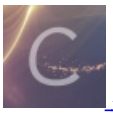
攻防世界—OldDriver

原创

C+J+H 于 2020-10-16 18:24:02 发布 757 收藏 1

分类专栏： 密码题 网络安全

本文链接：https://blog.csdn.net/addisonision/article/details/109121865



密码题 同时被 2 个专栏收录

1 篇文章 0 订阅

订阅专栏

网络安全

2 篇文章 0 订阅

订阅专栏

OldDriver

题目来源： XCTF 4th-WHCTF-2017 附件

题目描述：有个年轻人得到了一份密文，身为老司机的你能帮他看看么？

题目场景： 暂无


```
[{"c": 736606757474117146172206513324291608049550591366325033008274746538367689397041147655074839484143741810531235397109500342432267961694037112302898218950204 2, "e": 10,
"n": 251625070523397144218396888737345961777511240367238310033009597611378114907152057429417384065481502408617793017841336521659082279174154831375853889862748 03},
{"c": 219628253233004691517959202898868865627909427715468585008421798065664357671038039788851487721393054843196882493689995037844415073834760959462580113179514 61, "e": 10,
"n": 239768595899044197983208120976818586523254737918912327104319972028978195806349370709006252132180953307668771902124180232973417328088394883085511264099831 93},
{"c": 656968942027406695783598339058358528657008761904811014118770058419379269523540507781154435516929038235714937410707640608615410335189789079359899768705 3983, "e": 10,
"n": 185037828368585400439745580356016546109489155056452198201502510623051201487455459065675486501918320908234828526043464783353537845010767619226053618487036 23},
{"c": 450824616804451351845249388271353639063674154155180582179033897379761597127186724858437981311412547819528469269592866894655362548317963326605712296754 7052, "e": 10,
"n": 233830874785455122187131579329347461107217068190774234180602200836577134285035828019098071428026473679942897750155951005411683670830975061938094513650107 23},
{"c": 229661056702912823355888430182441615527644863731179428659669040761911223374355425532767439388176867295547143154948189227538801989458972224221372684276116 72, "e": 10,
"n": 317756490898614286710579090761441528707967225281125804794420733650539160125072734330284517554369870547224960577497317584759583011640827550031956320053084 93},
{"c": 179633130634050457429681369162198383521355617853895343812629792645853978968444708790236865085403551609985331229702392610702060892171531266493908256467120 87, "e": 10,
"n": 222463420229434328206961904441556652899283786538411726322832278881744954022486330610106155726421265845911037503389192139456460748338239055216430258790539 49},
{"c": 165241753470902945038057065397370532098611767959756387302268314080050748256048294831013154094822779704550539033314619158674926924954816824731640407401463 9, "e": 10,
"n": 253954611426706312681561061360283257443933584366175286779672493473535249246550011518495440222017725000332808223726613443526074347386960517790957365478130 43},
{"c": 155857717344883510394566313940404977595686794295106192197661917808076753617418592904907324511126487766481267797593684282051946847215164970262909817862393 52, "e": 10,
"n": 320565088927441849012894132877280398913038323115486081410882278763267536741541247751327769284819353781847567567851075407816325702953304867382681731678090 47},
{"c": 896512342163769405004421684452337916334747802912481503283281322505073255852423966064874628488414074678882368188601057734225484101459457006746790568235979 7, "e": 10,
"n": 528497662695418274742281894288206485741625395959853959922616498099074357422630205510500642688903333928771735728116915998412531504602199868179644619707365 53},
{"c": 135609457565430230085293881084469408471378530384370952445730358885312885773708290656663200693978983948484848470303210189156383818339355809583427199889782 47, "e": 10,
"n": 304159848003075789329463999875590889683556383543448233593972044191912418027217724994866156616990809985024399015855739508890479185379066878407250054962386 21}]
```


