

# HGAME 2021 week3 writeup

## Crypto

### LikiPrime

LikiPrime[已完成]

描述

Wow! RSA!

题目地址 <https://prime.liki.link/>

基准分数 250

当前分数 250

完成人数 43

#### 下载得代码

```
#!/usr/bin/env python3

import random
from libnum import s2n
from secret import secrets, flag

def get_prime(secret):
    prime = 1
    for _ in range(secret):
        prime = prime << 1
    return prime - 1

random.shuffle(secrets)

m = s2n(flag)
p = get_prime(secrets[0])
q = get_prime(secrets[1])
n = p * q
e = 0x10001
c = pow(m, e, n)

print("n = {}".format(n))
print("e = {}".format(e))
print("c = {}".format(c))
```

# n =

54480662578076527470362713889486540748591255021354202965062029859315189978396605  
66909014990944243667121934730267489179347110584556437961995117277785655935072352  
10471103749410209708428398554921045548457596717901688849110662006431551066171932  
41663991199835668973820397856942107803308420028326687835768515214777667811777301  
84118498363548686118560688296238480430905193595405961700128815181081343064720012  
09554224511908523620331293629994567633160923078515324787126043639972293248909282  
31743561589383273771046819398109277725236276142862880607175974306347753022257321  
68627610067560133580625728982295047579308641098722187252431318882430828324755964  
14341055382043397510388566153178797955354433740194210175735661605334278427963826  
45257612906381492293282290091167114882841499126596308310511811133517609760659106  
62007716689271971091481689237703779521406001541275618678202267875909401859492397  
91079405614967994735255149734157657559884622856408371334371327945887694841157583  
45488712834389335879569948749343202759878091651313990065628228749899051654855861  
90933144327823010135060087016313346488684414100985186285654232311076126919516379  
32929961651079801802627277235114289178164922207502776459622987767976004949513336  
67625344584228921383503930551975304974574547999422721901663712035432220321550490  
24090390710036052902064162308087692386918527919568126221866883986473750573671020  
66074869115310255610942615484688632815636854194831122945220666215456542098196307  
29109439974566550367158285111558035205190151293969910755432001132582172707112666  
59255886714938820191456489562716156543164403219053802212312765761900339403703133  
72783531071424333120440758646896149373089526503999343561782359884923387763614060  
63121639109865757863881574108696140718725257319281225590679935121087856822217023  
32733281574520542008914729209077239374901359663637027537059976976910914303558245  
35210953592699998553550797879973463843206032130110385893590948147419089764497483  
50484578664207026761891970239156797131863132566708791641536507750329437545587756  
64802256638829907634379439983164158483265098835872284899637347878548819596838513  
24638822085341902685051299305175500860101304573399058668299312927574701741002443  
90627674854278375731265389589854644671154749136163469076240220156880259297040239  
01048764086196802153415204926780478064298833052055627451253647946021068705815066  
81757893277071319158953845175078078660179608196467657260838076736379038608564972  
66318537119000663680614845720866964513910465439613131483104774794192030552306409  
71182532649432431514480233745395878459081809539376448027105464977578218874490130  
7027663871874871746470590469320230424450955567169537

# e = 65537

```
# c =
27472304656869343644929408715153248683928689753531302237846149586193226559658524
72626685704693541599170802117023089169653475239630815894826788344800551943789903
83244668002602101123854420784609037376693496552570502646685579670193045681644760
03371712074047631859356381314220275797370223904764150956047318838551436803476580
41475555395117369764258885702873268794540138189946394791022684064023107977712763
01050540373899230975720916201036158560040085923566525805554530408680304457848239
63084812467846920422018102448364940681809087475322202648045000194369310580771229
81438352230105142486359659078087421422741826949936653889611564621526352962261094
50945961119785494233980909934047754641703574730410152021685991701533369283007476
25215963351763010512528768843121649012913980511576697293053821980686770728713963
01532176831880030907761920077930151057094846403428175672447021775760982351719578
57240185525756224913394808461290609368016105155540767298421844084496676890629476
69775458756995253120785957525187827300384774112337418322486945805846155099612540
01903540028967209593334479006669050737815450878202536673494253315217540329764335
13550163674681305591065426732567741788842596758878948187820038338135003782249432
44145564262630622993102978542978860571516981688110026087044274942703988102857401
13422081879305121465497284624729384486924042269774783148988004427702322075980549
45682652967033493668448155374629677160486873168967742551866186111255422134879287
89033976848558608638046481533559393886009981988081183983196592236577929776547498
11101087819365277573572395556838299580474502740218350144950620659087760126464884
34564200851049885463697273124612569331498876656220381633200293350324343788986307
02767278792679860899857063832251565899221643895851518749616156123340494044272105
75996338071547332195506960774004491011707124920689629962269768257079600997923163
90249496415319256426718926121755091762577558746608819225004845686955157772212213
01172884965160819874524331172952658800119642626891005230555851266302821794197693
07967711845044069897157484221584128103974182407553885172154865857141473065117496
80100058255979478004135651321329204211567252410077812576106703564561988637786725
42473692677891402214281880316254585726954129418133854015185930387538559001852054
89943065983187789786963430408980404289094050861336769181010547830918793539878878
28947218860827466966726806023669857183011921990449184039111497573444819463447627
72558236351226158716656971440746603633587421806448284139682429625801828213166515
83215693982452743159433370039743897072216855095688844123698745297458491116059452
828366633503448889148896657676191573646532434154
```

