

# BUUCTF Crypto RSA5 wp

原创

唏嘘的羊腰子 于 2020-03-15 14:48:56 发布 1154 收藏

分类专栏: [BUUCTF Crypto](#) 文章标签: [python](#) [安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/weixin\\_44017838/article/details/104878645](https://blog.csdn.net/weixin_44017838/article/details/104878645)

版权



[BUUCTF Crypto](#) 专栏收录该内容

29 篇文章 2 订阅

订阅专栏

## BUUCTF Crypto RSA5 wp

本题 $e$ 较大, 不建议使用中国剩余定理求解, 在不同的 $n$ 中试试寻找公因数求解

下面展示 `exp`代码。

```
// An highlighted block
from gmpy2 import *
n1 = 20474918894051778533305262345601880928088284471121823754049725354072477155873778848055073843345820697886641
0868426124865412501839659660015913420315629535617933323416413343028479961084174663606881398665051796895165893056
3690213721018562465085490678003720441220630994919908000557692277577372243886376211775042932758579209344742398000
2401200613302943834212820909269713876683465817369158585822294675056978970612202885426436071950214538262921077409
0761604174366998361388011626213148456087968702068347041167077631698473872233078289085709449844169730194275297900
29089766264949078038669523465243837675263858062854739083634207
c1 = 97446390824333086572897876921359540078205339859689774131627572259641501891292950863739385091922496927176638
8710025195039896961956062895570062146947736340342927974992616678893372744261954172873490878805483241196345881721
1640786511560671199578164227685244420256880794626567556059821041740016353458740221330454023440100459611117201519
904120344775585180276906930906901873854185413018369220475876142712127998200299393974534369567190001529679063746
4880337375511536424796890996526681200633086841036320395847725935744757993013352804650575068136129295591306569213
300156333650910795946800820067494143364885842896291126137320
n2 = 20918819960648891349438263046954902210959146407860980742165930253781318759285692492511475263234242002509419
0795456440517552513113926357634125534997445064215660747212688223373216372659422267903438398561821005755398453588
7749371833423758582126338818112654518972342926214963065128944655340219053113552083610421716026834968852516837521
3462570213612845898989694324269410202496871688649978370284661017399056903931840656757330859626183773396574056413
017367064465401999731556304662394536372329369040637065511606502950312733856194707405935102672859579058015663625
02262757750629162937373721291789527659531499435235261620309759
c2 = 15819636201971185538694880505120469332582151856714070824521803121848292387556864177196229718923770810072104
1554320386825114349793530897918610874151440878556791343833968978174587265438830935676003252045961566493059303525
752740394254708363550026911458644357553382113396926695154515805274593825257430132769682234711505361405242302883
5532509220641378760800693351542633860702225772638930501021571415907348128269681224178300248272689705308911282208
6854596682005070571834206629591139560775847817379832547887030482756989214270298842825574683343996778499623421961
40864403989162117738206246183665814938783122909930082802031855
n3 = 25033254625906757272369609119214202033162128625171246436639570615263949157363273213121556825878737923265290
57955187382437487095746716398954206348941663671365464248671721923122507411526968411942808635253547168333594862482
0364446146593550051790151323373915288294301017727654512830841293455583008777612835512593291484645947022110200766
6912211992310538890654396487111705385730502843589727289829692152177134753098649781412247065660637826282055169991
8240991109165768561888769756213766066342589277840257871422633671529471087207572224466864156274797036660318716356
56314282727051189190889008763055811680040315277078928068816491
c3 = 41853085294168740058312307810140924071984513859556773996685018339026234783956692794048839907251843327091524
```

