攻防世界 Crypto高手进阶区 3分题 OldDriver

原创

思源湖的鱼 于 2020-12-07 13:28:52 发布 441 收藏

分类专栏： ctf 文章标签： 密码学 ctf 攻防世界 rsa crypto

本文链接：https://blog.csdn.net/weixin_44604541/article/details/110814842

前言

继续ctf的旅程

攻防世界Crypto高手进阶区的3分题

本篇是OldDriver的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

解题过程

得到密文

[{"c": 73660675747411714617220651332429160804955059136632503300827474653836768939704114765507483948414374181053123539710950034243226796169403711230289821895020 42, "e": 10, "n": 25162507052339714421839688873734596177751124036723831003300959761137811490715205742941738406548150240861779301784133652165908227917415483137585388986274803},
{"c": 21962825323300469151795920289886886562790942771546858500842179806566435767103803978885148772139305484319688249368999503784441507383476095946258011317951461, "e": 10, "n": 23976859589904419798320812097681858652325473791891232710431997202897819580634937070900625213218095330766877190212418023297341732808839488308551126409983193},
{"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}]

给了10组RSA的加密信息

- 共有10个公钥
- 所有的n都是互质的

低加密指数广播攻击

脚本

```
import libnum
import gmpy2

dic = [{"c": 73660675747411714617220651332429160804955059136632503300827474653836768939704114765507483948414374181053123539710950034243226796169403711230289821895020 42, "e": 10, "n": 25162507052339714421839688873734596177751124036723831003300959761137811490715205742941738406548150240861779301784133652165908227917415483137585388986274803},
{"c": 21962825323300469151795920289886886562790942771546858500842179806566435767103803978885148772139305484319688249368999503784441507383476095946258011317951461, "e": 10, "n": 23976859589904419798320812097681858652325473791891232710431997202897819580634937070900625213218095330766877190212418023297341732808839488308551126409983193},
{"c": 65696894202740669578359833905835852865700876190481101411877005841937926952354050778115443551692903823571493741070764060861541033518978907935989976870539 83, "e": 10, "n": 18503782836858540043974558035601654610948915505645219820150251062305120148745545906567548650191832090823482852604346478335353784501076761922605361848703623},
{"c": 45082461680445135184524938827135363906367415415518058217903389737976159712718672485843798131141254781952846926959286689465536254831796332660571229675470 52, "e": 10, "n": 23383087478545512218713157932934746110721706819077423418060220083657713428503582801909807142802647367994289775015595100541168367083097506193809451365010723},
{"c": 22966105670291282335588843018244161552764486373117942865966904076191122337435542553276743938817686729554714315494818922753880198945897222422137268427611672, "e": 10, "n": 31775649089861428671057909076144152870796722528112580479442073365053916012507273433028451755436987054722496057749731758475958301164082755003195632005308493},
```

{"c": 179633130634050457429681369162198383521355617853895343812629792645853978968444708790236865085403551609985331229702392610720206892171531266493908256467120 87, "e": 10, "n": 22246342022943432820696190444155665289928378653841172632283227888174495402248633061010615572642126584591103750338919213945646074833823905521643025879053949},
{"c": 165241753470902945038057065397370532098611767959756387302268314080050748256048294831013154094822779704550539033314619158674926924954816824731640407401463 9, "e": 10, "n": 25395461142670631268156106136028325744393358436617528677967249347353524924655001151849544022201772500033280822372661344352607434738696051779095736547813043},
{"c": 155857717344883510394566313940404977595686794295106192197661917808076753617418592904907324511126487766481267797593684282051946847215164970262909817862393 52, "e": 10, "n": 32056508892744184901289413287728039891303832311548608141088227876326753674154124775132776928481935378184756756785107540781632570295330486738268173167809047},
{"c": 896512342163769405004421684452337916334747802912481503283281322505073255852423966064874628488414074678882368188601057734225484101459457006746790568235979 7, "e": 10, "n": 52849766269541827474228189428820648574162539595985395992261649809907435742263020551050064268890333392877173572811691599841253150460219986817964461970736553},
{"c": 135609457565430230085293881084469408471378530384370952445730358885312885773708290656663200693978983948484848470303210189156383818339355809583427199889782 47, "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])
```

得到flag：`flag{wo0_th3_tr4in_i5_leav1ng_g3t_on_it}`

## 结语

RSA
```