简单的rsa，直接上代码

```

import gmpy2

n =
15361898878235696574667000105109009720717806584760935092206242960407549236363501
41721369634637099960797410424785647945883377241253698036574016171736926854787656
79305816624609468565620307223307834219959554473785941197585503297598493935350183
44139103042143621239011469955648205934903904045564846822159998174879695774419450
39972397014827014100300290292700276798425409997228874624348108438164371973195836
07025618186635697305976249665612688247376108935160320686131200898556905800476205
89196079907477458543783300282393495461746306096415443274084362956267239186823089
34909039891974881493887293847809706526715623164848720332941242261571171188616463
40597233621672361185214584972483051157645107627319152918821554940117132954626032
21439763218477455674584662524137991730891776826849188975650354165106378834014987
69559274683699800223282667833991991879978124682745961708268742595543064181551841
68780157285144772871929341939578335329966872345542802638170681068054408484756688
30505180172049674756979856286907198648267160926305328986853052888831678087029867
946180609
e = 65537
c =
79271876280260553227839409015506519378939536600655346097140017119244569630956030
13667085470146144874981960574233466397443449977149997357471575431695025415526421
12792742458525353399996126506677910325962345120811170908229213934705931214913766
54264623818163291782294846802753686574500030467013559850140097009154394174668264
46848877329284810802949440433122207430136944380576095681081740197798597559437163
70251171244889298697822928557767241086599188963468602462907190279377862069254854
82342766786531956483054627036235793693099564816062230430409030821805597205512355
15700080661234190693094571406679557502413049745325301747588707839920522910923018
86400900398847537125874296993238159030838154303553904314963487162292769564595304
42493318890580816997838849659649869198520757681191854865067299584816888485477301
31040350180411446263394686119546781350542737049112800140601734883325024073000156
07842759235048437997661556158686088265640319895236141159912535842267682895490879
75422256114189692339855029003163428969031618118940618263083025942732091311328022
70416006
p =
10407932194664399081925240327364085538615262247266704805319112350403608059673360
29801223944173232418484242161395428100779138356624832346490813990660567732076292
41295093892203457731833496615835504729594205476898112116936771475484788669625013
84438260291732348885311160828538416585028255604666224831890918801847068222203140
521026698435488732958028878050869736186900714720710555703168729087
q =
14759799152141802350848986227373817363120661453331697751477712164785702978780789
49377407337049389289382748507531496480477281264838760259191814463365330269540496
96120111343015690239609398909022625932693502528140961498349938822283144859860183
43185362309237726413902094902318364468996082107954829637630942366309454108327937
69905399982457186322944729636418890623372171723742105636440368218459649632948538
69690587265048691443463745750728044182367681351785209934866084717257940842231667
80976702240119902801704748944874269247421088235368084850725022405194525875428753
49976558572670229633962575212637477897785501552646522609988869914013540483809865
681250419497686697771007
fn= (p-1)*(q-1)
d = gmpy2.invert(e,fn)
m = gmpy2.powmod(c,d,n)
print(hex(m))

```

得hex并转换，得flag

0x6867616d657b4d657273336e6e657e5072214d655e7265346c31795f73302b354f2d6c6937746c65217d

hgame{Mers3nne~Pr!Me^re4l1y\_s0+50~1i7tle!}

# MISC

# A R K

A R K[已完成]

