BUUCTF_Crypto题目： RSA5

原创

好想变强啊 已于 2022-03-18 10:58:09 修改 48 收藏

分类专栏： BUUCTF刷题记录 文章标签： python 网络安全

于 2022-03-18 10:43:58 首次发布

本文链接：https://blog.csdn.net/qq_38798840/article/details/123566783

BUUCTF刷题Crypto篇

文章目录

前言

记录一道BUUCTF网站上考察RSA的题目，在Crypto分类下的第2页，题目名称是“RSA5”。我刚开始刷题，感觉这道题还是蛮有特点的，不过不知道这里面是什么数学原理，循环遍历所有的n两两求最大公约数，得到的其中两个n的最大公约数刚好是素数所以可以作为p，然后再用n除以p得到的也是素数作为q，这是题目导致的巧合吗？

一、原题

下载题目的文件打开后，发现是20组不同的n和c的值，而它们对应的全是同一个m，且已知e=65537。拿到题之后感觉事情并不简单，尝试去在线网站分解n是分解不出来的，于是先去搜索了一波别人写的wp，便知道了解题步骤，本题解题的关键是借助这些n，对题目给出的n两两求解最大公约数，就找到了p，接下来就是自己写脚本再实现一遍了。

RSA5.txt

```
m = xxxxxxxx
e = 65537
========== n c ==========
n =
204749188940517785333052623456018809280882844711218237540497253540724771558737788480550738433458206978866410868426124865412501839659660015913420315629535617933323416413343028479961084174663606881398665051796895165893056369021372101856246508549067800372044122063099491990800055769227757737224388637621177504293275857920934474239800024012006133029438342128209092697138766834658173691585858222946750569789706122028854264360719502145382629210774090761604174366998361388011626213148456087968702068347041167077631698473872233078289085709449844169730194275297900290897662649490780386695234652438376752638580628547390836342070
c =
974463908243330865728978769213595400782053398596897741316275722596415018912929508637393850919224969271766388710025195039896961956062895570062146947736340342927974992616678893372744261954172873490878805483241196345881721164078651156067119957816422768524442025688079462656755605982104174001635345874022133045402344010045961111720151990412034477755851802769069309069018738541854130183692204758761427121279982002993939745343695671900015296790637464880337375511536424796890996526681200633086841036320395847725935744757993013352804650575068136129295591306569213300156333650910795946800820067494143364885842896291126137320

n =
209188199606488913494382630469549022109591464078609807421659302537813187592856924925114752632342420025094190795456440517552513113926357634125534997445064215660747212688223373216372659422267903438398561821005755398453588774937183342375858212633881811265451897234292621496306512894465534021905311355208361042171602683496885251683752134625702136128458989896943242694102024968716886499783702846610173990569039318406567573308596261837733965740564130173676064465401999731556304662394536372329369040637065511606502950312733856194707405935102672859579058015663625022627577506291629373737212917895276595314994352352616203097 59
c =
158196362019711855386948805051204693325821518567140708245218031218482923875568641771962297189237708100
```

CSDN @好想变强啊

二、解题步骤

1.计算最大公约数得到p

循环遍历题目给出的n，两两求解最大公约数，得到的最大公约数可以作为p，有了p也就可以计算q。因为这里的n都很大，写求解最大公约数的脚本的时候，不要用那种效率很低的写法，会半天出不来运行结果，我用的是辗转相除法。

2.计算求解RSA明文所需的其他值

有了p，也就可以计算出q，再根据RSA的理论知识，计算出d。

3.套公式计算出明文

根据RSA的加解密公式计算出明文，在Python中用pow函数即可，三个参数分别是c、d和n。注意最后输出前要用long_to_bytes转换成Bytes输出才是flag的形式。调用long_to_bytes要先from Crypto.Util.number import *。没有Crypto库的话，先去pip3 install pycryptodome。

