

backpack

发表于 2021-05-21 分类于 [Challenge](#) , [2020](#) , [XCTF高校网络安全专题挑战赛](#) , [鲲鹏计算专场](#) , [Crypto](#)
[Challenge](#) | [2020](#) | [XCTF高校网络安全专题挑战赛](#) | [鲲鹏计算专场](#) | [Crypto](#) | [backpack](#)

[点击此处](#)获得更好的阅读体验

WriteUp来源

[官方WP](#)

题目描述

题目考点

解题思路

EXP，请将以下脚本拼接

```
from Crypto.Util.number import long_to_bytes import hashlib from factordb.factordb import FactorDB pubkey1 = [
8930448158498015802128308882328123144827, 4465224079249007901064154441164061572462,
2232612039624503950532077220582030786213, 5621262632766512873643055551054058775649,
2810631316383256436821527775527029387868, 5910272271145889116787780828526558076471,
7460092748527205456770907355026322420739, 3730046374263602728385453677513161210371,
6369979800086062262569743779519623987722, 7689946512997292029661888830522855376388,
8349929869452906913207961356024471070722, 8679921547680714354980997618775278917878,
4339960773840357177490498809387639458996, 6674936999874439487122266345456863111997,
3337468499937219743561133172728431556032, 6173690862922870770157583527127259160557,
7591802044415696283455808704326672962794, 3795901022207848141727904352163336481389,
1897950511103924070863952176081668240744, 948975255551962035431976088040834120378, 4979444240730241916093004984783460442695,
248972212036512095804650249391730221350, 1244861060182560479023251246195865110695,
5127387143045541137888642563860975937901, 706865018447703146732133822693531351501,
3534325092238515733660669111346765675781, 6272119159073518765207351496436426220389,
3136059579536759382603675748218213110236, 1568029789768379691301837874109106555114,
5288971507838450744027935877817596660119, 2644485753919225372013967938908798330079,
5827199489913873584384000910217442547580, 7418556357911197690569017395871764656325,
3709278178955598845284508697935882328185, 6359595702432060321019271289730984546600,
3179797851216030160509635644865492273322, 609485538562275978631834763195789519227,
3047427769281137989315917381597894759610, 6028670497594829893034975631561990762311,
3014335248797414946517487815780995381206, 6012124237352968371635760848653541073121,
3006062118676484185817880424326770536557, 1503031059338242092908940212163385268336, 751515529669121046454470106081692634186,
4880714377788821421604251993803889699594, 6945313801848671609179142937664988232375,
3472656900924335804589571468832494116175, 1736328450462167902294785734416247058102, 868164225231083951147392867208123529068,
4939038725569802873950713374367105147046, 2469519362784901436975356687183552573567,
5739716294346711616864695284354819669282, 2869858147173355808432347642177409834695,
5939885686540938802593190761851748299861, 2969942843270469401296595380925874149937,
5989928034589495599025314631225980457481, 2994964017294747799512657315612990228800,
6002438621601634798133345598569538496930, 3001219310800817399066672799284769248469,
150060965540040869953336399642384624256, 750304827700204349766668199821192312156, 4880109026804363073260351040673639538626,
2440054513402181536630175520336819769341, 5724983869655351666692104700931453267169,
2862491934827675833346052350465726633620, 5936202580368098815050043115995906699348,
7473057903138310305902038498760996732185, 8241485564523416051328036190143541748658,
8625699395215968924041035035834814256872, 8817806310562245360397534458680450510990,
8913859768235383578575784170103268638021, 8961886497071952687664909025814677701539,
4480943248535976343832454512907338850799, 674542823722249070293244197216712807950,
3372714118611124535146622098608356404003, 1686357059305562267573311049304178202011, 843178529652781133786655524652089100991,
4926545877780651465270344703089087933016, 2463272938890325732635172351544543966520,
1231636469445162866317586175772271983301, 5120774847676842331535810028649179374201,
7065344036792682064144921955087633069619, 8037628631350601930449477918306859917362,
4018814315675300965224738959153429958670, 6514363770791911380989386420339758361901,
7762138498350216588871710150932922563455, 3881069249175108294435855075466461281731,
6445491237541815045594944478496274023443, 7727702231725168421174489180011180394209,
3863851115862584210587244590005590197127, 1931925557931292105293622295002795098614, 965962778965646052646811147501397549328,
482981389482823026323405573750698774701, 241490694741411513161702786875349387333, 4625701960324966654957868334200718076198,
2312850980162483327478934167100359038139, 5661382103035502562116484024313222901626,
7335647664472012179435258952919654833358, 3667823832236006089717629476459827416696,
1833911916118003044858814738229913708385] ct1 = 249003040588627839758979396486400138564443 t = abs(2*pubkey1[3]-pubkey1[2]) for i
in range(-100, 100): f = list(FactorDB(t+i)) if len(f) == 2: print(t+i) print(f) p = f[0][0] q = f[1][0] c1 = ct1%p c2 = ct1%q - q pt = c1 - c2 if
hashlib.sha1(long_to_bytes(pt)).hexdigest() == "51d6169bcc32acab2a4d3b1a8d9ced0c9a909974": print(p, q) nonce1 = long_to_bytes(pt) break
```

