134 2
63751451689625993896137458818446912886810840477552196059495156549292559164564637151606757593654338993071730619 48
451396093081300, 44846522954890932053452170548384737961090700275209642378685662035957105157761437451596217747093
40184447898863172923031838332798135371236227342430345512 5, 43158163002980268176859470096906775042752252325756903
26753318665414950343899706693208163836199791355423358776145222224660723542761969533958356085445398 9, 52573321691
12127949412305299557469240851099800784379573409693234444619841081780056117325707423228680768458974203389464304 62
44979672762218377487299434722, 78975503743849048875139671132167750007737641139527654076250439956834743086913573 5
71025487701135143990307573349117383200384161730830845584001521282185 97, 16715592176910978920444709654700402674 8
77294038545030836200964815915690676092911057809944017537042556707857254981332695607631934503809537266544340983 77
, 13997295715451071253747239124428639199617619156231247326729836233417198543504118262938847989649348778500848314
55568760705291543869519193001389362890061 5, 47229599794488613098124056349473823155280392998354765758670868622165
06331517723232454016531684322664750644360847878935254800163060407604016861880791479 2, 35258213694320046701654200
01088431258831232157210554477700428004659134435442070611991589320543066450059358841865520410287398450014852451 88
93396701626955]

plaintext = ''
n = N
for cipher in ct:
    if gmpy2.jacobi(cipher, n) == -1:
        plaintext += '1'
    else:
        plaintext += '0'
    print(long_to_bytes(int(plaintext, 2)))
```

所谓的同态加密，简单介绍下，从la佬学习过来

密钥生成

和RSA一样，先选取两个大素数p和q，N=pq，z是N的二次非剩余中的一个随机数

pk=(N, z)，sk=(p, q)

何为**二次非剩余**

- 当存在某个X，$X \equiv d \ (mod \ p)$ 成立，称d是模p的二次剩余
- 当对任意的X，$X \equiv d \ (mod \ p)$ 不成立，称d是模p的二次非剩余

加密

明文空间是{0, 1}

对于明文m，从取随机数$r \in Z_n^*$.

解密

对于密文c，如果c是模n的二次剩余，则m=0，否则为1

为什么安全呢，从la佬拉来的话

GM加密系统的安全性是基于模n的二次剩余问题。对于私钥的拥有者，知道大整数n的因子分解，求解模n的二次剩余问题是容易的；而对于攻击者，无法获知n的因子分解，求解模n的二次剩余问题是困难的，继而保证了该加密方案的安全性

虽然我连n都分解不了，但是用雅克比可以做出来，雅克比是啥，后续补充

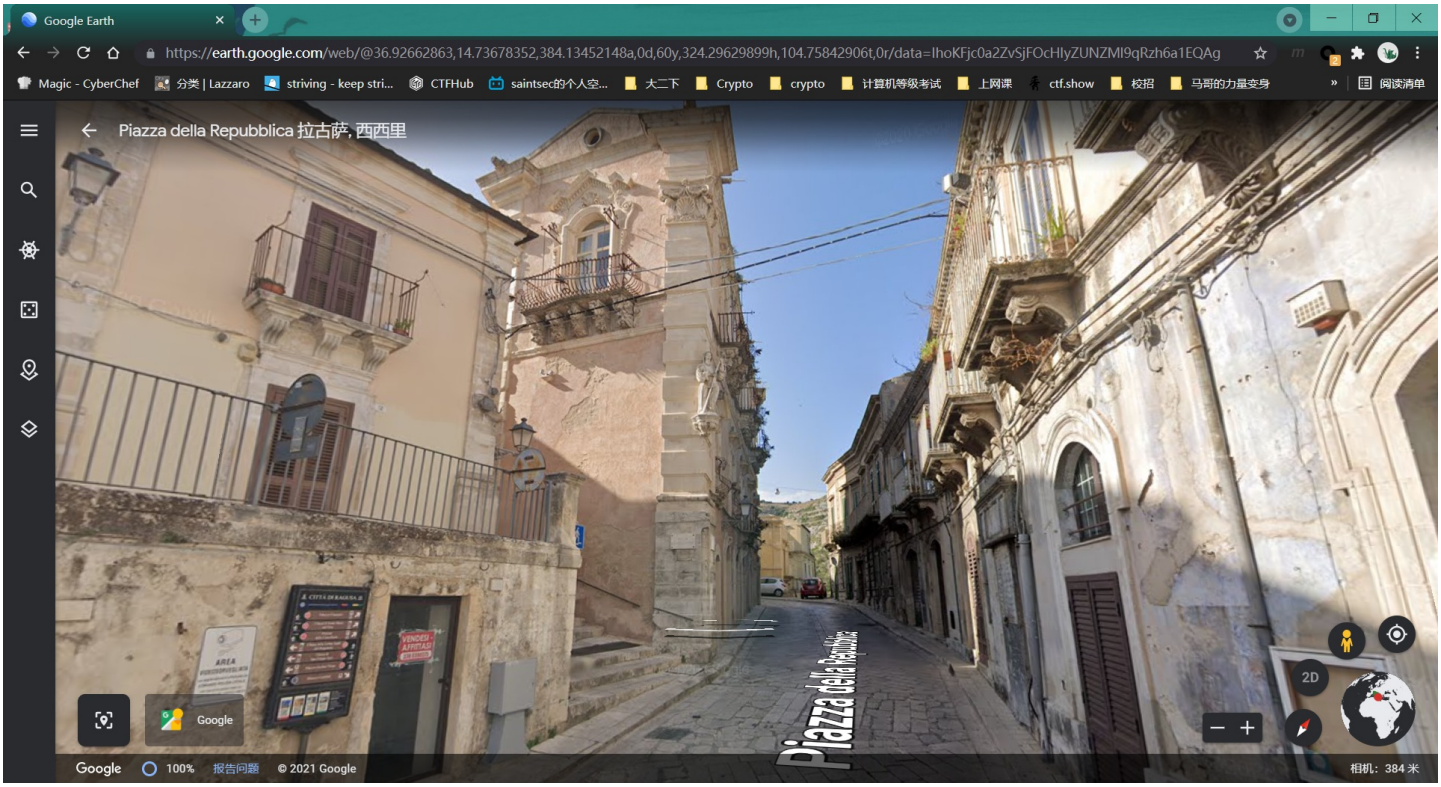
Really Awesome CTF

没有密码学，又要被饿死了；所以手空看了下别方向的题目