4.写Python脚本

下面给出的是本题的完整代码，注释有点儿多，包含了自己在写代码中的一点发现。
最后的输出是
flag{abdcbe5fd94e23b3de429223ab9c2fdf}
代码如下：

```python
from operator import invert  #这个是调用了invert后自动出来的^_^
from gmpy2 import *  #gmpy2中也有invert也可以用gmpy2.invert
from Crypto.Util.number import *

"""该函数返回两个数的最大公约数"""
```

```python
def gcd(x, y):
    if y > x:
        x, y = y, x   # y为较小值
    while(x % y != 0):  #上面的比较大小也可以省略，因为如果x较小，第一次进while循环后也会交换xy
        a=x%y
        x=y
        y=a
    return y

'''究极简单的写法'''
# def gcd(a,b):
#     while b!=0:
#         a,b=b,a%b
#     return a

'''像菜鸟教程上给的求gcd的代码就太基础了运行起来太慢，所以要用上面的辗转相除法来求gcd'''
# def hcf(x, y):
#     """该函数返回两个数的最大公约数"""

#     # 获取最小值
#     if x > y:
#         smaller = y
#     else:
#         smaller = x

#     for i in range(1,smaller + 1):
#         if((x % i == 0) and (y % i == 0)):
#             hcf = i

#     return hcf

e = 65537

n1 = 20474918894051778533305262345601880928088284471121823754049725354072477155873778848055073843345820697886641
08684261248654125018396596600159134203156295356179333234164133430284799610841746636068813986650517968951658930563690213721018562465085490678003720441220630994919908000557692277577372243886376211775042932758579209344742398000240120061330294383421282090926971387668346581736915858582229467505697897061220288542643607195021453826292107740907616041743669983613880116262131484560879687020683470411670776316984738722330782890857094498441697301942752979002908976626494907803866952346524383767526385806285473908363420 7
c1 = 97446390824333086572897876921359540078205339859689774131627572259641501891292950863739385091922496927176638871002519503989696195606289557006214694773634034292797499261667889337274426195417287349087880548324119634588172116407865115606711995781642276852444202568807946265675560598210417400163534587402213304540234401004596111172015199041203447775585180276906930906901873854185413018369220475876142712127998200299393974534369567190001529679063746488033737551153642479689099652668120063308684103632039584772593574475799301335280465057506813612929559130656921330015633365091079594680082006749414336488584289629112613732 0
n2 = 20918819960648891349438263046954902210959146407860980742165930253781318759285692492511475263234242002509419079545644051755251311392635763412553499744506421566074721268822337321637265942226790343839856182100575539845358877493718334237585821263388181126545189723429262149630651289446553402190531135520836104217160268349688525168375213462570213612845898989694324269410202496871688649978370284661017399056903931840656757330859626183773396574056413017367606446540199973155630466239453637232936904063706551160650295031273385619470740593510267285957905801566362502262757750629162937373721291789527659531499435235261620309759
c2 = 15819636201971185538694880505120469332582151856714070824521803121848292387556864177196229718923770810072104155432038682511434979353089791861087415144087855679134383396897817458726543883093567600325204596156649305930352575274039425470836355002691145864435755333821133969266951545158052745938252574301327696822347115053614052423028835532509220641378760800693351542633860702225772638930501021571415907348128269681224178300248272689705308911282208685459668200507057183420662959113956077584781737983254788703048275698921427029884282557468334399677849962342196140864403989162117738206246183665814938783122909930082802031855
```

```
n3 = 25033254625906757272369609119214202033162128625171246436639570615263949157363273213121556825878737923265290
57955187382437487095746716398954206348941663671365464248671721923122507411526968411942808635253547168335948624820
03644461465935500517901513233739152882943010177276545128308412934555830087776128355125932914846459470221102007660
69122119923105388906543964871117053857305028435897272898296921521771347530986497814122470656606378262820551699918
82409911091657685618887697562137660663425892778402578714226336715294710872075722244668641562747970366603187163560
56314282727051189190889008763055811680040315277078928068816491
c3 = 41853085294168740058312307810140924071984513859556773996685018339026234783956692794048839907251843327091524
43372583701076198786635291739356770857286702107156730020004358955622511061410661058982622055199736820808203841446
79630528439465171443091869038948692056083467231615814645318378941214093902902932475603535808175442664516003326 2
92433024867521610827098015704970548862026348512948095281476400286528001918512766244931832427938327776641625814222
75143923532168798413011028271543085249029048997452212503111742302302065401051458066585395360468447460658672952851
64354719382277521838785362345363802549238912220450755590886 2