4337258370107619878663529173935677085728670210715673002000435895562251106141066105898262205519973682080820384144  
6796305284394651714430918690389486920560834672316158146453183789412140939029029324756035358081754426645160033262  
9243302486752161082709801570497054886202634851294809528147640028652800191851276624493183242793832777664162581422  
7514392353216879841301102827154308524902904899745221250311174230230206540105145806658539536046844746065867295285  
1643547193822775218387853623453638025492389122204507555908862

n4 = 21206968097314131007183427944486801953583151151443627943113736996776787181111063957960698092696800555044199  
1567656779353731495982211847922868122132946177498346076963021161367456628166581170554278033152300427006951257184  
0164681048487306477500522108917405682472492216085581052723675138960501757954523587686499841987306521729482024473  
0785120525126565815560229001887622837549118168081685183371092395128598125004730268910276024806808565802081366898  
904032509920453785997056150497645234925288838794196421891096490091323815866733900276147666050389510158530867211  
68018787523459264932165046816881682774229243688581614306480751

c4 = 45210380110447584418911284684672330884938857508505889857085199111547780905971361261502890418934541266744681  
4139347266233735036171221269486731162297044070772794111326383235717314177585522797374257108897459347630208411177  
062576422283836627755956088704294885989213855147268065451781491660927974836558061071225985667740518477086531592  
2331071754700682919036075057994329319896637074770179046114262137702383970057437303860800319556941584665584755997  
519402450391676291265767840244823484528683134174715429567782855677943594026714067990668653186246762723840100345  
9101637191297209422470388121802536569761414457618258343550613

n5 = 22822039733049388110936778173014765663663303811791283234361230649775805923902173438553927805407463106104699  
7739941583757040330934717613877998521683378985269805217536143078996690159313878199274218753163045915219015928238  
1441775644769570104584677350862937139701305368455304218572505999679153239162642971241699499088969373280518194797  
0071429309599614973772736556299404246424791660679253884940021728846906344198854779191951739719342908761330661910  
477119933428550774242910420952496929605686154799487839923424336353744421535716780645207631497932943607878217517  
03543288696726923909670396821551053048035619499706391118145067

c5 = 15406498580761780108625891878008526815145372096234083936681442225155097299264808624358826686906535594853622  
6873792689694684330723881497866073953964241043188208794437431123587065467539352157560783459593752996507185557596  
9888785231801759750307431735674512251448180784374562642979786146301294017279761258903168671818539034538929585107  
5279278516147076602270178540690147808314172798987497259330037810328523464851895621851859027823681655934104713689  
5398480471630886668964736655001581790461965382107788977302095727084300676584117559598660335317004605515563809939  
82706171848970460224304996455600503982223448904878212849412357

n6 = 21574139855341432908474064784318462018475296809327285532337706940126942575349507668289214078026102682252713  
7577030815530931088232140637915184822898467801973298211395079747637802602903096008849208119598429255405839670856  
7084876531787744148091485232927637577640568978457140463585220409762260065622271480854187225233587703756138840625  
7181715278766652824786376262249274960467193961956690974853679795249158751078422296580367506219719738762159965958  
8778061874610706890712909481819495612541443107769433348597751216501862458460317205079449878384897231278972234168  
02436021278671237227993686791944711422345000479751187704426369

c6 = 20366856150710305124583065375297661819795242238376485264951185336996083744604593418983336285185491197426018  
5950314446521232884614918790210960282036941366832034416929870695635130260018614357221179855599096926709073475635  
9457826588080654039677722390695549102628684316863736759340034281472569436607833703093710403599356967295936134728  
789414302718684685677298305832891971670298222142848848117768499996617588305301483085428547267337070998767412540  
2259115081968422531343559012638611215006502402967467029675942244016502201687805371416544892150191421222843081162  
84129004257364769474080721001708734051264841350424152506027932

n7 = 25360227412666612490102161131174584819240931803196448481224305250583841439581008528535930814167338381983764  
9912965756372319165476479705737582694111682193023705416847891251125050211485068096430819502376237031810256965859  
9804469569132201218366042463649689707304555740076874594378734254826738656462546214315017611365626445021002392557  
1945961405709276631990731602198104287528528055650050486159837612279600415259486306154947514005408907590083747758  
953115486124865486720633820591350634409425280314029519585576308335037751120107156042781143255289937710812335352  
47118481765852273252404963430792898948219539473312462979849137

c7 = 19892772524651452341027595619482734356243435671592398172680379981502759695784087900669089919987705675899945  
6586486238000902725991545901230821896450218009580768615183973254395211399956520263771323682325021086200334000513  
4612775769862388614262179342322574924028651166655609178785168397801750698331007352439828727973768009178733354753  
8239920607761080988243639547570818363788673249582783015475682109984715293163137324439862838574460108793714172603  
672477668313564113044468819986747795011881636006644880329436396948286989847394922006996844627489228835500026529  
13518229322945040819064133350314536378694523704793396169065179

n8 = 22726855244632356029159691753451822163331519237547639938779517751496498713174588935566576167329576494790219  
3607278771660741364961299272962969969700480828704888044565649866671293881365561370133462281189819368995106875895

