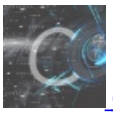
BUUCTF RSA5浅析

原创

贮藏的仓鼠 于 2019-11-19 10:45:57 发布 1966 收藏 4

分类专栏： CTF 文章标签： RSA CTF

本文链接：https://blog.csdn.net/qq_42391153/article/details/103135502



RSA5

这道题看起来很麻烦，实际上是一道比较简单的题

```
m = xxxxxxxx
e = 65537

m=pow(c,d,n)
========== n c ==========
n = 20474918894051778533305262345601880928088284471121823754049725354072477155873778848055073843345820697886641086842612486541250183965966001591342031562953561793332341641334302847996108417466360688139866505179689516589305636902137210185624650854906780037204412206309949199080005576922775773722438863762117750429327585792093447423980002401200613302943834212820909269713876683465817369158585822294675056978970612202885426436071950214538262921077409076160417436699836138801162621314845608796870206834704116707763169847387223307828908570944984416973019427529790029089766264949078038669523465243837675263858062854739083634207
c = 97446390824333086572897876921359540078205339859689774131627572259641501891292950863739385091922496927176638871002519503989696195606289557006214694773634034292797499261667889337274426195417287349087880548324119634588172116407865115606711995781642276852444202568807946265675560598210417400163534587402213304540234401004596111172015199041203447775585180276906930906901873854185413018369220475876142712127998200299393974534369567190001529679063746488033737551153642479689099652668120063308684103632039584772593574475799301335280465057506813612929559130656921330015633365091079594680082006749414336488584289629112613732 0

n = 20918819960648891349438263046954902210959146407860980742165930253781318759285692492511475263234242002509419079545644051755251311392635763412553499744506421566074721268822337321637265942226790343839856182100575539845358877493718334237585821263388181126545189723429262149630651289446553402190531135520836104217160268349688525168375213462570213612845898989694324269410202496871688649978370284661017399056903931840656757330859626183773396574054013017367606446540199973155630466239453637232936904063706551160650295031273385619470740593510267285957905801566362502262757750629162937373721291789527659531499435235261620309759
c = 15819636201971185538694880505120469332582151856714070824521803121848292387556864177196229718923770810072104155432038682511434979353089791861087415144087855679134383396897817458726543883093567600325204596156649305930352575274039425470836355002691145864435755333821133969266951545158052745938252574301327696822347115053614052423028835532509220641378760800693351542633860702225772638930501021571415907348128269681224178300248272689705308911282208685459668200507057183420662959113956077584781737983254788703048275698921427029884282557468334399677849962342196140864403989162117738206246183665814938783122909930082802031855

n = 25033254625906757272369609119214202033162128625171246436639570615263949157363273213121556825878737923265290579551873824374870957467163989542063489416636713654642486717219231225074115269684119428086352535471683359486248203644461465935500517901513233739152882943010177276545128308412934555830087776128355125932914846459470221102007666912211992310538890654396487111705385730502843589727289829692152177134753098649781412247065660637826282055169991824099110916576856188876975621376606634258927784025787142263367152947108720757222446686415627479703666031871635656314282727051189190889008763055811680040315277078928068816491
```

```
c = 4185308529416874005831230781014092407198451385955677399668501833902623478395669279404883990725184332709152443372583701076198786635291739356770857286702107156730020004358955622511061410661058982622055199736820808203841446796305284394651714430918690389486920560834672316158146453183789412140939029029324756035358081754426645160033262924330248675216108270980157049705488620263485129480952814764002865280019185127662449318324279383277766416258142275143923532168798413011028271543085249029048997452212503111742302302065401051458066585395360468447460658672952851643547193822775218387853623453638025492389122204507555908862

n = 2120696809731413100718342794448680195358315115144362794311373699677678718111106395796069809269680055504419915676567793537314959822118479228681221329461774983460769630211613674566281665811705542780331523004270069512571840164681048487306477500522108917405682472492216085581052723675138960501757954523587686499841987306521729482024473078512052512656581556022900188762283754911816808168518337109239512859812500473026891027602480680856580208136689890403250992045378599705615049764523492552888387941964218910964900913238158667339002761476660503895101585308672116801878752345926493216504681688168277422924368858161430648075 1