n4 = 21206968097314131007183427944486801953583151151443627943113736996776787181111063957960698092696800555044199
15676567793537314959822118479228681221329461774983460769630211613674566281665811705542780331523004270069512571840
16468104848730647750052210891740568247249221608558105272367513896050175795452358768649984198730652172948202447 3
07851205251265658155602290018876228375491181680816851833710923951285981250047302689102760248068085658020813668980
90403250992045378599705615049764523492552888387941964218910964900913238158667339002761476660503895101585308672116
80187875234592649321650468168816827742292436885816143064807 51
c4 = 45210380110447584418911284684672330884938857508505889857085199111547780905971361261502890418934541266744681
41393472662337350361712212694867311622970440707727941113263832357173141775855227973742571088974593476302084111770
06257642228383662775595608870429488598921385514726806545178149166092797483655806107122598566777405184770865315920
23310717547006829190360750579943293198966370747701790461142621377023839700574373038608003195569415846655847559975
19402450391676291265767840244823484528683134174715429567782855677794359402671406799066865318624676272384010034 5
91016371912972094224703881218025365697614144576182583435506 13

n5 = 22822039733049388110936778173014765663663303811791283234361230649775805923902173438553927805407463106104699
77399415837570403309347176138779985216833789852698052175361430789966901593138781992742187531630459152190159282381
44417756447695701045846773508629371397013053684553042185725059996791532391626429712416994990889693732805181947970
07142930959961497377273655629940424642479166067925388494002172884690634419885477919195173971934290876133066191 0
47711993342855077424291042095249692960568615479948783992342433635374744215357167806452076314979329436078782175170
35432886967269239096703968215510530480356194997063911181450 67
c5 = 15406498580761780108625891878008526815145372096234083936681442225155097299264808624358826686906535594853622
68737926896946843307238814978660739539642410431882087944374311235870654675393521575607834595937529965071855575969
88878523180175975030743173567451225144818078437456264297978614630129401727976125890316867181853903453892958510 7
52792785161470766022701785406901478083141727989874972593300378103285234648518956218518590278236816559341047136895
39848047163088666896473665500158179046196538210778897730209572708430067658411755959866033531700460551556380993 9
82706171848970460224304996455600503982223448904878212849412357

n6 = 21574139855341432908474064784318462018475296809327285532337706940126942575349507668289214078026102682252713
75770308155309310882321406379151848228984678019732982113950797476378026029030960088492081195984292554058396708 56
70848765317877441480914852329276375776405689784571404635852204097622600656222714808541872252335877037561388406 25
71817152787666528247863762622492749604671939619566909748536797952491587510784222965803675062197197387621599659 58
87780618746107068907129094818194956125414431077694333485977512165018624584603172050794498783848972312789722341 68
02436021278671237227993686791944711422345000479751187704426369
c6 = 20366856150710305124583065375297661819795242238376485264951185336996083744604593418983336285185491197426018
59503144465212328846149187902109602820369413668320344169298706956351302600186143572211798555990969267090734756 35
94578265880806540396777223906955491026286843168637367593400342814725694366078337030937104035993569672959361347 28
78941430271868468567729830583289197167029822221428488481177684999966175883053014830854285472673370709987674125 40
22591150819684225313435590126386112150065024029674670296759422440165022016878053714165448921501914212228430811 62
84129004257364769474080721001708734051264841350424152506027932

n7 = 25360227412666612490102161131174584819240931803196448481224305250583841439581008528535930814167338381983764
99129657563723191654764797057375826941116821930237054168478912511250502114850680964308195023762370318102569658 59
98044695691322012183660424636496897073045557400768745943787342548267386564625462143150176113656264450210023925 57
19459614057092766319907316021981042875285280556500504861598376122796004152594863061549475140054089075900837477 58
95311548612486548672063382055913506344094252803140295195855763083350377511201071560427811432552899377108123353 52
47118481765852273252404963430792898948219539473312462979849137
c7 = 19892772524651452341027595619482734356243435671592398172680379981502759695784087900669089919987705675899945
65864862380009027259915459012308218964502180095807686151839732543952113999565202637713236823250210862003340005 13
```

```
