**HGAME比赛第二周WP**

****

至于为什么没有写re一方面是因为最开始两天解题时遇到了点困难，babyre不知道为什么线程调试失败，浮点异常，最后也没找到好方法，backpack revenge因为这两天出去玩没啥时间看（enmm写了也是现学现写）

**CRYPTO**

题目一：midRSA

解题过程：打开py文件，看到以下代码：

def padding(flag):

return flag+b'\xff'\*(64-len(flag))

flag=padding(flag)

m=bytes\_to\_long(flag)

p=getPrime(512)

q=getPrime(512)

e=3

n=p\*q

c=pow(m,e,n)

m0=m>>208

这道题出题人有个大失误，注意观察这里的flag只与m有关,RSA中的n,c,e就没有用到，这也是题目非预期原因，利用这个bug写出脚本，甚至后面的0xff不用管

from Crypto.Util.number import long\_to\_bytes  
  
m0 = 13292147408567087351580732082961640130543313742210409432471625281702327748963274496942276607  
m=m0<<208  
  
flag = long\_to\_bytes(m)  
print(flag)

flag值：hgame{0ther\_cas3s\_0f\_c0ppr3smith}

题目二：backpack

解题过程：这是题目from Crypto.Util.number import \*  
import random  
from secret import flag  
a=[getPrime(32) for \_ in range(20)]  
p=random.getrandbits(32)  
assert len(bin(p)[2:])==32  
bag=0  
for i in a:  
 temp=p%2  
 bag+=temp\*i  
 p=p>>1  
  
enc=bytes\_to\_long(flag)^p  
  
print(f'enc={enc}')  
print(f'a={a}')  
print(f'bag={bag}')  
"""  
enc=871114172567853490297478570113449366988793760172844644007566824913350088148162949968812541218339  
a=[3245882327, 3130355629, 2432460301, 3249504299, 3762436129, 3056281051, 3484499099, 2830291609, 3349739489, 2847095593, 3532332619, 2406839203, 4056647633, 3204059951, 3795219419, 3240880339, 2668368499, 4227862747, 2939444527, 3375243559]  
bag=45893025064  
"""

脚本如下

from Crypto.Util.number import long\_to\_bytes  
enc = 871114172567853490297478570113449366988793760172844644007566824913350088148162949968812541218339  
a = [3245882327, 3130355629, 2432460301, 3249504299, 3762436129, 3056281051, 3484499099, 2830291609, 3349739489, 2847095593, 3532332619, 2406839203, 4056647633, 3204059951, 3795219419, 3240880339, 2668368499, 4227862747, 2939444527, 3375243559]  
bag = 45893025064  
  
flag = enc ^ bag  
flag = long\_to\_bytes(flag)  
print(flag)

其实根本不需要写算法，因为移位后p只有12位，直接异或对于flag改变不大，最后flag也是我猜的，这应该是非预期的点吧,最后输出是下面的

b'hgame{M@ster\_0f ba3kpack\_m4nag3ment+t\x1a\xc7\x04'

flag值：hgame{M@ster\_0f ba3kpack\_m4nag3ment!}

题目三：midRSA revenge

解题过程：from Crypto.Util.number import \*  
from secret import flag  
m=bytes\_to\_long(flag)  
p=getPrime(1024)  
q=getPrime(1024)  
e=5  
n=p\*q  
c=pow(m,e,n)  
m0=m>>128  
print(f'n={n}')  
print(f'c={c}')  
print(f'm0={m0}')  
  
"""  
n=27814334728135671995890378154778822687713875269624843122353458059697288888640572922486287556431241786461159513236128914176680497775619694684903498070577307810263677280294114135929708745988406963307279767028969515305895207028282193547356414827419008393701158467818535109517213088920890236300281646288761697842280633285355376389468360033584102258243058885174812018295460196515483819254913183079496947309574392848378504246991546781252139861876509894476420525317251695953355755164789878602945615879965709871975770823484418665634050103852564819575756950047691205355599004786541600213204423145854859214897431430282333052121  
c=456221314115867088638207203034494636244706611111621723577848729096069230067958132663018625661447131501758684502639383208332844681939698124459188571813527149772292464139530736717619741704945926075632064072125361516435631121845753186559297993355270779818057702973783391589851159114029310296551701456748698914231344835187917559305440269560613326893204748127999254902102919605370363889581136724164096879573173870280806620454087466970358998654736755257023225078147018537101  
m0=9999900281003357773420310681169330823266532533803905637  
"""