pubkey2 = [

11617089574048495627606452331959034000544383535732546369818309032016631319516586852335070823009683246490168,

2001316448779658155848404988571514130088911102130256360263677343682117455943065046963232757394199191045541,

10006582243898290779242029428575708154455551065128180138367183811408105872797153252348161637869709955522750,

500329112194914538962101247142878540772227775532564090065919335920529363985766261740808189348549797761419,

2501645560974572694810506235714392703861138887766282045032959667960264681992883130870404904674274898880695,

154554424812596200208607683759282098254748877814712419787100266165393413718121318623089933226495017240763,

77277212406298100460438478796410491273744389073562098355013308296706890606593115449696613247508620412,

18068480321087238767702342929133829876253791528800764224822273493087285330480074917353422194195981322110633,

23238859861315953128531995184302539568743815098664365287765659574217444461424809079472408442987348228855770,

11619429930657976564265997592151269784371907549332182643882829787108722230712404539736204221493674114427881,

2001433466610132202681382251811259522802873108930074497295937127122816291154973890663799456636194625014381,

242117870338229947580877349776412543920183558887290242004291688287883251950258566217597074207454880307637,

12105893516911497379043867488820627196009177944364510212001245844143941625977629283063798537103727440153837,

6052946758455748689521933744410313598004588972182255106000622922071970812988814641531899268551863720076902,

172310938000020808944179059194078142961921382035510728354834288709787202679178941561646980165289427838892,

86155465400001040472420895259703907148096061917755536417741744354893601339589470780829490082644713919470,

4307773270000052022360447647985195357404803455088777682088708572177446800669794735390411745041322356959776,

2153886635000026011180223823992597678702401727544388841044524286088723400334897367695205872520661178479919,

107694331750001300555011191196629883935120086377219442052217714304436170016744868384760293626330589239943,

14743091359522340247475087967573774050292519766150080385615611399158962626849566217949881401952862420386,

7371545679761170123737939837866887025146259883075040192807805699597991323134247981359749407009761431210229,

368577283988058506186869918933443512573129941537520096403902849798995661567123990679874703504880715605130,

16047056120712626275615308679202346386903484305032743223556474252573299626968333616135634697641797925603019,

2228273761128646882488478059336797824068661486780354787132759953960451609668938428863514694710256530601947,

2531880608133665718592506274940402354265125007765416056892090280465402760101924083522745469324485833101385,

12659403040668328592962531374702011771325625038827080284460451402327013800509620417613727346622242916550710,

63297015203341642964812656873510058856628125194135401422302257011635069002548102080686367331121458275380,

173694704609394158929214565634111275344832559397075324646963567825555246312176725199129182544918296938144,

86847352304697079464607288217055637867241627969853766232348178391277762315608836259956491272459148469061,

18546987316007187717911187860588406523979000732756671486971931747237690607762815802095479641525587142034980,

23478113358775927603636417650029827892606419700642318918840488701292647100066179521843437166652151138817936,

11739056679387963801810882501491394630320985032115945942024435064632355033089760921718583362075569408987,

5869528339693981900909104412507456973151604925160579729710122175323161775016544880460859291663037784704512,

17139383870619324695135375925989353117192721796844273040209583915335382683693044061026126991720876460152711,