n8 = 22726855244632356029159691753451822163331519237547639938779517751496498713174588935566576167329576494790219360727877166074136496129927296296996970048082870488804456564986667129388136556137013346228118981936899510687589585286517151323048293150257036847475424044378109168179412287889340596394755257704938006162677656581509375471102546261355748251869048003600520034656264521931808651038524134185732929570384705918563982065684145766427962502261522481994191989820110575981906998431553107525542001187655703534683231777988419268338249547641335718393312295800044734534761692799403469497954062897856299031257454735945867491191
c8 = 60401197951758564075410823600235322046147238586886367248227127175727597939602463418003081497398098712343130496297329347975697810530006861856663748339784032905250725987740017313502447445907727957010651295618981165764999841859206612711236653561327191936654742355968842391080306058827778688561223782226811405705191803212869769471540422726224113039810113025862256308598927317246405746581254782871151984062538473679798837680008126053954829526986896044777194789475954421859214806526378683356732332006621006210250615008957296053056658646931229525573618715231653002060703256603530955927780377673953603292313313228236100600060
n9 = 232973337914430532973630007868353360952522908184619500545426583274845074065946327857127674599589179430955225942282054234282073451288997458009273191472576697738126695427828392377443051800982765788419294963459639975122442193767017876160462353971393818948374355626625910607684769973335387480652940331416105022523252928018168122689341713619343999515486272677914010897039373890125865810802233130601594562388570807406995286664113030299348070112149539841697858447141596277920169264909552826978771416146388063976893067953283447784786920847542167534258425578188994679451026467763426551676553842248605040860831478412522327609410264677634265516765538422486050408608314784125223276094
c9 = 54181203012083787131158894655799642578718141145150460960909601597378590768292585169203615778539039259541984068437573036875578483023022002292959169024302057378436018067007382347566985757086124249284804408687391200758886816720622065291565664212766111078029174189936250296906271968138303263698742497776192396033006058768659675157190797971159105786535627878990193101399459049580248824178337363048947654334894762345753567552751472565773870228733489069001496349407471045138501541181069911370726433086202846631082830522457509452289953878034321288421522515492926989474076636438958534326500293520920183728344570542711028169340
n10 = 28873667904715682722987234293493200306976947898711255064125115933666968678742598858722431426218914462903521596341771131695619382266194233561677824357379805303885993804266436810606263022097900266975250431575654686915049693091467864820512767070713267708993899899011156106766178906700336111712803362113039613548672937053397875663144794018087017731949087794894903737682383916173267421403408140967713071026001874733487295007501068871044649170615709891451856792223215526696220161842742664778581287321318748202431466508948902745314372299799561625186955234673012098210919745879882268512656931714326782335211089576897310591491
c10 = 99198804637868366849879579790915274774714449963923752440755278418655091601816665430163176349635124375103241987024163228413774894170295723884744500758014629968252446575302861074281863541728367165028176090705909297692619323242753532899393025364403106286983492448720640057006445202237276709507879242960042968830329789412008833626539933516385458602071790224724926712566304272284618526681180353170214286759548749470151977459169181977251211222363693827415339830234622559139246928062493874490166298658233164023660176578441669198466834978518423880582838562199005355674271036038699550661934255013852553220979015314021038838691
c11 = 14915270502032949898828292485603951848049772777471261431039572191646241875284410478373512635804406864747673804640055402646279101264831299306683440958145475921150610578434701314980750604203951110086190271990370199257012366601665630682456839757877628043595201647016916909164825910261385827055582468694961627597808784371379608230000439882273030038764105031213701633037116033594307645393375978668625084515281582851032518100587418796878752183841602825061727066133594776572154207348160493933395937554892185887966070602618979052334532686714116106310473404594879374795119334503694622137957389330190014718031576077917385384671
n12 = 27646746423759020111007828653264027999257847645666129907789026054594393648800236117046769112762641778865620892443423100189619327585811384883515424918752749559627553637785037359639801125213256163008431942593727931931898
```