OSINT(Open source intelligence)，公开来源情报，社工类的题目。这里有几题就是给一张照片，然后根据图上的信息，在比赛方提供的小地图上标出该照片拍摄的位置，应该要求精确度挺高的

OSINT-Triangles

主要的信息是一个广告牌和指路牌，首先定位是意大利的拉古萨，然后根据指路牌上的一些景点的名字找到



OSINT-Skyline（not sovle）

没有文字信息有点难

好嘛，我按照wiki百科上所有的摩天轮列表依次找过去都无果，wiki百科上的应该也不完整

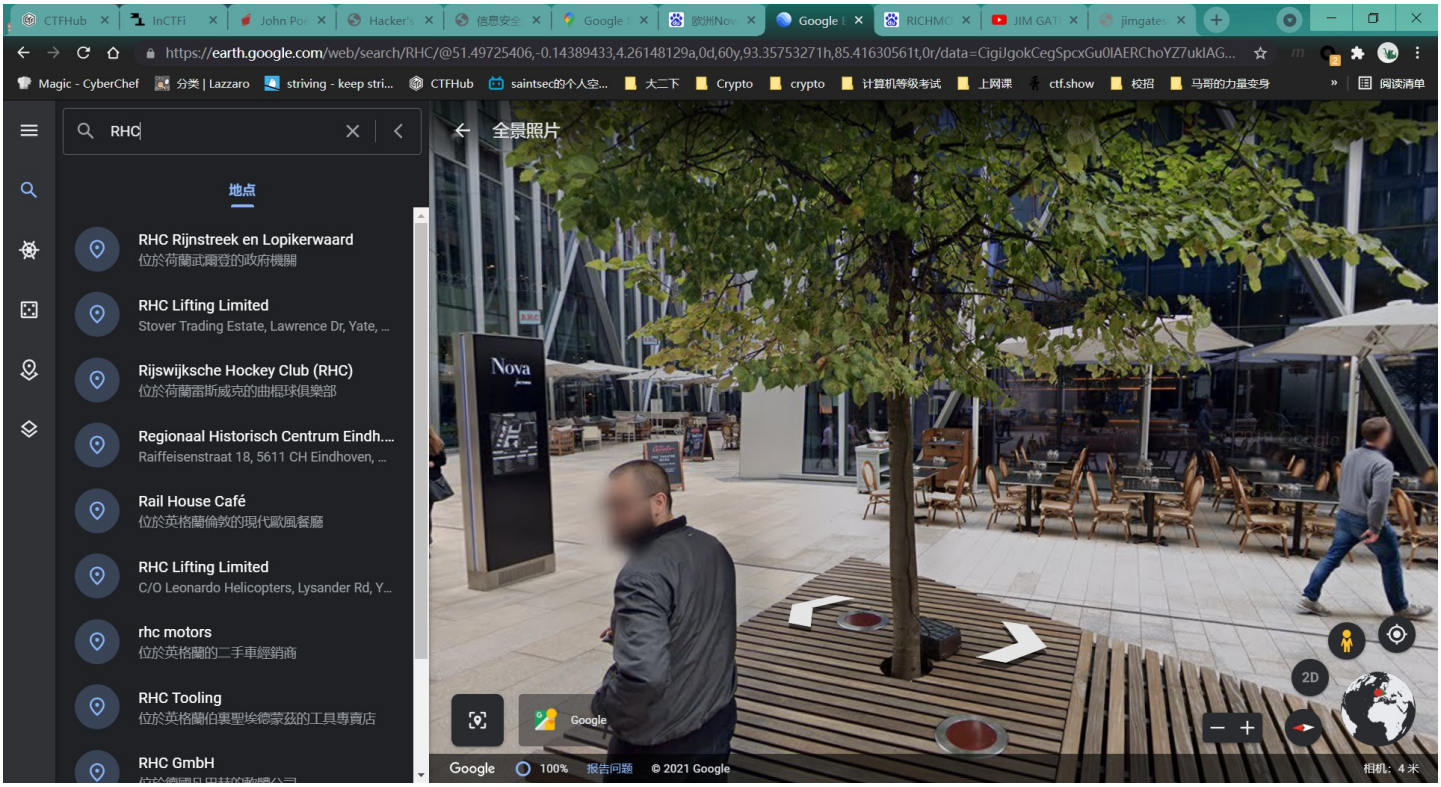
OSINT-Silver Darlings

这道题有文字信息啊，而且是家知名的宾馆之类的吧，提取照片中的`Cafe de la Mairie`还有`Chambre dhôtes`等字样就能直接用搜索引擎搜到，位于法国

是不是都在欧洲啊

OSINT-John Poet

主要抓住R.H.C.（这不是红帽杯吗哈哈哈哈），一开始还以为是香水店，最后发现是酒店`Rail House Café`



OSINT-50m on the Right

简单题，但是没有出

翻译了几乎所有的文字的，但是搜索无果

先来看广告牌上的信息

- `Bistrô`是葡萄牙语小酒馆的意思，并不是特定的店名
- 紧接着的两句话，上面一句是葡萄牙语`Cozinhar com Estilo,Saborear com Prazer`，在线翻译是`烹饪风格,愉快地品尝`，也对应下面英文的解释
- 接下来两个模块的字有点重影看不清
- 左下角是三个葡萄牙的电视：`sport tv,enfica tv,eleven sports`
- 右下角好像是地图一样的东西，难道是临海的意思？

然后再来看交通指示牌上面混合用着西班牙语，葡萄牙语以及加利西亚语，应该是某些禁止的意思，但没什么用

看到车牌`56-UZ-11`，查了一下葡萄牙的车牌符合此格式

所以综上应该是葡萄牙或者是葡萄牙上面的西班牙的加利西亚自治区

然后就没有然后了

评论区师傅提醒我了，竟然直接搜`葡萄牙 bistro 24`就有，这家餐馆的名字确实是叫`bistro 24`；当初我还以为是24小时营业的意思，还是不能放过细节。也确实该地在葡萄牙沿海

社工类题目的做法还得多训练下

SSTF

Crypto-RSA101

开胃菜题，不会有tutorial