227743116360819960922248511682730301189213280232686119695459314785341493138031293651308760841749795797876746,

25591775518813331790805079561100775225235594506704302308418022034458365200418446450077766746255467738802,

127958875940666859402539780550387612611779725303521515420901101722741826002092232503888338212763369

86 22438899783680219572521544758462882080210291847629309443505955974893176885609184886069177529230643462364924,
87 25424069592612443530941596098967065670722065258078637897107500815120390238989364063830286110504679298982888,
88 26916654497078555510151621769219157465977951963303302123908273235233996915679453652710840401141697217291874
89]

1 pubkey2 += [
2 27662946949311611499756634604345203363605895315915634237308659445290800254024498447151117546460206176446389,
3 13831473474655805749878317302172601681802947657957817118654329722645400127012249223575558773230103088223220,
4 21120356438100236619619982370821925471518393163242891734681687688996501859690896232583476732504409111912030,
5 10560178219050118309809991185410962735759196581621445867340843844498250929845448116291738366252204555956002,
6 5280089109525059154904995592705481367879397991405405361466835210961124562732461362029072934591563051138989031,
7 2640044554762529577452497796352740683939799145405361466835210961124562732461362029072934591563051138989031,
8 1320022277381264788726248898176370341969899572702680733417605480562281366230681014536467295781525569494501,
9 660011138690632394363124449088185170984949786351340366708802740281140683115340507268233647890762784747251,
10 330005569345316197181562224544092585492474893175670183354401370140570341557670253634116823945381392373685,
11 143696224854449918432716048320076709233631567808518182670317235127440869669636067476127557862445593987251,
12 7184811242722495921635802416003835461681578390425909133515861756372043483481803373806377878931024131993630,
13 3592405621361247960817901208001917730840789195212954566757930878186021741740901686903188939465512065996861,
14 1600082251145295772508977432373658349603731393187046045873348826676681266705522464247291815622113600798836,
15 2220503095649881260722571088160391637863576300199213404721266961057208129712382852919343253700414368199828,
16 25307135179021740048293679160537582819934707484363589877715156308202405861040963047255368972739564751900343,
17 12653567589510870024146839580268791409967353742181794938857578154101202930520481523627684486369782375950207,
18 6326783794755435012073419790134395704983676871090897469428789077050601465260240761813842243184891187975100,
19 31633918973777175060367098950671978524918384355454487347143945385253007326301203809069211215924455936987587,
20 15786315649461192497699178667269223556862838552036707542711720096936452162499831811249157906685580364794218,
21 7893157824730596248849589333634611778431419276018353771355860048468226081249915905624578953342790182397113,
22 18151198613137631869105618386552930519832628972273160061032452851907914836809729573607986822560752658998976,
23 9075599306568815934552809193276465259916314486136580030516226425953957418404864786803993411280376329499495,
24 18742419354056741711957228316373857260575076577332273190612636040650780505387204014197694051529545732550165,
25 9371209677028370855978614158186928630287538288666136595306318020325390252693602007098847025764772866275102,
26 4685604838514185427989307079093464315143769144333068297653159010162695126346801003549423512882386433137595,
27 16547422120029426458675477259282356788188803906430517324181102332755149359358172122570409102330550784369239,
28 224783307607870469740185623493768030247113212874728218374450739940513764758635768208090189705463295985071,
29 11239165380393523487009281174688401512355660643739620918722536997025688237931928841040450948527316479992531,
30 5619582690196761743504640587344200756177830321869810459361268498512844118965964420520225474263658239996260,
31 2809791345098380871752320293672100378048891516093490522968063424925642205948298221026011273713182911998177,
32 14048956725491904358761601468360501890445758046745261484031712462821102974149110513005636856591455999066,
33 14907067537046928962618903793153649725139148124497709482774681389987907311055517173360725530172314847800006,
34 21658153469295798225990275616312449493186493396512837916741863522667755451712530207476060110975514991700403,
35 250336964354202328576759615278918493772101660325204021372545458900767952204103672453372740137711506350666,
36 125168482177101164288379807639459246886050830162602106686272729450383976102051836226686370068857531825341,