19972755276862677561847983302910124969257371603070669570251098228355574085104702267248574343246464777288231421517611473225749724028416401691401868904455721892030026223465284063240606727337526930100840986019318082236673587728205783314326102263756503786736122321348320031950012144905869556204017430593656052867939493633163499580242224763404338807022510136217187779084917996171602737036564991036724299

c12 = 219915241289572605360437712848549203931058081267001282221258567755068857219711931093613159611291908146746471364648870878939906608949616128382050864010188854576674889118986542702355619801111746033237212809111974882865852693568495792630434563163194764958886962193442198665168611876541805092478812512512789193462671299047392773862892403943845751243311356559435138310099340233974570821846997377343888237633068053264303958499357702138175333872354863070088924109206116699326930181655694174458858108257496093886272312358409126446546858196209316633462975963348344986617890164503717692036501099947718724041857702301729340139711

n13 = 205454874058169287317389883744750126868279337097897843918557068351362702709334012030193291369376508783861171877765306393425721232371880539786226972825214739179782828304321611532212161941698796695419988406913830254872208508720754360643084999249585179797279544029656121960814043416515173263640415192501250364248226343542687738954656989208834392229965812263585958739939766046998306139323207205541300116712979444335150471805654844951910038875998912890379820102163578310783281590289532220569181893658407115886710933330131174540343136228550827958131223385624462230412111922770892250783246821080338430239035501728919596735511

c13 = 142274391881910294612504766927905396546191998884873194291144145579753763086889080281408171572055798040597838076413055773857247585301385149729622090622305761074061424026034843756260773451908830940976360197713778663395315119651366505674123638891831596161884492637524753286632453110599883379960473592632888374363055888480445729377594244665868702805124243368070647298945158405524047568795906987970463333364454651204450875876217439066242796217796347723788029591097144005161837183232672738247365401685459464444375862992141104247381599573883507859993485351715535693730882515527123912883652952676656913577196160116136287721751

n14 = 27359727711584277234897157724055852794019216845229798938655814269460046384353568138598567755392559653460949444557879120040796798142218939251844762461270251672399546774067275348291003962551964648742053215424620256999345448398805278592777049668281558312871773979931343097806878701114056030041506690476954254006592555275342579529625231194321357904668512121539514880704046969974898412095675082585315458267591016734924646294357666924293908418345508902112711075232047998775303603175363964055048589769318562104883659754974955561725694779754279606726358588624791988159992768392349521420172105938873719506454184173559125679874

c14 = 37885297842482550270816745408770163728078482227768879204534888782471379305782967974376479224945104837676511504929333560932889659437415702689438619870242766107127174091399464095139630431144639331460884300042377471634228029592502966025706493630161515813640067958942265995847080725826969967405188876067854607758510298142803593857630910789023019572264846204285136046305851315111670157631905912258842027728404565636431595078057110041139014175037511810508236382078035331114295109116161608513917547544347648195680548508238109011598212978497900056461021293540357353501244768387866615420890455096569103486767428449570088574574

n15 = 27545937603751737248785220891735796468973329738076209144079921449967292572349424539010502287564030116831261268197384650511043068738911429169730640135947800885987171539267214611907687570587001933829208655100828045651391618089603288456570334500533178695238407684702251252671579371018651675054368606282524673369983034682330578308769886456335818733827237294570476853673552685361689144261552895758266522393004116017849397346259119221063821663280935820440671825601452417487330105280889520007917979115568067161590058277418371493228631232457972494285014767469893647892888681433965857496916110704944758070268626897045014782837

c15 = 14069112970608895732417039977542732665796601893762401500878786871680645798754783315693511261740059725171342404186571066972546332813667711135661176659424619936101038903439144294886379322591635766682645179888058617577572409307484708171144488708410543462972008179994594087473935638026612679389759756811490524127195628741262871304427908481214992471182859308828778119005750928935764927967212343526503410515793717201360360437981322576798056276657140363332700714732224848346808963992302409037706094588964170239521193589470070839790404597252990818583717869140229811712295005710540476356743378906642267045723633874011649259842