c = 4521038011044758441891128468467233088493885750850588985708519911154778090597136126150289041893454126674468141393472662337350361712212694867311622970440707727941113263832357173141775855227973742571088974593476302084111770625764222838366277559560887042948859892138551472680654517814916609279748365580610712259856677740518477086531592233107175470068291903607505799432931989663707477017904611426213770238397005743730386080031955694158466558475599751940245039167629126576784024482348452868313417471542956778285567779435940267140679906686531862467627238401003459101637191297209422470388121802536569761414457618258343550613

n = 2282203973304938811093677817301476566366330381179128323436123064977580592390217343855392780540746310610469977399415837570403309347176138779985216833789852698052175361430789966901593138781992742187531630459152190159282381441775644769570104584677350862937139701305368455304218572505999679153239162642971241699499088969373280518194797007142930959961497377273655629940424642479166067925388494002172884690634419885477919195173971934290876133066191047711993342855077424291042095249692960568615479948783992342433635374744215357167806452076314979329436078782175170354328869672692390967039682155105304803561949970639111814506 7
c = 1540649858076178010862589187800852681514537209623408393668144222515509729926480862435882668690653559485362268737926898694684330723881497866073953964241043188208794437431123587065467539352157560783459593752996507185557596988878523180175975030743173567451225144818078437456264297978614630129401727976125890316867181853903453892958510752792785161470766022701785406901478083141727989874972593300378103285234648518956218518590278236816559341047136895398480471630886668964736655001581790461965382107788977302095727084300676584117559598660335317004605515563809939827061718489704602243049964556005039822234489048782128494123 57
n = 2157413985534143290847406478431846201847529680932728553233770694012694257534950766828921407802610268225271375770308155309310882321406379151848228984678019732982113950797476378026029030960088492081195984292554058396708567084876531787744148091485232927637577640568978457140463585220409762260065622271480854187225233587703756138840625718171527876665282478637626224927496046719396195669097485367979524915875107842229658036750621971973876215996595887780618746107068907129094818194956125414431077694333485977512165018624584603172050794498783848972312789722341680243602127867123722799368679194471142234500047975118770442636 9
c = 2036685615071030512458306537529766181979524223837648526495118533699608374460459341898333628518549119742601859503144465212328846149187902109602820369413668320344169298706956351302600186143572211798555990969267090734756359457826588080654039677722390695549102628684316863736759340034281472569436607833703093710403599356967295936134728789414302718684685677298305832891971670298222142848848117768499996617588305301483085428547267337070998767412540225911508196842253134355901263861121500650240296746702967594224401650220168780537141654489215019142122284308116284129004257364769474080721001708734051264841350424152506027932

n = 2536022741266661249010216113117458481924093180319644848122430525058384143958100852853593081416733838198376499129657563723191654764797057375826941116821930237054168478912511250502114850680964308195023762370318102569658599804469569132201218366042463649689707304555740076874594378734254826738656462546214315017611365626445021002392557194596140570927663199073160219810428752852805565005048615983761227960041525948630615494751400540890759008374775895311548612486548672063382055913506344094252803140295195855763083350377511201071560427811432552899377108123353524711848176585227325240496343079289894821953947331246297984913 7
c = 1989277252465145234102759561948273435624343567159239817268037998150275969578408790066908991998770567589994565864862380009027259915459012308218964502180095807686151839732543952113999565202637713236823250210862003340005134612775769862388614262179342322574924028651166655609178785168397801750698331007352439828727973768009178733354753823992060776108098824363954757081836378867324958278301547568210998471529316313732443986283857446010879371417260367247776683135641130444688199867477950118816360066448803294363969482869898473949220069968446274892288355000265291351822932294504081906413335031453637869452370479339616906517 9
```

```
n = 2272685524463235602915969175345182216333151923754763993877951775149649871317458893556657616732957649479021936072787716607413649612992729629699697004808287048880445656498666712938813655613701334622811898193689951068758958
528651715132304829315025703684747542404437810916817941228788934059639475525770493800616267765658150937547110254
6261355748251869048003600520034656264521931808651038524134185732929570384705918563982065684145766427962502261522
4819941919898201105759819069984315531075255420011876557035346832317779884192683382495476413357183933122958000447
3453476169279940346949795406289785629903125745473594586749119 1