37 204630438096273919590998141017085869749194608423940837087858864749257216766950308019291291962336333713127,
38 10231521904813695979549907050854293487459730421197041854392943237462860838347515400964564598116818166856595,
39 5115760952406847989774953525427146743729865210598520927196471618731430419173757700482282299058409083428308,
40 176625001769757577395683004824491980024818519394563243638952758637039517005771650471036838495418562109514555,
41 225858697892602126144649739609602226318578453040456049948309021461935602990705865631411659359863622557704,
42 11292934894630106307232486980480111815928922652022802497415451073096780149535298428157058296799319311278859,
43 19851087148087386898297067209975680538581380660275384424062248364222191870952420834874226494289017223439855,
44 9925543754043693449148533604987840269290690330137692212031124182111095935476210417437113247144508611719959,
45 191673914877941804692550952222954476526264499332829281370084918729349763922876829514253969461611873660410,
46 23788315444669423979308368980850397013248051583930397816039565287038476678146210035552824330620163504630616,
47 26098777423107045734335008210160823137240945126229182083374305471193040135257876638572109511199439320115751,
48 27254008412325856611848327824816036199237391897378574217041675563270321863813709940081752101489077227858313,
49 136270042061629283059241639124080180961869594868927108520837781635160931906854970040876050744538613929149,
50 21018121803853797897642905675939633680426267308608626729614941718491382262138199105816135371261626874765043,
51 10509060901926898948821452837969816840213133654304313364807470859245691131069099552908067685630813437382497,
52 5254530450963449474410726418984908420106566827152156682403735429622845565534549776450433842815406718691260,
53 26272652206172473720536320949245421005328413576078341201867714811422787274788822701692140770335945630,
54 15518252313513196113283505324481851735643561041052022345955456685079513187568409064909205806593209247473256,
55 21963745857528931801322576381976550498438699854789994348332251170213558389968976153250300249185962191537053,
56 25186492629536799645342111910723899879836269261658980349520648412780580991169259697420847470482338663568951,
57 1259324631476839826710559553619493991813463082949017460324206390290495584629848710423735241169331784468,
58 205012428581565336016351697416599600575986649678728623743684930868947043977086545150909213509942233692680,
59 10250621429078266828008175848708299800287993324839364131367342465434473521988543272575454606754971116846348,
60 5125310714539133414004087924354149900143996662419682065683671232717236760994271636287727303377485558423177,
61 2562655357269566707002043962177074950071998331209841032841835616358618380497135818143863651688742779211591,
62 15485947379407117098181845700824162105652918499868903691775440635853110986433339529867629171733728957406233,
63 7742973689703558549090922850412081052826459249934451845887720317926555493216669764933814585866864478703151,
64 18076106545624113019226285144941665157030148959231209098298382986637079542793106503262604638822798907152001,
65 23242672973584390254293966292206457209131993813879587724503714202099234156758132487426999665300752471376444,
66 2582595617856452887182780686583885323518291624120377703777362637199881699725799754807009197178539733803488619,
67 27117597794554598180594727152655051248208377454865871694157712821758788086172488649300295935159224469544736,
68 27763418598049632834978187296063150254721108061696919022433379238553195839271015945445845313468969802572788,
69 280836899979715016216991736776719975797747336511244268657121244695039971582079593518620002623842469086835,
70 14043164998985750810849586838835987988736682565223432850662234751998579101397967593100013119212345442,
71 7021582249949287540542479341941799939494368341278110671642803111737599928955069898379655000655960617271708,
72 17715410825746977514952063390706524600364103504903038511175924383542601760662306569985524846217337876436278,
73 8857705412873488757476031695353262300182051752451519255587962191771300880331153284992762423108668938218182,
74 1863347240720907812341883956741225578070794521048972480314850392355945223635034826329078557443692036909546,
75 931673620360453906170941978370612789035397260524487140157425196177972611817517413164603927821846018454763,
76 18862987802574603275535533611588688575793905636886418876141648808563664855272358686618716985250280577027846,
77 9431493901287301637767766805794344287896952818443209438070824404281832427636179343309358492625140288513923,
78 18920366651415984563564707122632796774565395743485587894389935029814718010002861292450376592201927712057386,