n16 = 25746162075697911560263181791216433062574178572424600336856278176112733054431463253903433128232709054141607100891177804285813783247735063753406524678030561284491481221681954564804141454666928657549670266775659862814924386584148785453647316864935942772919140563506305666207816897601862713092809234429096584753263707828899780979223118181009293655563146526792388913462557306433664296966331469906428665127438829399703002867800269947855869262036714256550075520193125987011945192273531732276641728008406855871598678936585324782438668746810516660152018244253008092470066555682727138937298747951929576231036251316270602513451

c16 = 17344284860275489477491525819922855326792275128719709401292545608122859829827462088390044612234967551682879954301458425842831995513832410355328065562098763660326163262033200347338773439095709944202252494552172589503915965931524326523663289777583152664722241920800537867331030623906674081852296232306336271542832728410803631170229642717524942333398424670351436315044011407270832707324642374439152638658805803087761112197189617463788429246441

```
42717324942352390842467051436315044011407270852707324642574459152638638803803087761112197189617463788429246441421272435738249725338194790793810231035858620990633821297575601240746761506222887060941100755677064034429206964726277976076979628730261122405274983085359032326639390285870367240
n17 = 232884869341171203150369194185881362270284854941379301963237153362088493278339656938946705672179717279212438391299691287838530157601554467705906960375826848459371327900473632163620872778613369647608902140597327793830203492048032057258702254299859395701415082200412868578100481646967070186637584168077089106714774073660988834308118619330149734093901799485777125797493522994403105436890356514653998679084288855412377761434043763334429493970632492237023550515717905551512038668218679085317337887849786674787076729845395124315495586724677527120045193003189992081020767325014125891049047349837898953587536640774868945294990
c17 = 107382544181140765480714488449640464681416217406032143849863541891052369770710014292715606364280759704598909582749417625281164451711610400408333578761346897498469400526193927503946835048160811934323506694524461132856389825517625866563291090072140199449758164348277688827046304600012094522391628965761918763246623331538355339566002952551583770251984269509440406432354302110110635860324677243297357859473720517590421381710541658548424729905838008099848932325490927664005103000835855130141712204231034522928914961418069563003965406823816683675645694278130920640539931035376359943111430107088148518672397064925772032899024
n18 = 19591441383958529435598729113936346657001352578357909347657257239777540424811749817783061233235817916560689138344041497732749011519736303038986277394036718790971374656832741054547056417771501234494768509780369075443550907847298246275717420562375114406055733620258777905222169702036494045086017381084272496162770259955811174440490126514747876661317750649488774992348005044389081101686016446219264069971370646319546429782904810063020324704138495608761532633106997533224448710603836930444819322658015058196469985351920830368725516834057661239684879076489809007121180523461745335139780091317571675475958575523705865339 73
c18= 38349170988872029319819687046591193416244322947593619195539375510534996074403332340181891419702463022993857425482785898960332828949812003532706371272134831721825298904959034256491167559016311016658763017998656127177503600890851791427506646034541936420530163847145158558683687235089222717671902855211377856880756228329248292483627744764562328268858010469693845195493854282595915667168908446046962587836393908541530393294807262051471992471836215351724508259790471324954396038408065012549971670511424271573817998907253237655588038080301094680486822520287202413574786147046100891208103671924143520341774846885023640228872
n19 = 19254242571588430171308191757871261075358521158624745702744057556054652332495961196795369630484782930292003238730267396462491733557715379956969694238267908985251699834707734400775311452868924330866502429576951934279223234676654749272932769107390976321208605516299532560054081301829440688796904635446986086191156842271268059970762004259219036753174909942343204432795076377432107630203621754552804124408792358220071862369443201584155711893388877350138023238624566616551246804054720492816226651467017802504094070614892556444425915920269485861799532473383304622064493223627552558344088839860178294589481899206318863310603
