InfantRSA[已完成]

描述

真*签到题

p = 681782737450022065655472455411;

q = 675274897132088253519831953441;

e = 13;

c = pow(m,e,p*q) = 27569846508236107014517368841149631154217290260855985901984 1

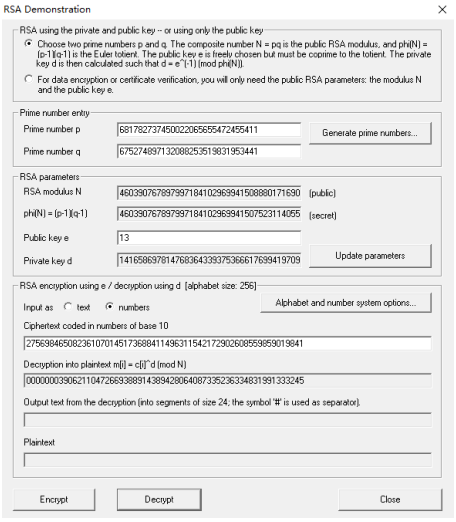
题目地址 https://paste.ubuntu.com/p/9hVzhnxqPc/

基准分数 50

当前分数 50

完成人数 183

基础的 RSA 密码



拿到工具里解密一下 将十进制转化为字符串

hgame{t3Xt6O0k_R5A!!!}

Affine[已完成]

描述

Some basic modular arithmetic...

题目地址 http://hgame-static.n3ko.co/week1/Affine_task.py

基准分数 75

当前分数 75

完成人数 131

```
#!/usr/bin/env python3
# -*- coding: utf-8 -*-
import gmpy2
from secret import A, B, flag
assert flag.startswith('hgame{') and flag.endswith('}')

TABLE = 'zxcvbnmasdfghjklqwertyuiop1234567890QWERTYUIOPASDFGHJKLZXCVBNM'
MOD = len(TABLE)

cipher = ''
for b in flag:
    i = TABLE.find(b)
    if i == -1:
        cipher += b
    else:
        ii = (A*i + B) % MOD
        cipher += TABLE[ii]

print(cipher)
# A8I5z{xr1A_J7ha_vG_TpH410}
```

分析加密代码 还原代码如下

```
#!/usr/bin/env python3
# -*- coding: utf-8 -*-

# A = 13, B = 14, a = 105
TABLE = 'zxcvbnmasdfghjklqwertyuiop1234567890QWERTYUIOPASDFGHJKLZXCVBNM'
MOD = len(TABLE)
cipher = 'A8I5z{xr1A_J7ha_vG_TpH410}'
B = 14
a = 105

plaintext = ''
for b in cipher:
    i = TABLE.find(b)
    if i == -1:
        plaintext += b
    else:
        ii = a * (i - B) % MOD
        plaintext += TABLE[ii]
print(plaintext)
```

hgame{M4th_u5Ed_iN_cRYpt0}

not_One-time[已完成]

描述

In cryptography, the one-time pad (OTP) is an encryption technique that cannot be cracked, but...

Just XOR ;P

nc 47.98.192.231 25001

hint: reduced key space

题目地址 http://hgame-static.n3ko.co/week1/not_One-time_task.py

基准分数 150

当前分数 150

完成人数 45

```
#!/usr/bin/env python3
# -*- coding: utf-8 -*-
import os, random
import string, binascii, base64


from secret import flag
assert flag.startswith(b'hgame{') and flag.endswith(b'}')

flag_len = len(flag)

def xor(s1, s2):
    #assert len(s1)==len(s2)
    return bytes( map( (lambda x: x[0]^x[1]), zip(s1, s2) ) )

random.seed( os.urandom(8) )
keystream = ''.join( [ random.choice(string.ascii_letters+string.digits) for _ in range(flag_len) ] )
keystream = keystream.encode()
print( base64.b64encode(xor(flag, keystream)).decode() )
```