描述

星藏点雪 月隐晦明 以夕为重 泼雪作屏

补充说明：明日方舟是一款塔防游戏，可以将部署单位放置在场地中。并且具有自律功能，可以记录部署的操作。

翻译：没用 没用 出题人用部署单位画了个东西 背景是白色的

本题目所有解题操作均只用流量，与网址无关


题目地址 [https://1.oss.hgame2021.vidar.club/ark\\_faf7cb41607dbb224f79bc470b5f2836.pcapng](https://1.oss.hgame2021.vidar.club/ark_faf7cb41607dbb224f79bc470b5f2836.pcapng)

基准分数 250

当前分数 250

完成人数 19

打开流量包，注意到其中获取 `ssl.log` 的信息，找到并导出 `ssl.log`，再从 `TLS` 中重新导入，发现新的 `http` 内容，并在其中发现一长串 `base64`，转为 `16` 进制后发现压缩包文件头（文件头要稍作修改）

 default_entry	376 344	10 356	2021-02-1...	2021-02-1...	2021-02-1...	A	-	8261DBA2 Deflate	NTFS
---	---------	--------	--------------	--------------	--------------	---	---	------------------	------

发现文件并加后缀名 `json`，并在其中发现 `row` 和 `col`，根据 `hint` 得知是画图

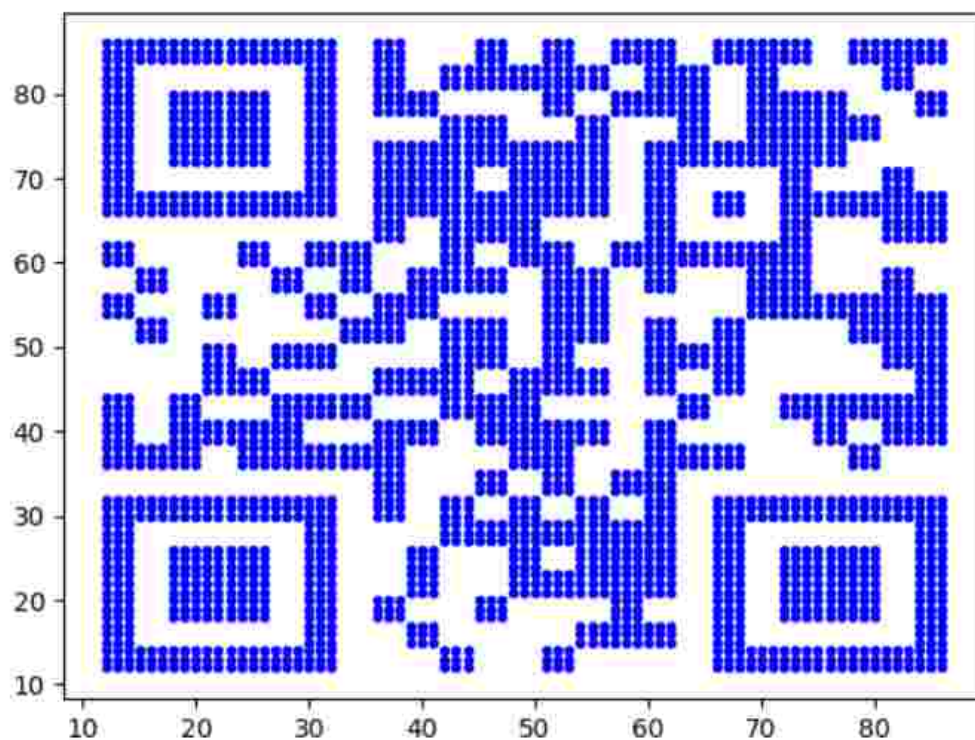
```
from matplotlib import pyplot as plt
import numpy as np
import json

with open("default_entry.json", "r") as f:
    data = json.load(f)
lists=list(data['journal']['logs'])
row=[]
col=[]
for i in lists:
    row.append(i['pos']['row'])
    col.append(i['pos']['col'])

for i in range(len(row)):
    plt.plot(row[i], col[i], '.b')

plt.show()
```

用脚本画图后发现二维码



```
hgame{Did_y0u_ge7_Dusk?}
```

这周难度突然增加，再加上有些摸鱼，发现啥也做不出😓,下周不能再摸了