c = 6040119795175856407541082360023532204614723858688636724822712717572759793960246341800308149739809871234313049629732934797569781053000686185666374833978403290525072598774001731350244744590772795701065129561898116576499984
185920661271123665356132719193665474235596884239108030605882777868856122378222681140570519180321286976947154042
2726224113039810113025862256308598927317246405746581254782871151984062538473679798837680008126053954829526986896
0447771947894759544218592148065263786833567323320066210062102506150089572960530566586469312295255736187152316530
0206070325660353095592778037767395360329231331322823610060006
```

```
n = 2329733379144305329736300078683533609525229081846195005454265832748450740659463278571276745995891794309552259422820542342820734512889974580092731914725766977381266954278283923774430518009827657884192949634596399751224421
9376701787616046235397139381894837435562662591060768476997333538748065294033141610502252325292801816812268934171
3619343999515486272677914010897039373890125865810802233130601594562388570807406995286664113030299348070112149539
8416978584471415962779201692649095528269787771416146388063976893067953283447784786920847542167534258425578188994 6
7945102646776342655167655384224860504086083147841252232760941
c = 5418120301208378713115889465579964257871814114515046096090960159737859076829258516920361577853903925954198406843757303687557848302302200229295916902430205737843601806700738234756698575708612424928480440868739120075888681
6720622065291565664212766111078029174189936250296906271968138303263698742497776192396033006058768659675157190797
9711591057865356278789901931013994590495802488241783373630489476543348947623457535675527514725657738702287334890
6900149634940747104513850154118106991137072643308620284663108283052245750945228995387803432128842152251549292698
9474076636438958534326500293520920183728344570542711028169 34
```

```
n = 2887366790471568272298723429349320030697694789871125506412511593366696867874259885872243142621891446290352159634177113169561938226619423356167782435737980530388599380426643681060626302209790026697525043157565468691504969
3091467864820512767070713267708993899899011156106766178906700336111712803362113039613548672937053397875663144794
0180870177319490877948949037376823839161732674214034081409677130710260018747334872950075010688710446491706157098
9145185679223231552669622016184274266477858128732131874820243146650894890274531437229979956162518695523467301209
8210919745879882268512656931714326782335211089576897310591491
c = 9919880463786836684987957979091527477471444996392375244075527841865509160181666543016317634963512437510324198702416322841377489417029572388474450075801462996825244657530286107428186354172836716502817609070590929769261932
3242753532899393025364403106286983492448720640057006445202237276709507879242960042968830329789412008833626539933
5163854586020717902247249267125663042722846185266811803531702142867595487494701519774591691819772512112223636938
2741533983023462255913924692806249387449016629865823316402366017657844166919846683497851842388058283856219900535
5674271036038699550661934255013852553220979015314021038838 69
```

```
n = 2232468594753965372249993246940960753306541915734781396195807568904769046526640438419948368390859478731244552815963552783390447580189038145565380726550121732875787135273129300030343820531581679266391757906667484230774384
5261771032363928568844669895768092515658328756229245837025261744260614860746997931503548788509983868038349720225
3057309855762936752690737090223507008365100540676417537132129999543070225244958855833617073785137421625663390101
3435490786373320592184503891822446390378984188140081407458726172028387976012207090146651711826542286342037692153
6734845502100251460872499122236686832189549698020737176683019
c = 1491527050203294989882829248560395184804977277747126143103957219164624187528441047837351263580440686474767380464005540264627910126483129930668344095814547592115061057843470131498075060420395111008619027199037019925701236
6601665630682456839757877628043595201647016916909164825910261385827055582468694961627597808784371379608230000439
8822730300387641050312137016330371160335943076453933759786686250845152815828510325181005874187968787521838416028
2506172706613359477657215420734816049393339593755489218588796607060261897905233453268671411161063104734045948793 7
4795119334503694622137957389330190014718031576077917385384 67
```

```
n = 2764674642375902011100782865326402799925784764566612990778902605459439364880023611704676911276264177886562089244342310018961932758581138488351542491875274955962755363778503735963980112521325616300843194259372793193189819
9727552768626775618479833029101249692573716030706695702510982283555740851047022672485743432464647772882314215176