异或加密 密钥范围已知 密钥长度与明文相同

选取五十组密文 逐个字符与密钥范围逐个异或 取交集

```
h
hg
hga
hgam
hgame
hgame{
hgame{z
hgame{zr
hgame{zr3
hgame{zr3u
hgame{zr3us
hgame{zr3us1
hgame{zr3usln
hgame{zr3uslnG
hgame{zr3uslnG+
hgame{zr3uslnG+M
hgame{zr3uslnG+M3
hgame{zr3uslnG+M3$
hgame{zr3uslnG+M3$5
hgame{zr3uslnG+M3$5a
hgame{zr3uslnG+M3$5ag
hgame{zr3uslnG+M3$5age
hgame{zr3uslnG+M3$5age-
hgame{zr3uslnG+M3$5age-&
hgame{zr3uslnG+M3$5age-&&
hgame{zr3uslnG+M3$5age-&&~
hgame{zr3uslnG+M3$5age-&&~r
hgame{zr3uslnG+M3$5age-&&~rE
hgame{zr3uslnG+M3$5age-&&~rEd
hgame{zr3uslnG+M3$5age-&&~rEdu
hgame{zr3uslnG+M3$5age-&&~rEduC
hgame{zr3uslnG+M3$5age-&&~rEduC23
hgame{zr3uslnG+M3$5age-&&~rEduC23d
hgame{zr3uslnG+M3$5age-&&~rEduC23d_
hgame{zr3uslnG+M3$5age-&&~rEduC23d_k
hgame{zr3uslnG+M3$5age-&&~rEduC23d_k3
hgame{zr3uslnG+M3$5age-&&~rEduC23d_k3Y
hgame{zr3uslnG+M3$5age-&&~rEduC23d_k3Y-
hgame{zr3uslnG+M3$5age-&&~rEduC23d_k3Y-5
hgame{zr3uslnG+M3$5age-&&~rEduC23d_k3Y-5P
hgame{zr3uslnG+M3$5age-&&~rEduC23d_k3Y-5P4
hgame{zr3uslnG+M3$5age-&&~rEduC23d_k3Y-5P4C
hgame{zr3uslnG+M3$5age-&&~rEduC23d_k3Y-5P4Ce
hgame{zr3uslnG+M3$5age-&&~rEduC23d_k3Y-5P4Ce}
hgame{zr3uslnG+M3$5age-&&~rEduC23d_k3Y-5P4Ce}
Press any key to continue . . .
```

选取的组数不足有两个字符未完全确定 但只有两种可能

hgame{r3us1nG+M3$5age-&&~rEduC3d_k3Y-5P4Ce}

Reorder[已完成]

描述

We found a secret oracle and it looks like it will encrypt your input...

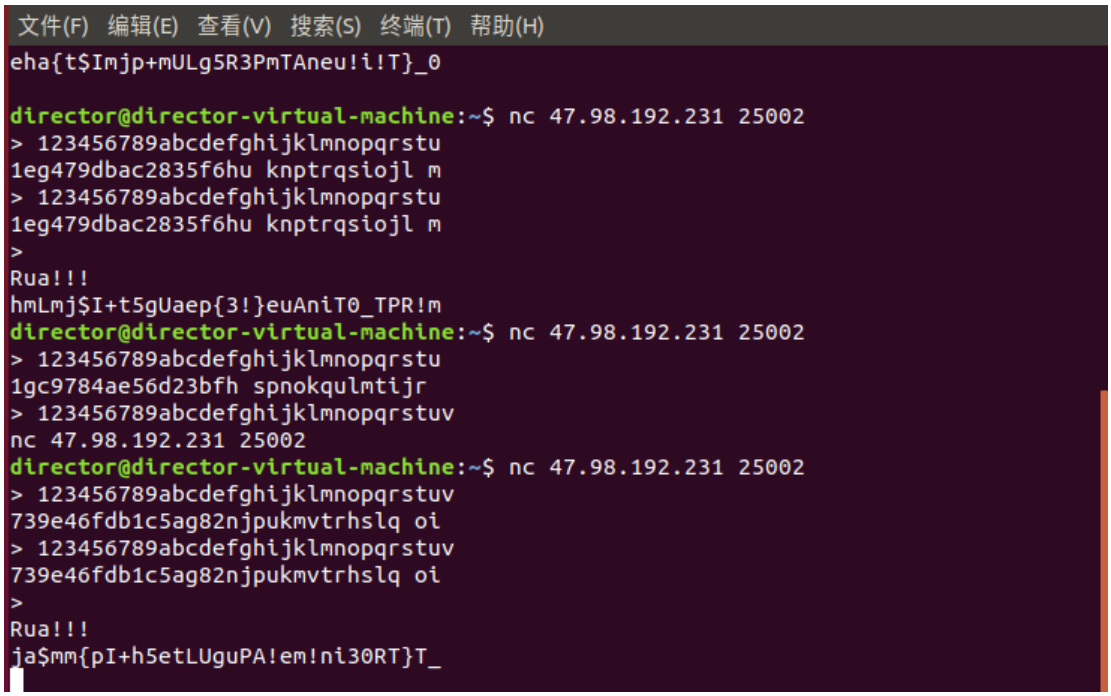
nc 47.98.192.231 25002

题目地址 https://www.baidu.com

基准分数 75

当前分数 75

完成人数 91



测试后发现每次链接后 所得加密方式均不同 输入不同的字符根据加密方式倒推明文

hgame{jU$t+5ImpL3_PeRmuTATi0n!!}

欢迎参加HGame！[已完成]