```
# nc rsa101.sstf.site 1104

from base64 import b64encode, b64decode
from Crypto.Util.number import getStrongPrime, bytes_to_long, long_to_bytes
from os import system

p = getStrongPrime(512)
q = getStrongPrime(512)
n = p * q
e = 65537
d = pow(e, -1, (p - 1) * (q - 1))

print("[RSA parameters]")
print("n =", hex(n))
print("e =", hex(e))

def sign(msg):
 m = bytes_to_long(msg)
 s = pow(m, d, n)
 return long_to_bytes(s)

def verify(s):
 s = bytes_to_long(s)
 v = pow(s, e, n)
 return long_to_bytes(v)

def welcome():
```

```
 print("\nWelcome to command signer/executor.")
 print("Menu : 1. Verify and run the signed command")
 print("       2. Generate a signed command")
 print("       3. Base64 encoder")
 print("       4. Exit")

while True:
 welcome()
 sel = input(" > ").strip()
 if sel == "1":
  sgn = input("Signed command: ").strip()
  sgn = b64decode(sgn)
  cmd = verify(sgn)

  commands = ["ls -l", "pwd", "id", "cat flag"]
  if cmd.decode() in commands:
   system(cmd)
  else:
   print("Possible commands: ", commands)

 elif sel == "2":
  cmd = input("Base64 encoded command to sign: ")
  cmd = b64decode(cmd)
  if cmd == b"cat flag":
   print("It's forbidden.")
  else:
   print("Signed command:", b64encode(sign(cmd)).decode())

 elif sel == "3":
  cmd = input("String to encode: ").strip().encode()
  print("Base64 encoded string:", b64encode(cmd).decode())

 elif sel == "4":
  print("bye.")
  exit()

 else:
  print("Invalid selection.")
```

大致意思是要用d给`cat flag`的字节流进行加密才能真正获得flag，这个过程相当于用RSA签名；但是`cat flag`被滤过，有web那味儿了

虽然可以获得用同一个d签名后的`ls -l`，`pwd`，`id`，但仔细一想并不能构成什么攻击，我的解释是因为虽然有过了一段时间就换密钥的说法，但是才3次应该还不构成攻击；这条路行不通

不知道有没有命令行的绕过方法，比如用`;`之类的

瞄了一眼提示哦，好；既然另外三个没什么软用，直接从`cat flag`下手，易得`bytes_to_long(b'cat flag')=7161132565001953639=103 * 408479 * 170205956447`，全部不行就一个一个来，最后因为遵从

$$m \equiv (m\ m\ m\ ) \equiv \qquad ^{d} \qquad _{d}$$

这个没想到需要好好反思下

```python
#!/usr/bin/env python
# -*- coding: utf-8 -*-

# nc rsa101.sstf.site 1104.
from base64 import b64encode, b64decode
from Crypto.Util.number import getStrongPrime, bytes_to_long, long_to_bytes
from pwn import *

context(log_level='debug')

sh = remote('rsa101.sstf.site', 1104)
sh.recvuntil(b'n =')
n = int(sh.recvline().decode()[3:], 16)

cf = b'cat flag'
cf = bytes_to_long(cf)
d = factor(cf)
mi = []
m = 1
for i in range(len(d)):
    sh.recvuntil(b'>')
    sh.sendline(b'2')
    sh.recvuntil(b'Base64 encoded command to sign:')
    sh.sendline(b64encode(long_to_bytes(d[i][0])))
    sh.recvuntil(b'Signed command:')
    mi.append(sh.recvline())
    m *= bytes_to_long(b64decode(mi[i]))

m = m % n
# sh.recvuntil(b'v')
sh.sendline(b'1')
sh.recvuntil(b'Signed command:')
sh.sendline(b64encode(long_to_bytes(m)))
sh.recvline()
sh.recvline()
sh.recvline()
sh.recvline()
sh.recvline()
```