1147322574972402841640169140186890445572189203002622346528406324060672733752693010084098601931808223667358772882
0578331432610226375650378673612232134832003195001214490586955620401743059365605286793949363316349958024222476340
4338807022510136217187779084917996171602737036564991036724299
c = 2199152412895726053604377128485492039310580812670012822212585677550688572197119310936131596112919081467464 71
```

```
364648870878939906608949616128382050864010188854576674889118986542702355619801111746033237212809111974882865852693568495792630434563163194764958886962193442198665168611876541805092478812512512789193462671299047392773862892403943845751243311356559435138310099340233974570821846997377343888237633068053264303958499357702138175333872354863070088924109206116699326930181655694174458858108257496093886272312358409126446546858196209316633462975963348344986617890164503717692036501099947718724041857702301729340139713
n = 205454874058169287317389883744750126868279337097897843918557068351362702709334012030193291369376508783861171877765306393425721232718805397862269728252147391797828283043216115322121619416987966954199884069138302548722085087207543606430849992495851797972795440296561219608140434165151732636404151925012503642482263435426877389546569892088343922299658122635859587399397660469983061393232072055413001167129794443351504718056548449519100388759989128903798201021635783107832815902895322205691818936584071158867109333301311745403431362285508279581312233856244622304121119227708922507832468210803384302390355017289195967355 1
c = 142274391881910294612504766927905396546191998884873194291144145579753763086889080281408171572055798040597838076413055773857247585301385149729622090622305761074061424026034843756260773451908830940976360197713778663395315119651366505674123638891831596161884492637524753286632453110599883379960473592632888374363055888480445729377594244665868702805124243368070647298945158405524047568795906987970463333364454651204450875876217439066242796217796347723788029591097144005161837183232672738247365401685459464444375862992141104247381599573883507859993485351715535693730882515527123912883652952676656913577196160116136287721 75

n = 273597277115842772348971577240558527940192168452297989386558142694600463843535681385985677553925596534609494445578791200407967981422189392518447624612702516723995467740672753482910039625519646487420532154246202569993454483988052785927770496682815583128717739799313430978068787011140560300415066904769542540065925552753425795296252311943213579046685121215395148807040469699748984120956750825853154582675910167349246462943576669242939084183455089021127110752320479987753036031753639640550485897693185621048836597549749555617256947797542796067263585888624791988159992768392349521420172105938873719506454184173559125679 87
c = 378852978424825502708167454087701637280784822277688792045348887824713793057829679743764792249451048376765115049293335609328896594374157026894386198702427661071271740913994640951396304311446393314608843000423774716342280295925029660257064936301615158136400679589422659958470807258269699674051888760678546077585102981428035938576309107890230195722648462042851360463058513151116701576319059122588420277284045656364315950780571100411390141750375118105082363820780353311142951091161616085139175475443476481956805485082381090115982129784979000564610212935403573535012447683878666154208904550965691034867674284495700885745 7
n = 275459376037517372487852208917357964689733297380762091440799214499672925723494245390105022875640301168312612681973846505110430687389114291697306401359478008859871715392672146119076875705870019338292086551008280456513916180896032884565703345005331786952384076847022512526715793710186516750543686062825246733698303468233057830876988645633581873382723729457047685367355268536168914426155289575826652239300411601784939734625911922106382166328093582044067182560145241748733010528088952000791797911556806716159005827741837149322863123245797249428501476746989364789288868143396585749691611070494475807026862689704501478283 7
c = 140691129706088957324170399775427326657966018937624015008787868716806457987547833156935112617400597251713424041865710669725463328136677111356611766594246199361010389034391442948863793225916357666826451798880586175775724093074847081711444887084105434629720081799945940874739356380266126793897597568114905241271956287412628713044279084812149924711828593088287781190057509289357649279672123435265034105157937172013603604379813225767980562766571403633327007147322248483468089639923024090377060945889641702395211935894700708397904045972529908185837178691402298117122950057105404763567433789066422670457236338740116492598 42