分析：

给了10组RSA的加密信息，共有10个公钥，并且所有的n都是互质的，因此想到了低加密指数广播攻击

```
import libnum
import gmpy2
dic = [{“c”:
736606757474117146172206513324291608049550591366325033008274746538367689397041147655074839484143741810531235397109500342432267961694037112302898218950204 2, “e”: 10, “n”:
251625070523397144218396888737345961777511240367238310033009597611378114907152057429417384065481502408617793017841336521659082279174154831375853889862748 03},
{“c”:
219628253233004691517959202898868865627909427715468585008421798065664357671038039788851487721393054843196882493689995037844415073834760959462580113179514 61, “e”: 10, “n”:
239768595899044197983208120976818586523254737918912327104319972028978195806349370709006252132180953307668771902124180232973417328088394883085511264099831 93},
{“c”:
```

65696894202740669578359833905835852865700876190481101411877005841937926952354050778115443551692903823571493741070764060861541033518978907935989976870539 83, “e”: 10, “n”: 18503782836858540043974558035601654610948915505645219820150251062305120148745545906567548650191832090823482852604346478335353784501076761922605361848703623},
{“c”: 45082461680445135184524938827135363906367415415518058217903389737976159712718672485843798131141254781952846926959286689465536254831796332660571229675470 52, “e”: 10, “n”: 23383087478545512218713157932934746110721706819077423418060220083657713428503582801909807142802647367994289775015595100541168367083097506193809451365010723},
{“c”: 22966105670291282335588843018244161552764486373117942865966904076191122337435542553276743938817686729554714315494818922753880198945897222422137268427611672, “e”: 10, “n”: 31775649089861428671057909076144152870796722528112580479442073365053916012507273433028451755436987054722496057749731758475958301164082755003195632005308493},
{“c”: 17963313063405045742968136916219838352135561785389534381262979264585397896844470879023686508540355160998533122970239261072020689217153126649390825646712087, “e”: 10, “n”: 22246342022943432820696190444155665289928378653841172632283227888174495402248633061010615572642126584591103750338919213945646074833823905521643025879053949},
{“c”: 16524175347090294503805706539737053209861176795975638730226831408005074825604829483101315409482277970455053903331461915867492692495481682473164040740146 39, “e”: 10, “n”: 25395461142670631268156106136028325744393358436617528677967249347353524924655001151849544022201772500033280822372661344352607434738696051779095736547813043},
{“c”: 15585771734488351039456631394040497759568679429510619219766191780807675361741859290490732451112648776648126779759368428205194684721516497026290981786239352, “e”: 10, “n”: 32056508892744184901289413287728039891303832311548608141088227876326753674154124775132776928481935378184756756785107540781632570295330486738268173167809047},
{“c”: 89651234216376940500442168445233791633474780291248150328328132250507325585242396606487462848841407467888236818860105773422548410145945700674679056823597 97, “e”: 10, “n”: 52849766269541827474228189428820648574162539595985395992261649809907435742263020551050064268890333392877173572811691599841253150460219986817964461970736553},
{“c”: 13560945756543023008529388108446940847137853038437095244573035888531288577370829065666320069397898394848484847030321018915638381833935580958342719988978247, “e”: 10, “n”: 30415984800307578932946399987559088968355638354344823359397204419191241802721772499486615661699080998502439901585573950889047918537906687840725005496238621}]
n = []
C = []
for i in dic:
n.append(i[“n”])
C.append(i[“c”])

for i in n:

```
#  for j in n:
    #  if i == j:
        #  continue
    #  else:
        #  if gmpy2.gcd(i, j) != 1:
            #  print i, j
```

N = 1
for i in n:
N *= i

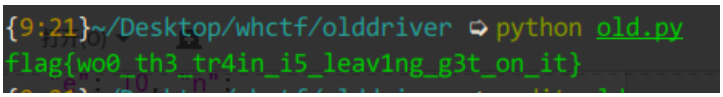
Ni = []
for i in n:
Ni.append(N / i)

T = []
for i in xrange(10):
T.append(long(gmpy2.invert(Ni[i], n[i])))

X = 0
for i in xrange(10):
X += C[i] * Ni[i] * T[i]

m10 = X % N
m = gmpy2.iroot(m10, 10)
print libnum.n2s(m[0])

运行结果



flag{wo0_th3_tr4in_i5_leav1ng_g3t_on_it} (最你好运)