8528651715132304829315025703684747542404437810916817941228788934059639475525770493800616267765658150937547110254  
6261355748251869048003600520034656264521931808651038524134185732929570384705918563982065684145766427962502261522  
4819941919898201105759819069984315531075255420011876557035346832317779884192683382495476413357183933122958000447  
34534761692799403469497954062897856299031257454735945867491191

c8 = 60401197951758564075410823600235322046147238586886367248227127175727597939602463418003081497398098712343130  
4962973293479756978105300068618566637483397840329052507259877400173135024474459077279570106512956189811657649998  
4185920661271123665356132719193665474235596884239108030605882777868856122378222681140570519180321286976947154042  
2726224113039810113025862256308598927317246405746581254782871151984062538473679798837680008126053954829526986896  
0447771947894759544218592148065263786833567323320066210062102506150089572960530566586469312295255736187152316530  
0206070325660353095592778037767395360329231331322823610060006

n9 = 23297333791443053297363000786835336095252290818461950054542658327484507406594632785712767459958917943095522  
5942282054234282073451288997458009273191472576697738126695427828392377443051800982765788419294963459639975122442  
1937670178761604623539713938189483743556266259106076847699733353874806529403314161050225232529280181681226893417  
1361934399951548627267791401089703937389012586581080223313060159456238857080740699528666411303029934807011214953  
9841697858447141596277920169264909552826978771416146388063976893067953283447784786920847542167534258425578188994  
67945102646776342655167655384224860504086083147841252232760941

c9 = 54181203012083787131158894655799642578718141145150460960909601597378590768292585169203615778539039259541984  
068437573036875578483023022022929591690243020573784360180670073823475669857570861242492848044086873912007588868  
1672062206529156566421276611107802917418993625029690627196813830326369874249777619239603300605876865967515719079  
7971159105786535627878990193101399459049580248824178337363048947654334894762345753567552751472565773870228733489  
0690014963494074710451385015411810699113707264330862028466310828305224575094522899538780343212884215225154929269  
8947407663643895853432650029352092018372834457054271102816934

n10 = 2887366790471568272298723429349320030697694789871125506412511593366696867874259885872243142621891446290352  
1596341771131695619382266194233561677824357379805303885993804266436810606263022097900266975250431575654686915049  
6930914678648205127670707132677089938998990111561067661789067003361117128033621130396135486729370533978756631447  
9401808701773194908779489490373768238391617326742140340814096771307102600187473348729500750106887104464917061570  
9891451856792232315526696220161842742664778581287321318748202431466508948902745314372299799561625186955234673012  
098210919745879882268512656931714326782335211089576897310591491

c10 = 9919880463786836684987957979091527477471444996392375244075527841865509160181666543016317634963512437510324  
1987024163228413774894170295723884744500758014629968252446575302861074281863541728367165028176090705909297692619  
3232427535328993930253644031062869834924487206400570064452022372767095078792429600429688303297894120088336265399  
3351638545860207179022472492671256630427228461852668118035317021428675954874947015197745916918197725121122236369  
3827415339830234622559139246928062493874490166298658233164023660176578441669198466834978518423880582838562199005  
35567427103603869955066193425501385255322097901531402103883869

n11 = 2232468594753965372249993246940960753306541915734781396195807568904769046526640438419948368390859478731244  
5528159635527833904475801890381455653807265501217328757871352731293000303438205315816792663917579066674842307743  
8452617710323639285688446698957680925156583287562292458370252617442606148607469979315035487885099838680383497202  
2530573098557629367526907370902235070083651005406764175371321299995430702252449588558336170737851374216256633901  
0134354907863733205921845038918224463903789841881400814074587261720283879760122070901466517118265422863420376921  
536734845502100251460872499122236686832189549698020737176683019