这道题是RSA中的m高位泄露，学习一下找个脚本就好了，这里我用了在线sage网站（不想下载），将部分脚本放到sage中跑出来就行，网址<https://sagecell.sagemath.org/>

n=27814334728135671995890378154778822687713875269624843122353458059697288888640572922486287556431241786461159513236128914176680497775619694684903498070577307810263677280294114135929708745988406963307279767028969515305895207028282193547356414827419008393701158467818535109517213088920890236300281646288761697842280633285355376389468360033584102258243058885174812018295460196515483819254913183079496947309574392848378504246991546781252139861876509894476420525317251695953355755164789878602945615879965709871975770823484418665634050103852564819575756950047691205355599004786541600213204423145854859214897431430282333052121

c=456221314115867088638207203034494636244706611111621723577848729096069230067958132663018625661447131501758684502639383208332844681939698124459188571813527149772292464139530736717619741704945926075632064072125361516435631121845753186559297993355270779818057702973783391589851159114029310296551701456748698914231344835187917559305440269560613326893204748127999254902102919605370363889581136724164096879573173870280806620454087466970358998654736755257023225078147018537101

m\_high=9999900281003357773420310681169330823266532533803905637

m\_high <<= 128

e = 5

PR.<x> = PolynomialRing(Zmod(n))

m = m\_high + x

f = m^e - c

f = f.monic()

x = f.small\_roots(X = 2^128,beta = 0.4)

if x:

m = m\_high + x[0]

print((int(m)))

得到m=3402789736593180236658155503802934243882633217001276110520820253391839278880462965966606922621

然后用python转换为字节输出即可

Flag：hgame{c0ppr3smith\_St3re0typed\_m3ssag3s}

题目四：babyRSA

解题过程：#这是题目

from Crypto.Util.number import \*  
from secret import flag,e  
m=bytes\_to\_long(flag)  
p=getPrime(64)  
q=getPrime(256)  
n=p\*\*4\*q  
k=getPrime(16)  
gift=pow(e+114514+p\*\*k,0x10001,p)  
c=pow(m,e,n)  
print(f'p={p}')  
print(f'q={q}')  
print(f'c={c}')  
print(f'gift={gift}')  
"""  
p=14213355454944773291  
q=61843562051620700386348551175371930486064978441159200765618339743764001033297  
c=105002138722466946495936638656038214000043475751639025085255113965088749272461906892586616250264922348192496597986452786281151156436229574065193965422841  
gift=9751789326354522940  
"""

# 这是脚本

from Crypto.Util.number import \*  
import gmpy2  
p= 14213355454944773291  
q=61843562051620780386348551175371930486064978441159200765618339743764001033297  
c=10500213872246694649593663865603821408804347575163902508525511396508874927246190689258  
gift = 9751789326354522940  
  
n= p\*\*4\*q  
d= gmpy2.invert(65537,p-1)  
temp = pow(gift,d,p)  
e= temp - 11451413  
phi = p\*\*3\*(p-1)\*(q-1)  
print(gmpy2.gcd(e,phi))

#73561  
res = Zmod(n)(c).nth root(e, all=True)  
for m in res:  
 flag = long\_to\_bytes(int(m))  
 if b"hgame" in flag:  
 print(flag)  
 break

刚开始我们可以试求出e，但是这时候我们发现求不出结果，用print(gmpy2.gcd(e,phi))，发现e与phi不互素，所以上google查找各种办法，让我找到了一个类似的方法输出e=73561，最后利用sage碰出来，这里依旧是使用sage

Flag：hqame{Adleman\_Mand3r\_Miller\_M3thed}