79 9460183325707992281782353561316398387282697871742793947194967514907359005001430646225188296100963856028683,
80 18934711363626329885572000500393823824258268270135380148952006585127481298685486943908291493939839495814779,
81 9467355681813164942786000250196911912129134135067690074476003292563740649342743471954145746969919747907380,
82 4733677840906582471393000125098455956064567067533845037238001646281870324671371735977072873484959873953733,
83 16571458621225624980377323782284852608649202868030905693973523650814736958520457488784233782631837504777282,
84 8285729310612812490188661891142426304324601434015452846986761825407368479260228744392116891315918752388666,
85 4142864655306406245094330945571213152162300717007726423493380912703684239630114372196058445657959376194369,
86 1627605202842553686722798919252123120669806969276784638710121328402564391599828806893726568718337255897587,
87 232426457149851021782948183159962402336959541806479063689051294696866237541846860242560630248560759749219,
88 11171322857492551089147409157998120116982977090323953184452564734843311877092343012121280315124263097874618
89]

1 pubkey2 += [
2 19790281129518609289254528298734684689108407879425959767580805195095457734730943126856337503451489116737749,
3 9895140564759304644627264149367342344554203939712979883790402597547728867365471563428168751725744558368873,
4 4947570282379652322313632074683671172277101969856489941895201298773864433682735781714084375862872279184440,
5 16678404841962159905837639757077460216755470319192228146302123477060734013026139511652739533820793707392672,
6 8339202420981079952918819878538730108377735159596114073151061738530367006513069755826369766910396853696322,
7 1837422091126287372114023365900498968480578691406204071193005369693898529944130649870888229344555994648607,
8 23391730156403770605250940549238119473019812791295003281319549676143294445905424870150138460561635565124748,
9 11695865078201885302625470274619059736509906395647501640659774838071647222952712435075069230280817782562409,
10 2005255239873276395993558857045154498871872532087733995684410246709625407661127838333231961029766459081616,
11 24230895820708971942677603148258201880052855600307850173196727951028614500015335539962313326404240797341239,
12 26320067611126819716019625293864725570643347134417908261952886803188109046192439390776854009091477966471056,
13 2736465350635743602690636366667987415938592901472937306330966229267856319280991316184124350435096551035976,
14 13682326753167871801345318183333993707969296450736468653165483114633928159640495658092062175217548275518013,
15 2104578307735626964535482811402621484601567559632217501937264384990765876005019449841728433498131705559425,
16 24727511239450468567357565125436935372917703114080091926323155020169184734187281345716561562638423420580155,
17 12363755619725234283678782562718467686458851557040045963161577510084592367093640672858280781319211710290069,
18 20386497510634950886520215001094858473846345112784006156935311582716097979731591957224837736548963422945678,
19 1019324875531747544326010750054742923692317255639200307850173196727951028614500015335539962313326404240797341239,
20 5096624377658737721630053750273714618461586278196001539233827895679024494932897989306209434137240855736397,
21 16752931889601702605495850594872481939847712473361983944971436775513314043651220615448802062957977995668639,
22 8376465944800851302747925297436240969923856236680991972485718387756657021825610307724401031478988997834317,
23 4188232972400425651373962648718120484961928118340495986248591938783285109128051538622005157394498917198,
24 16298736186972546570367805044094684873097883934342311684759524261296605164117419772697603759104817259039,
25 8149368093486273285183902522047342436548941696717115584237976212306483025820587098863398801879552408629558,
26 18279303747515470387272774980759295848891390182622540967473510933827043309095065170227396746829133772115213,
27 2334427157454086938317211210115272555062614425575253659091278294587323450732304205909395710303924453858035,
28 2587675548803736821383942932479326090814822654705161004900161974967463521550923723750395205531319794729419,
29 12938377744018684106919714662396630450474113273525805002450080987483731760775461861875197602770659897364740,
30 20673808572781675798140681050933939857653975971026885676579563321415667676572502551733296147274687516482797,
31 24541523987163171643751164245202594559447319777426013644304488381635634471022869662345419526701326041815,
32 122707619935815858218755821226012972797219536988713006821522441908178172355114883317270976350663020958,