c11 = 149152705020329498988282924856039518480497727747126143103957219164624187528441047837351263580440686474767  
3804640055402646279101264831299306683440958145475921150610578434701314980750604203951110086190271990370199257012  
366601665630682456839757877628043595201647016916909164825910261385827055824686949616275978087843713796082300004  
398822730300387641050312137016330371160335943076453933759786862508451528158285103251810058741879687875218384160  
2825061727066133594776572154207348160493933395937554892185887966070602618979052334532686714116106310473404594879  
37479511933450369462213795738933019001471803157607791738538467

n12 = 2764674642375902011100782865326402799925784764566612990778902605459439364880023611704676911276264177886562  
0892443423100189619327585811384883515424918752749559627553637785037359639801125213256163008431942593727931931898  
199727552768626775618479833029101249692573716030706695702510982283555740851047022672485743432464647728823142151  
7611473225749724028416401691401868904455721892030026223465284063240606727337526930100840986019318082236673587728  
8205783314326102263756503786736122321348320031950012144905869556204017430593656052867939493633163499580242224763  
404338807022510136217187779084917996171602737036564991036724299

c12 = 2199152412895726053604377128485492039310580812670012822212585677550688572197119310936131596112919081467464  
7136464887087893990660894961612838205086401018885457667488911898654270235561980111174603323721280911197488286585  
2693568495792630434563163194764958886962193442198665168611876541805092478812512512789193462671299047392773862892

4039438457512433113565594351383100993402339745708218469973773438882376330680532643039584993577021381753338723548  
6307008892410920611669932693018165569417445885810825749609388627231235840912644654685819620931663346297596334834  
498661789016450371769203650109994771872404185770230172934013971

n13 = 2054548740581692873173898837447501268682793370978978439185570683513627027093340120301932913693765087838611  
7187776530639342572123237188053978622697282521473917978282830432161153221216194169879669541998840691383025487220  
8508720754360643084999249585179797279544029656121960814043416515173263640415192501250364248226343542687738954656  
989208834392229965812263585958739939766046998306139323207205413001167129794443351504718056548449519100388759989  
1289037982010216357831078328159028953222056918189365840711588671093333013117454034313622855082795813122338562446  
223041211192277089225078324682108033843023903550172891959673551

c13 = 1422743918819102946125047669279053965461919988848731942911441455797537630868890802814081715720557980405978  
3807641305577385724758530138514972962209062230576107406142402603484375626077345190883094097636019771377866339531  
5119651366505674123638891831596161884492637524753286632453110599883379960473592632888374363055888480445729377594  
2446658687028051242433680706472989451584055240475687959069879704633333644546512044508758762174390662427962177963  
477237880295910971440051618371832326727382473654016854594644437586299214110424738159957388350785999348535171553  
569373088251552712391288365295267665691357719616011613628772175

n14 = 2735972771158427723489715772405585279401921684522979893865581426946004638435356813859856775539255965346094  
9444557879120040796798142218939251844762461270251672399546774067275348291003962551964648742053215424620256999345  
4483988052785927770496682815583128717739799313430978068787011140560300415066904769542540065925552753425795296252  
3119432135790466851212153951488070404696997489841209567508258531545826759101673492464629435766692429390841834550  
8902112711075232047998775303603175363964055048589769318562104883659754974955561725694779754279606726358588862479  
198815999276839234952142017210593887371950645418417355912567987

c14 = 378852978424825502708167454087701637280784822276887920453488878247137930578296797437647922494510483767651  
1504929333560932889659437415702689438619870242766107127174091399464095139630431144639331460884300042377471634228  
0295925029660257064936301615158136400679589422659958470807258269699674051888760678546077585102981428035938576309  
1078902301957226484620428513604630585131511167015763190591225884202772840456563643159507805711004113901417503751  
1810508236382078035331114295109116161608513917547544347648195680548508238109011598212978497900056461021293540357  
35350124476838786661542089045509656910348676742844957008857457