n = 257461620756979115602631817912164330625741785724246003368562781761127330544314632539034331282327090541416071008911778042858137832477350637534065246780305612844914812216819545648041414546669286575496702667756598628149243865841487854536473168649359427729191405635063056662078168976018627130928092344290965847532637078288997809792231181810092936555631465267923889134625573064336642969633146990642866512743882939970300286780026994785586926203671425655007552019312598701194519227353173227664172800840685587159867893658532478243866874681051666015201824425300809247006655568727713893729874795192957623103625131627060251345 1
c = 173442848602754894774915258199228553267922751287197094012925456081228598298274620883900446122349675516828799543014584258428319955138324103553280655620987636603261632620332003473387734390957099442022524945521725895039159659315243265236632897775831526647222419208005378673310306239066740818522962323063362715428327284108036311702296427175249423323908424670351436315044011407270832707324642374439152638658805803087761112197189617463788429246441421272435738249725338194790793810231035858620990633821297575601240746761506222887060941100755677064034429206964726277976076979628730261122405274983085359032326639390285870367 24
n = 232884869341171203150369194185881362270284854941379301963237153362088493278339656938946705672179717279212438391299691287838530157601554467705906960375826848459371327900473632163620872778613369647608902140597327793830203 4
```

```
92048032057258702254299859395701415082200412868578100481646967070186637584168077089106714774073660988834308118619330149734093901799485777125797493522994403105436890356514653998679084288855412377761434043763334429493970632492237023550515717905551512038668218679085317337887849786674787076729845395124315495586724677527120045193003189992081020767325014125891049047349837898953587536640774868945294990
c = 107382544181140765480714488449640464681416217406032143849863541891052369770710014292715606364280759704598909582749417625281164451711610400408333578761346897498469400526193927503946835048160811934323506694524461132856389825517625866563291090072140199449758164348277688827046304600012094522391628965761918763246623331538355339566002952551583770251984269509440406432354302110110635860324677243297357859473720517590421381710541658548424729905838008999848932325490927664005103000835855130141712204231034522928914961418069563003965406823816683675645694278130920640539931035376359943111430107088148518672397064925772038990240
n = 195914413839585294355987291139363466570013525783579093476572572397775404248117498177830612332358179165606891383440414977327490115197363030389862773940367187909713746568327410545470564177715012344947685097803690754435509078472982462757174205623751144060557336202587779052221697020364940450860173810842724961627702599558111744404901265147478766613177506494887749923480050443890811016860164462192640699713706463195464297829048100630203247041384956087615325633106997533224448710603836930444819322658015058196469985351920830368725516834057661239684879076489809007121180523461745335139780091317571675475958575523705863539732
c = 383491709888720293198196870465911934162443229475936191955393755105349960744033323401818914197024630229938574254827858989603328289498120035327063712721348317218252989049590342564911675590163110166587630179986561271775036008908517914275066460345419364205301638471451585586836872350892227176719028552113778568807562283292482924836277447645623282688580104696938451954938542825959156671689084460469625878363939085415303932948072620514719924718362153517245082597904713249543960384080650125499716705114242715738179989072532376555880380803010946804868225202872024135747861470461008912081036719241435203417748468850236402288732
n = 192542425715884301713081917578712610753585211586247457027440575560546523324959611967953696304847829302920032387302673964624917335577153799569696942382679089852516998347077344007753114528689243308665024295769519342792232346766547492729327691073909763212086055162995325600540813018294406887969046354469860816911568422712680599707620042592190367531749099423432044327950763774321076302036217545528041244087923582200718623694432015841557118933888773501380232386245666165512468040547204928162266514670178025040940706148925564444259159202694858617995324733833046220644932236275525583440888398601782945894818992063188633106032
c = 67905535339912972058045619912254931053123988251876822507801975107847652264296632842204004805630393419385997833467240510762112656634686438264301090132450140358111782950819399586870874773128677202899645060978197620952444791293599988676718118197381966878846966804634586613743109946107600947426411575020492087552743448643753662358968451941151910017029142336742493856682031548650744420202240800387911846576127391675529089811299152554611419106402299132972437006463256990385618923617789400776669078263024744389535889398373582282424348718185109878727127025678089109440512194763108872991739831765232049776510179013267917188 9
```