33 6135380996790792910937791061300648639860976829944356503411076122095408908617755724165586354881675331510508,
34 3067690498395396455468895530650324319930488414972178251705538061047704454308877862082793177440837665755262,
35 15738464949970031974215271485060786790582163541750072301207291858197654023339210551837093934609776400678041,
36 7869232474980158620763574253039339529108177087503615060364592098827011669605275918546967304888200339052,
37 3934616237492507993103817871265196697645540885437518075301822964549413505834802637959273483652444100169549,
38 16171927819518587741232732655368222979439689776982742213005434309948508549102172939775334087715579617885231,
39 22290583610531627615297190047419736120336764222755354281857239982648056070735858090683364389747147376743001,
40 11145291805265813807684295902370986806016838211377677140928619991324028035367929045341682194873573688371553,
41 5572645902632906903824297511854934030084191055688838570464399655662014017683964522670841097436786844185758,
42 2786322951316453451912148755927467015042095527844419285232154997831007008841982261335420548718393422092919,
43 15597781176430560470636898097699358138137967098186192817970600326589305300605762751463407620248554278846905,
44 22003510288987613979999272768585303699685902883357079584339822990968454446487652996527401156013634707223862,
45 110017551444938609899963638429265184984295144167853979261699114954842272234238649826370057806817353611957,
46 19705497273019237239680641911881950555538395055103253071439478575415915407806684869927547634892766244606382,
47 9852748636509618619840320955940975277769197527551626535719739287707957703903342434963773817446383122303216,
48 492637418254809309920160477904876388845987637781326785988643853978851951671217481886980723191561151637,
49 24631731921740465496008023898524381944229383188790663329934821926989425975835608740943454361595780575816,
50 15436213280336036072160863839228246540338069025207936492319490238637296509172689425166169073070155458088331,
51 7718106640168018036080431919614123270169034512603968246159745119318648254586344712583084536535077729044184,
52 18063673020856342762721039679542686265701436590565967298434395387333125923477943977087239614156896432322558,
53 90318365104281713813605198397713431328507182958298364921719769366656296173897198854619807078448216161261,
54 18720537955986419435361083639621296197042278481905474999963121674507083277054257615067507249428581675881098,
55 23564888678765543462361365539546272729138058575216720675336083664927343434711900428329450970603648405740968,
56 25987064040155105475861506489508760995185948621872343513022564660137473513540721834960422831191181770670911,
57 27198151720849886482611576964490005128209893645200154931865805157742538552955132538275908761484948453135907,
58 27803695561197276985986612201980621194721866156864060641280641724254065450710726623773889933651726631831794368385,
59 13901847780598638492993306100990313597360933078432030320643712703272535536331168944966825863315915897184216,
60 6950923890299319246496653050495156798680466539216015160321856351636267768165584472483412931657957948592146,
61 3475461945149659623248326525247578399340233269608007580160928175818133884082792236241706456828978974296069,
62 159423506733471635563049869823594138302870359690798696543498691558286873822617738916550578803847054948475,
63 22175795037445915522833317210915331545760437318797976658072016285465236165297855490253972635291281095274640,
64 11087897518722957761416658605457665772880218659398988329036008142732618082648927745126986317645640547637370,
65 19748568460133812625389153022464457517057028663963477339872526899040110837509235493359190504712177841619096,
66 98742842300669063126945765112322287582851423869373866994634295200554187546173466795952535608820809593,
67 19141761815805786901028111975351739009881176500254852510322654552433829505562080494135494972067402028205248,
68 9570880907902893450514055987675869504940588250127426255161327276216914752781040247067747486033701014102596,
69 4785440453951446725257027993837934752470294125063713127580663638108457376390520123533873743016850507051301,
70 2392720226951263626851399691896737623514706253185663790331819054228688195260061766936871508425253526589,
71 1196360113487861681314256998459483688117573531265928281895165909527114344097630030883468435754212626762856,

```
72 598180056743930840657128499229741844058786765632964140947582954763557172048815015441734217877106313381469,
73 299090028371965420328564249614870922029393382816482070473791477381778586024407507720867108938553156690753,
74 149545014185982710164282124807435461014696691408241035236895738690889293012203753860433554469276578345381,