n15 = 2754593760375173724878522089173579646897332973807620914407992144996729257234942453901050228756403011683126  
1268197384650511043068738911429169730640135947800885987171539267214611907687570587001933829208655100828045651391  
6180896032884565703345005331786952384076847022512526715793710186516750543686062825246733699830346823305783087698  
8645633581873382723729457047685367355268536168914426155289575826652239300411601784939734625911922106382166328093  
5820440671825601452417487330105280889520007917979115568067161590058277418371493228631232457972494285014767469893  
647892888681433965857496916110704944758070268626897045014782837

c15 = 1406911297060889573241703997754273266579660189376240150087878687168064579875478331569351126174005972517134  
2404186571066972546332813667711135661176659424619936101038903439144294886379322591635766682645179888058617577572  
4093074847081711444887084105434629720081799945940874739356380266126793897597568114905241271956287412628713044279  
0848121499247118285930882877811900575092893576492796721234352650341051579371720136036043798132257679805627665714  
0363332700714732224848346808963992302409037706094588964170239521193589470070839790404597252990818583717869140229  
811712295005710540476356743378906642267045723633874011649259842

n16 = 2574616207569791156026318179121643306257417857242460033685627817611273305443146325390343312823270905414160  
7100891177804285813783247735063753406524678030561284491481221681954564804141454666928657549670266775659862814924  
3865841487854536473168649359427729191405635063056662078168976018627130928092344290965847532637078288997809792231  
1818100929365556314652679238891346255730643366429696633146990642866512743882939970300286780026994785586926203671  
4256550075520193125987011945192273531732276641728008406855871598678936585324782438668746810516660152018244253008  
092470066555687277138937298747951929576231036251316270602513451

c16 = 1734428486027548947749152581992285532679227512871970940129254560812285982982746208839004461223496755168287  
9954301458425842831995513832410355328065562098763660326163262033200347338773439095709944202252494552172589503915  
965931524326523663289775831526647222419208005378673310306239066740818522962323063362715428327284108036311702296  
4271752494233239084246703514363150440114072708327073246423744391526386588058030877611121971896174637884292464414  
2127243573824972533819479079381023103585862099063382129757560124074676150622288706094110075567706403442920696472  
627797607697962873026112240527498308535903232663939028587036724