c19 = 67905535399129720580456199122549310531239882518768225078019751078476522642966328422040048056303934193859978334672405107621126566346864382643010901324501403581117829508193995868708747731286772028996450609781976209524447912935999886767181181973819668788469668046345866137431099461076000947426411575020492087552743448643753662358968451941151910017029142336742493856682031548650744420202240800387911846576127391675529089811299152554611419106402299132972437006463256990385618923617789400776669078263024744389535889398373582282424348718185109878727127025678089109440512194763108872991739831765232049776510179013267917188 9
n20 = 26809700251171279102974962949184411136459372267620535198421449833298448092580497485301953796619185339316064387798092220298630428207556482805739803420279056191194360049651767412572609187680508073074653291350998253938793269214230457117194434853888765303403385824786231859450351212449404870776320297419712486574804794325602760347306432927281716160368830187944940128907971027838510079519466846176106565164730963988892400240063089397720414921398936399927948235195085202171264728816184532651138221862240969655185596628285814057082448321749567943946273776184657698104465062749244327092588237927996419620170254423837876806659
c20 = 38621355660843401376986472712387941204199127152899052854850745121069261898665287042463221942460167752426501104314674830977406789498506928806795254613941681940403968845475604486278463088283349609082256858057285902980646671301748901528132153712913301179254879877441322285914544974519727307311002330350534857867516466612474769753577858660075830592891403551867246057397839688329172530177187042229028685862036140779065771061933528137423019407311473581832405899089709251747002788032002094495379614686544672969073249309703482556386024622814731015767810042969813752548617464974915714425595351940266077021672409858645427346

n=[n1,n2,n3,n4,n5,n6,n7,n8,n9,n10,n11,n12,n13,n14,n15,n16,n17,n18,n19,n20]

#计算所有给出的n的两两之间的最大公约数，把不是1的结果都输出出来，得到p
for i in range(len(n)):
```

```
    for j in range(i+1,len(n)):  #经实验发现range的首尾相同时，循环体内容不会执行所以没有报错
        if(gcd(n[i],n[j])!=1):
            print(i,j)  #本题的输出只有4 17，即n5和n18有最大公约数
            N=n[i]  #这里我选择用n5的值作为n，所以后面密文也要用c5
            p=gcd(n[i],n[j])
            print('n=',N)
            print('p=',p)
#p=132585806383798600305426957307612567604223562626764190211333136246643723811046149337852966828729052476725552361132437370521548707664977123165279305052971868012755509160408641100548744046621516877981864180076497524093201404558036301820216274968638825245150755772559259575544101918590311068466601618472464832499
q=N//p  #q=172130338499326278748088659642118539903263306644625489813269854049704514120598134934786316771912260248369075948864036229605563950070491992643125838594149381631362120542615545158696925360916086470107987771246645459433841320759048661246016875180635458357799131806734777129141845728102816378815607663660131827433
phi=(p-1)*(q-1)
d=invert(e,phi)
m=pow(c5,d,N)  #因为前面的N取的是n[4]，要注意其对应值是n5，所以密文是c5
#print(m)  #m=13040004482825176402070107903979416267670062118522537076883968693524598900675425175282673277
print(long_to_bytes(m))

'''最后这么写也能得到结果，调用bytes的函数不需要import Crypto库，但要注意先转16进制，然后调用fromhex时还要去掉最前面的0x(hex()函数的结果是str，fromhex()的参数也是str)，
实际上，long_to_bytes是在函数内部自行做了先把数字转16进制再将16进制数两两一组转换成ascii码对应字符'''
#print(hex(m))
#print(bytes.fromhex(hex(m)[2:]))
```

```
4 17
n= 228220397330493881109367781730147656636633038117912832343
138779985216833789852698052175361430789966901593138781992742
042185725059996791532391626429712416994990889693732805181947
988547791919517397193429087613306619104771199334285507742429
436078782175170354328869672692390967039682155105304803561949
p= 132585806383798600305426957307612567604223562626764190211
771231652793050529718680127555091604086411005487440466215168
554410191859031106846660161847246483249 9
b'flag{abdcbe5fd94e23b3de429223ab9c2fdf}'
```


总结

以上就是本题要记录的全部内容了~初学者总是想要记录下每一点的发现，有点冗余的感觉，可能以后做得多了见得多了就好啦？