描述

欢迎大家参加 HGAME 2020！

来来来，签个到吧～

Li0tIC4uLi0tIC4tLi4gLS4tLiAtLS0tLSAtLSAuIC4uLS0uLSAtIC0tLSAuLi0tLi0gLi4tLS0gLS0tLS0gLi4tLS0gLS0tLS0gLi4tLS4tIC4uLi4gLS0uIC4tIC0tIC4uLi0t

注：若解题得到的是无hgame{}字样的flag花括号内内容，请手动添加hgame{}后提交。

【Notice】解出来的字母均为大写

题目地址 https://www.baidu.com

基准分数 50

当前分数 50

完成人数 433

Base64 密码 摩斯密码

hgame{W3LC0ME_TO_2020_HGAM3}

壁纸[已完成]

描述

某天，ObjectNotFound给你发来了一个压缩包。

“给你一张我的新老婆的壁纸！怎样，好看吗？”

正当你疑惑不解的时候，你突然注意到了压缩文件的名字——“Secret”。

莫非其中暗藏玄机？

题目地址 http://oss-east.zhouweitong.site/hgame2020/week1/Secret_QsqPIFOPp8urcgwTszHT06HmsGYetoGy.zip

基准分数 75

当前分数 75

完成人数 295

```
Microsoft Windows [版本 10.0.17763.973]
(c) 2018 Microsoft Corporation。保留所有权利。

C:\Users\Director>binwalk C:\Users\Director\Desktop\HGAME\W12\Pixiv@纯白可憐.jpg
* suggest: you'd better to input the parameters enclosed in double quotes.
* made by pcat

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
30            0x1E            TIFF image data, big-endian, offset of first image directory: 8
1320930       0x1427E2        Zip archive data, encrypted at least v2.0 to extract, compressed size: 80, uncompressed si
ze: 108, name: flag.txt
1321138       0x1428B2        End of Zip archive, footer length: 45, comment: "Password is picture ID."


C:\Users\Director>_
```

压缩包里的图片用 binwalk 分析一下 分解出来一个压缩包

解压密码 picture ID（图片来源于 P 站）

解压一个文本文件 内容为 Unicode 编码 转中文

hgame{Do_y0u_KnOW_uNiC0d3?}

克苏鲁神话[已完成]

描述

ObjectNotFound几天前随手从Cosmos电脑桌面上复制下来的文件。

唔，好像里面有什么不得了的东西。

【hint1】请使用7zip。另外，加密的zip是无法解出密码的。

题目地址 http://oss-east.zhouweitong.site/hgame2020/week1/Cthulhu_lzWIREHNWbPveclo8wZrNBL9LOat8yO9.zip

基准分数 100

当前分数 100

完成人数 96

明文破解 解压出来 doc 文件打开密码是 txt 文件的培根密码（FLAGHIDDENINDOC）

Doc 文件里取消隐藏

hgame{Y0u_h@Ve_F0Und_mY_S3cReT}

签到题ProPlus[已完成]

描述

什么什么，签到题太简单没过瘾？

来来来，试试咱ObjectNotFound亲手做的这一道，包您满意！

【拼写错误修正】fenses -> fences

题目地址 http://oss-east.zhouweitong.site/hgame2020/week1/SignInProPlus_eEH43ZcCHfqS1XVW1mIVliBWBaD8juVI.zip

基准分数 150

当前分数 150

完成人数 169

Password 根据提示先栅栏后凯撒 得到解压密码 EAVMUBAQHQMVEPDT

Ook 解密 base32 解密 base64 解密 得到 png 的二进制数据复制进 txt 文件修改文件后缀名

hgame{3Nc0dInG_@IL_iN_0Ne!}

每日推荐[已完成]

描述

~~“这是一个，E99p1ant和ObjectNotFound之间发生的故事。”~~

~~“事情，还要从一个风和日丽的下午说起。ObjectNotFound正听着网易云每日推荐…”~~

算了算了，想不出什么题目介绍了，就这样吧。

题目地址 http://oss-east.zhouweitong.site/hgame2020/week1/Recommendation_0ddwpplx1thGhquA9kf0lGDHR4EFr1Y4.zip