e相同，固定为65537，但有很多个不同n和c，通过对不同的n进行gcd算法，得到其最大公约数

```
list=[n,n1,n2,n3,n4,n5,n6,n7,n8,n9,n10,n11,n12,n13,n14,n15,n16,n17,n18,n19]
for i in range(len(list)):
    for j in range(len(list)):
        print i,j
        try:
            print (gcd(list[i],list[j]))
        except:
            print "error ",i
        continue
```

得到第5和第18个n有最大公约数，即p

```
p=132585806383798600305426957307612567604223562626764190211333136246643723811046149337852966828729052476725552361132437370521548707664977123165279305052971868012755509160408641100548744046621516877981864180076497524093201404558036301820216274968638825245150755772559259575544101918590311068466601618472464832499
```

第十八个n

```
n=132585806383798600305426957307612567604223562626764190211333136246643723811046149337852966828729052476725552361132437370521548707664977123165279305052971868012755509160408641100548744046621516877981864180076497524093201404558036301820216274968638825245150755772559259575544101918590311068466601618472464832499
```

计算得到q

```
q=14776424353634671565943210562886945157970478713667149608271913669396786298144402743028669371547005823776674992959544923454243263899558267530934520365086207480530925004879183357232838981513476339011274012541659465783011077278725928734994389420862012622240588724702458378297490076482722114439482245145715287352 7
```

现在知道了e，p，q就可以求d了

```
e=65537
phi=(p-1)*(q-1)
d=gmpy2.invert(e,phi)
print d
```

得到d的值，

```
d=135627439456579434083645649623595954215534595200056475397191397386124763236736020353461345717774410325918788555648934306787954239930657429538516233221067121204625626081904265710678456053706263602618409162986022504741933474740962412386593158363257962675759288876161509844416349690093498477461533535106694148520021925643244388482543893258639985734238948280093383529254683471710866696062963093860369250002261737449136160742987335623046910234689697026159960020010880696263118096659477836024849523821667994491719473885561372445250428264207701044567389996798820393778857620304518210062847040902157559234657826327978960681 66
```

接下来就是用d解c了

```
t=p*q
list=[c,c1,c2,c3,c4,c5,c6,c7,c8,c9,c10,c11,c12,c13,c14,c15,c16,c17,c18,c19]
for i in range(len(list)):
    print i
    try:
        print (pow(list[i],d,t))
    except:
        print "error ",i
    continue
```

在运行结果中看出来，第十八个(c17)是最短的，先解码试试

```
m17=13040004482825176402070107903979416267670062118522537076883968693524598900675425175282673277

print hex(m17)

0x666c61677b6162646362653566643934653233623364653432393232336162396332666467d
```

将下面的16进制值在网上十六进制转字符得到：

```
flag{abdcbe5fd94e23b3de429223ab9c2fdf}
```

嗯~，差不多就是这样

总结：
RSA有多个n的情况下，位数差别不大，甚至是完全一样的长度，这样的话，n是差不多大的，使用gcd（）求p的值。

写的不好，望各位大佬见谅！！