75 14279392207865325099762964782139342361124267679968103692972970697019246442690873497725914123123995856973136,
76 713969610393266254988148239106967118056213383998405184648648534850962322134543674886285970615619979262486597,
77 3569848051966331274940741195534835590281066919992025923243242674254811610672718374431478530780998964243287,
78 15989543726755499382151194317503042425757452794259996136976144164801207601521130808011436611279857049922087,
79 7994771863377749691075597158751521212878726397129998068488072082400603800760565404005718305639928524961050,
80 399738593168887484553779857937576060643936319805640240360412003019003802270200289152819964262480555,
81 1620331266661677116744972300942350493383660093356482692476540848273952746374912971797126922299339699040675,
82 8101656333308385583724861504711752466918300466773241346238270424136976373187456485898563461149669849520375,
83 405082816665419279186243075235587623345915023386620673119135212068488186593728242949281730574834924760191,
84 2025414083327096395931215376177938116729575116693310336559567606034244093296864121474640865287417462380136,
85 1012707041663548197965607688088969058364787558346655168279783803017122046648432060737320432643708731190067,
86 506353520831774098982803844044484529182393779173327584139891901508561023324216030368660216321854365595036,
87 14457796461188220794172225641757866895208116223850646967424468778428082307846879635980027454050284750597940,
88 7228898230594110397086112820878933447604058111925323483712234389214041153923439817990013727025142375298978,
```

```
1 pubkey2 += [
2 17819068816069388943223880130175091354418948390226644917210640022280822373146491529790704209401928755449908,
3 231141541088070282162927637848231703078263935293773056339598428388142129827580173856910494509321945525414,
4 11557077054403514108146381892411585153913196764688652816979921419407106491379008692845524725295160972762734,
5 5778538527201757054073190946205792576956598382344326408489960709703553245689504346422762362647580486381366,
6 17093888964373212271717419192838520919095218525436146379599503182525578419029523794007078527213147810991143,
7 8546944482186606135858709596419260459547609262718073189799751591262789209514761897003539263606573905495564,
8 18478091941865636812610178517945254860390723965623019770254398623305196400942152569297466977692644520548195,
9 23443665671705152150985912978708252060812281317075493060481722139326399996655847905444430834735679828074565,
10 25926452536624909820173780209089750661023059992801729705595383897337001794512695573517912763257197481837715,
11 12963226268312454910086890104544875330511529996400864852797691948668500897256347786758956381628598740918882,
12 20686232834928561199724268772008062295872684332464415601753368802008052244812945514175175536703656938259888,
13 24547736118236614344542958105739655778553261500496190976231207228677827918591244377883285114241186036930346,
14 12273868059118307172271479052869827889276630750248095488115603614338913959295622188941642557120593018465188,
15 61369340295591535861357395264349139446383153751240477440557801807169456979647811094470821278560296509232601,
16 172730867155519105377486934829530816029367702182607704738342373125832086008677168031107985169505822418723,
17 22841163058548289013555170461212165432084957845176986699046234693303066939189110204811251338474110479008813,
18 25625201230046478251458408950341707346659398256852476524877640174325335265779326723201323015126412807304862,
19 12812600615023239125729204475170853673329699128426238262438820087162667632889663361600661507563206403652408,
20 6406300307511619562864602237585426836664849564213119131219410043581333816444831680800330753781603201826220,
21 3203150153755809781432301118792713418332424782106559565609705021790666908222415840400165376890801600913116,
22 1601575076877904890716150559396356709166212391053279782804852510895333454111207920200082688445400800456593,
23 800787538438952445358075279698178354583106195526639891402426255447666727055603960100041344222700400228327,
24 14605013469991809967359861359584713807908472432027303121055735955397635159712573600845718018000707767914610,
25 21507126435768238756075439952798153457115550277637125550298308053726193760410584212855634889711451757748,
26 107535632178841193641803771997639907672855777513881736794119540268630968802052921060927817744855725878898,
27 5376781608942059682090188599881995383642788887569408683970597701343154844010264605304639088722427862939452,
28 16893010505243363585725918019676622322438313778048687517339821678345379218189903923448016890250571499270169,