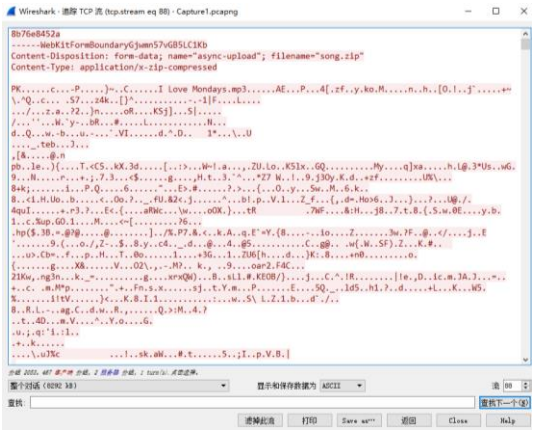
基准分数 100

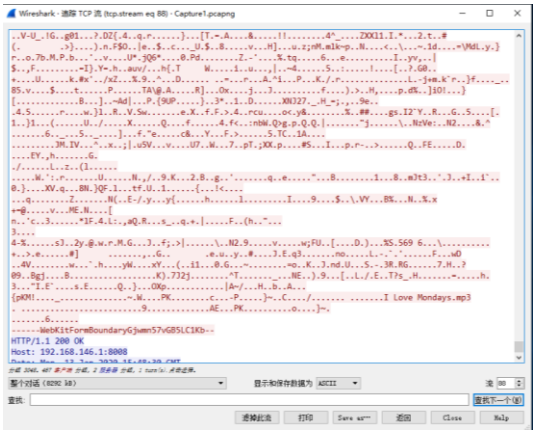
当前分数 100

完成人数 87

```
975142      0xEE126         GIF image data, version "89a", 416 x 26
994933      0xF2E75         HTML document header
995052      0xF2EEC         HTML document header
1097801     0x10C049        HTML document footer
1123187     0x112373        Copyright string: "Copyright 2010-2017, John Dyer (http://j.hn/)"
1490573     0x16BE8D        HTML document header
1491021     0x16C04D        HTML document footer
1637286     0x18FBA6        Copyright string: "Copyright (c) 2012 Yannick Albert (http://yckart.com)"
1637479     0x18FC67        Base64 standard index table
1678778     0x199DBA        GIF image data, version "89a", 20 x 20
1684386     0x19B3A2        PNG image, 48 x 64, 8-bit grayscale, non-interlaced
1688982     0x19C596        Zip archive data, encrypted at least v2.0 to extract, compressed size: 8289673, uncompress
ed size: 9388953, name: I Love Mondays.mp3
10075785    0x99BE89        HTML document header
10075904    0x99BF00        HTML document header
10451145    0x9F78C9        HTML document footer
10666376    0xA2C188        Copyright string: "Copyright jQuery Foundation and other contributors"
10670574    0xA2D1EE        Copyright string: "Copyright jQuery Foundation and other contributors"
10678201    0xA2EFB9        Copyright string: "Copyright jQuery Foundation and other contributors"
10681608    0xA2FD08        Copyright string: "Copyright jQuery Foundation and other contributors"
10867211    0xA5D20B        Copyright string: "Copyright 2010-2017, John Dyer (http://j.hn/)"
11233786    0xAB69FA        Copyright string: "Copyright (c) Facebook, Inc. and its affiliates."
11249666    0xABA802        Copyright string: "Copyright (c) Facebook, Inc. and its affiliates."
11487263    0xAF481F        HTML document header
11534649    0xB00139        HTML document footer
11710364    0xB2AF9C        Copyright string: "Copyright (c) 2017 Jed Watson."
11762002    0xB37952        Copyright string: "Copyright (c) 2017 Jed Watson."
11949627    0xB6563B        Ubiquiti firmware header, third party, "CRC32: 0xC0600, version: "_UP&&(i=-(window.innerHe
ight-o.bottom));t===r.ANCHOR_RIGHT&&(a=-(window.innerWidth-o.right));return{transform:"translate3d("+Str"
12116352    0xB8E180        Copyright string: "Copyright (c) Facebook, Inc. and its affiliates."
```

Binwalk 分析 发现里面有一个 zip 压缩包





Wireshark TCP 追踪到压缩包的开头和结尾 用十六进制编辑器取出

解压密码提示为 6 位数字 直接暴力破解

音频文件用 Au 打开显示频谱得到 flag

hgame{I_love_EDM233}