n17 = 2328848693411712031503691941858813622702848549413793019632371533620884932783396569389467056721797172792124  
3839129969128783853015760155446770590696037582684845937132790047363216362087277861336964760890214059732779383020  
3492048032057258702254299859395701415082200412868578100481646967070186637584168077089106714774073660988834308118  
6193301497340930017994857771257974935229944031054368903565146539986790842888554123777614340437633344294939706324

```
9223702355051571790555151203866821867908531733788784978667478707672984539512431549558672467752712004519300318999
208102076732501412589104904734983789895358753664077486894529499
c17 = 1073825441811407654807144884496404646814162174060321438498635418910523697707100142927156063642807597045989
0958274941762528116445171161040040833357876134689749846940052619392750394683504816081193432350669452446113285638
9825517625866563291090072140199449758164348277688827046304600012094522391628965761918763246623331538355339566002
9525515837702519842695094404064323543021101106358603246772432973578594737205175904213817105416585484247299058380
0899984893232549092766400510300083585513014171220423103452292891496141806956300396540682381668367564569427813092
064053993103537635994311143010708814851867239706492577203899024

n18 = 1959144138395852943559872911393634665700135257835790934765725723977754042481174981778306123323581791656068
9138344041497732749011519736303038986277394036718790971374656832741054547056417771501234494768509780369075443550
9078472982462757174205623751144060557336202587779052221697020364940450860173810842724961627702599558111744404901
2651474787666131775064948877499234800504438908110168601644621926406997137064631954642978290481006302032470413849
5608761532563310699753322444871060383693044481932265801505819646998535192083036872551683405766123968487907648980
900712118052346174533513978009131757167547595857552370586353973
c18 = 3834917098887202931981968704659119341624432294759361919553937551053499607440333234018189141970246302299385
7425482785898960332828949812003532706371272134831721825298904959034256491167559016311016658763017998656127177503
6008908517914275066460345419364205301638471451585586836872350892227176719028552113778568807562283292482924836277
4476456232826885801046969384519549385428259591566716890844604696258783639390854153039329480726205147199247183621
5351724508259790471324954396038408065012549971670511424271573817998907253237655588038080301094680486822520287202
41357478614704610089120810367192414352034177484688502364022887

n19 = 1925424257158843017130819175787126107535852115862474570274405755605465233249596119679536963048478293029200
3238730267396462491733557715379956969694238267908985251699834707734400775311452868924330866502429576951934279223
2346766547492729327691073909763212086055162995325600540813018294406887969046354469860816911568422712680599707620
0425921903675317490994234320443279507637743210763020362175455280412440879235822007186236944320158415571189338887
7350138023238624566616551246804054720492816226651467017802504094070614892556444425915920269485861799532473383304
622064493223627552558344088839860178294589481899206318863310603
c19 = 6790553533991297205804561991225493105312398825187682250780197510784765226429663284220400480563039341938599
7833467240510762112656634686438264301090132450140358111782950819399586870874773128677202899645060978197620952444
7912935999886767181181973819668788469668046345866137431099461076000947426411575020492087552743448643753662358968
4519411519100170291423367424938566820315486507444202022408003879118465761273916755290898112991525546114191064022
9913297243700646325699038561892361778940077666907826302474438953588939837358228242434871818510987872712702567808
91094405121947631088729917398317652320497765101790132679171889

n20 = 2680970025117127910297496294918441113645937226762053519842144983329844809258049748530195379661918533931606
4387798092220298630428207556482805739803420279056191194360049651767412572609187680508073074653291350998253938793
2692142304571171944348538887653034033858247862318594503512124494048707763202974197124865748047943256027603473064
3292728171616036883018794494012890797102783851007951946684617610656516473096398889240024006308939772041492139893
6399927948235195085202171264728816184532651138221862240969655185596628285814057082448321749567943946273776184657
698104465062749244327092588237927996419620170254423837876806659
c20 = 3862135566084340137698647271238794120419912715289905285485074512106926189866528704246322194246016775242650
1104314674830977406789498506928806795254613941681940403968845475604486278463088283349609082256858057285902980064
6671301748901528132153712913301179254879877441322285914544974519727307311002330350534857867516466612474769753577
8586600758305928914035518672460573978396883291725301771870422290286858620361407790657710619335281374230194073114
7358183240589908970925174700278803200209449537961468654467296907324930970348255638602462281473101576781004296981
3752548617464974915714425595351940266077021672409858645427346

n=[n1, n2, n3, n4, n5, n6, n7, n8, n9, n10, n11, n12, n13, n14, n15, n16, n17, n18, n19, n20]
c=[c1, c2, c3, c4, c5, c6, c7, c8, c9, c10, c11, c12, c13, c14, c15, c16, c17, c18, c19, c20]
for i in range(len(n)):
    for j in range(len(n)):
        if(i!=j):
            if(gcd(n[i],n[j])!=1):
                print(i+1, j+1)
                print(gcd(n[i],n[j]))
#(5, 18)
#132585806383798600305426957307612567604223562626764190211333136246643723811046149337852966828729052476725552361
1324373705215487076649771231652793050529718680127555091604086411005487440466215168779818641800764975240932014045
58036301820216274968638825245150755772559259575544101918590311068466601618472464832499
```

```
p=mpz(1325858063837986003054269573076125676042235626267641902113331362466437238110461493378529668287290524767255
5236113243737052154870766497712316527930505297186801275550916040864110054874404662151687798186418007649752409320
1404558036301820216274968638825245150755772559259575544101918590311068466601618472464832499)
q=n5/p
phi=(p-1)*(q-1)      #求欧拉函数
e=65537
d=invert(e,phi)      #求逆元
m=pow(c5,d,n5)
print(hex(m)[2:].decode('hex'))
#flag{abdcbe5fd94e23b3de429223ab9c2fdf}
```