29 226511249533940155375437827295739357938760762328832693402843366846491405279723582519705791014643317435491,
30 25530182177469341513452715084522592526534957445908146642366739661097047498824633412055550241396679226518211,
31 269697107895070045501407181261996920893884398057218056496537892658222325545597088326823472466587697181059521,
32 2768947509552583595384414350734085077559118362873011423623469156784964568983315784207433579183206158330185,
33 13844737947762917997692207175367042538779559181436505711811734578392482284491657889591603071735109,
34 21126988474653792743526927307419145900006698924982236031260390116870042938430600566847555740685159107382959,
35 10563494237326896371763463653709572950003349462491118015630195058435021469215300283423777870342579553691492,
36 5281747118663448185881731826854786475001674731245559007815097529217510734607650141711888935171289776845789,
37 16845493260104057837621689633163017868117756699886762679262071592282557163488596691651641813475002456223314,
38 226273663308243626634916685363171335646757976842073651498558623815080377929069966621581825262858795912100,
39 11313683165412181331745834268158566782337898842103682257492779311907540188964534983310759126313429397956057,
40 19861461283478424410553740853814908021785868755315824304100912483627571890667039112451076909046072266778463,
41 9930730641739212205276870426907454010892934377657912152050456241813785945333519556225538454523036133389248,
42 1916985021641939847319258933189351636063865723092939251379750948580694768851531398908466573150875634495046,
43 23789612211593303668340453186330300448648612595810452801044398301964149180610537320249930632464795385047977,
44 26099425806568985578851050312900774854941225632169209575876721978655876386490040280920662662121755260324415,
45 27254332604056826534106348876186012058087532150348587963292883817001739989429791761256028676950235197962663,
46 27831786002800747011733998157828630659660685409438277157000964736174671790899667501423711684364475166781780,
47 13915893001400373505866999078914315329830342704719138578500482368087335895449833750711855842182237583390870,
48 21162566201472520497614323259192782295532090686623552464604764011717469743909688496151625266980476359495850,
49 247859028015085939934879853493320157788296467757579407656904833532536668139615868871509997379595747548355,
50 12395251400754296996743992674666007889191942338787970382845241676626833406980793443575498968979787374213,
51 20401095401149482243052820057068628575212660503657923027268749036056935963219675588013574840734256504687551,
52 10200547700574741121526410028534314287606330251828961513634374518028467981609837794006787420367128252343809,
53 5100273850287370560763205014267157143803165125914480756817187259014233990804918897003393710183564126171882,
54 16754756625916019025062426226869203202518501897221223553763116457180918791587231069297394200981139630886391,
55 22581998013730343257120368331702262318761702828795495523608105624261191978387155443944646379927383243624,
56 11290999006865171628606018416585113115938085141437297476118040528132130595989193577722197223189963691621807,
57 564549950343258581430309208292556557969042570718648738059020264066065297994596788861098611594981845810950,
58 2822749751716292907151504604146278278984521285379432639029510132033032648997298394430549305797490922953469,
59 15615994576630480198256576021808763770109179976934645359869277893690318120832081801971998788103209253166,
60 7807997288315240099128288010904381885054589988471822679934638946845159060341710409005485999394051514626597
61 ]
62
63 ct2 = 2392102864029606341713283405820558372624777050411410395969738848933509252455825087540044061561675779855718270
64 print ("stage2")
65 t = abs (2*pubkey2[1]-pubkey2[0])
66 for i in range(-100, 100):
```

```

67 f = FactorDB(t+i)
68 #f = ecm.factor(t+i) 有点慢用factordb查...
69 f.connect()
70 if f.get_status() == "FF":
71     factlist = f.get_factor_list()
72     print(factlist)
73     p = factlist[0]
74     q = factlist[1]
75     c1 = ct2%p
76     c2 = ct2*q - q
77     pt = c1 - c2
78     print(hashlib.sh1(long_to_bytes(pt)).hexdigest())
79     if hashlib.sh1(long_to_bytes(pt)).hexdigest() == "2347411264fc395375fdfe3dbd6169283f3e4923":
80         print(p, q)
81         nonce2 = long_to_bytes(pt)
82         break
83 print(nonce1, nonce2)
84

```

Flag

1

- 本文作者: CTFHub
- 本文链接: <https://writeup.ctfhub.com/Challenge/2020/XCTF高校网络安全专题挑战赛/鲲鹏计算专场/Crypto/4Rm3MQzLJTKQZsqptdLu74.html>
- 版权声明: 本博客所有文章除特别声明外, 均采用 [BY-NC-SA](#) 许可协议。转载请注明出处!

[#Challenge #2020 #Crypto #XCTF高校网络安全专题挑战赛 # 鲲鹏计算专场
combinefsr
s34hunka](#)