

Crypto

Verification\_code

sha256 加密密文前四位未知暴力破解程序有 60 秒的限制还有验证码 考验手速的时候到了  
(奈何本人菜的真实)

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

import string, random
from hashlib import sha256

a = 'sha256(XXXX+aMJwX0l40xtmkCvS) == 6efc9feab7e913eaf9eecaab5d0f5f15df50adc7f104762192e49655e07351aa'

_hexdigest = a[33:]
key = string.ascii_letters+string.digits
proof = a[12:28]
x = ''

for t1 in key:
    for t2 in key:
        for t3 in key:
            for t4 in key:
                x = t1 + t2 + t3 + t4
                if sha256(x.encode()+ proof.encode()).hexdigest() == _hexdigest:
                    print (x)
```

```
director@director-virtual-machine:~$ nc 47.98.192.231 25678
sha256(XXXX+aMJwX0l40xtmkCvS) == 6efc9feab7e913eaf9eecaab5d0f5f15df50adc7f104762
192e49655e07351aa
Give me XXXX: Gwti
The secret code?
> I like playing Hgame
Ok, you find me.
Here is the flag: hgame{It3Rt00|S+I5_u$3fu1~Fo2_6rUtE-f0Rc3}
Bye~
```

Remainder

中国剩余定理 RSA (N 由多素数组成)

```
from Crypto.Util import number

e = 65537
# p
p = 945982963057133766525404116319494343013962351116733727382767546541882670108055225420680044531376785988913354081702776013819445842
# q
q = 150088216417404963893679242888992998793257903343994792697939121738029477790454833496600101388493792476973514786401036309378542808
# r
r = 145897736096689096151704740327665176308625097484116713780050311198775607465862066406830851710261868913835866335107146242979359964

c1 = 78430786011650521224561924814843614294806974988599591058915520397518526296422791089692107488534157589856611229978068659970976374
c2 = 49576356423474222188205187306884167620746479677590121213791093908977295803476203510001060180959190917276817541142411523867555147
c3 = 48131077962649497833189292637861442767562147447040134411078884485513840553188185954383330236190253388937785530658279768620213062

N = p * q * r
c0_t0_N0 = c1 * int(gmpy2.invert(q * r, p)) * (q * r)
c1_t1_N1 = c2 * int(gmpy2.invert(p * r, q)) * (p * r)
c2_t2_N2 = c3 * int(gmpy2.invert(p * q, r)) * (p * q)
c = (c0_t0_N0 + c1_t1_N1 + c2_t2_N2) % N

d = int(gmpy2.invert(e, ((p - 1) * (q - 1) * (r - 1))))
m = pow(c, d, N)
m = number.long_to_bytes(m)

print(m)

b'\n!hAyuFoUCamGW9BP7pGKCG811SEnwAOM8x\n***** DO NOT GUESS ME *****\nhg In number theory, \nam the Chinese \ne{ remainder
theorem \nCr states that if one\nT_ knows the \nw0 remainders of the \nNt Euclidean division\n+6 of an integer n \nOt by severa
l \nh3 integers, then \nR_ YOU CAN FIND THE \nmE FLAG, ;D\n!! \n!} \n***** USE YOUR BRAIN *****\ncl18KukOPUvpoe1LCpBchXHJ
TgmDknbFE2z\n'
Press any key to continue . . .
```

hgame{CrT\_w0Nt+6Oth3R\_mE!!!}

Inv

$n$  是满足  $\text{Pow}(c_1, n_1+1) = c_1 \text{ Pow}(c_2, n_2+1) = c_2$  的  $n_1, n_2$  最小公倍数  
模仿 RSA 的共模攻击

```
def Pow(X, E):
    Y = X
    E = bin(E)[3:]
    for e in E:
        Y = Mul(Y, Y)
        if e == '1':
            Y = Mul(X, Y)
    return Y

c1 = b'\xc8\xce\xbe*\xc5\x84\xdb\x05\x9b\x02\xac/\x0b\x8d'\xc2b\x89\x93\x86\xcd\x01\x1b\x44\xffa\x90\xaf, (\xae?\xa8\xa0\x8b\xfb\x97\x1n\x86fj\x074\x7fb0\xdc
c2 = b'U\x17\x8aB\xa0\x19\xab\x7fd0\x02)\xc0\xae\xcc/G_\xe3'\r\xfb\xaf\x00\xbihg1-\xc1\xffa\x8d\t8\x99k\x95\x93\xa8, \x07\xcd\x87\x01\x89\x86\xfbf48f\xdc \x90\xdc4

e1 = 595
e2 = 739

#n = 48720
def gcdext(x, y):
    for i in range(1000):
        for j in range(500):
            if 1 == ((x * i) + (y * j)) % 48720:
                return (i, j)

s, t = gcdext(e1, e2)
#sbox
sbox = Mul(Pow(c1, s), Pow(c2, t))

flag_c = b'\-\xa5{\xb9\x85J @\xfa\x91\x0b\x88\r4f\x89\xe5\r\x0\x84\x8f\xa0\x0i\xb0\xa4\x1b\x8fiw\x84'\xa2\xa4\x00\x91\x87\x10\r\\\x8c\x12'

j = -1
flag = ''
for i in flag_c:
    for k in sbox:
        j += 1
        if i == k:
            flag += chr(j)
            j = -1
            break
print(flag)
```

hgame{U\_kN0w~tH3+eXtEnD-EuC1d34n^A1G0rlthM}

notRC4

从最后开始逻辑倒退 纯脑力劳作

```
00 = [58, 246, 2, 113, 254, 127, 155, 66, 83, 172, 175, 176, 170, 106, 1, 178, 201, 99, 217, 96, 156, 101, 130, 236, 136, 245, 86, 116, 82, 230, 139, 210, 103, 179, 152]
flag_c = b'\xb8\xb3\x12\x0c\x0b\x12\xf090\xb3\x18\xea\x9c\x04\x98\x9e\x7f\x1d\x9a\xaf\x96\xea\x0e\xce\x83\xea\x1d\x19\x9a\x05\xbcH\x97\x82I\x9e'
len(flag_c) = 50
0 = []
key = 0
t = -1
for i in 00:
    t += 1
    if xor(bytes([i]), bytes([flag_c[49]])) == b'':
        key = i
        break
0.append(00[t])
0oo = 50
o00 = 0
for o00_1 in range(256):
    if t == (00[0oo] + 00[o00_1]) % 256:
        o00 = o00_1
        00[0oo], 00[o00] = 00[o00], 00[0oo]
        for o00_1 in range(256):
            if o00 == (o00_1 + 00[0oo]) % 256:
                o00 = o00_1
                break
        break
for 0oo in range(49, 0, -1):
    t = (00[0oo] + 00[o00]) % 256
    0.append(00[t])
    00[0oo], 00[o00] = 00[o00], 00[0oo]
    for o00_1 in range(256):
        if o00 == (o00_1 + 00[0oo]) % 256:
            o00 = o00_1
            break
flag = ''
for i in range(50):
    flag += str(xor(bytes([0[len(flag_c) - i - 1]]), bytes([flag_c[i]])), encoding = "utf-8")
print (flag)
```

hgame{00OoOO0o\_-REveR\$e~The~prG4-of~RC4\_+O0Oo00O0}

Misc

所见即为假

根据题意 zip 伪加密直接 winrar 修复 获取图片 zip 里提示 F5 并给了 key

```
C:\Users\Director\Desktop\F5\F5-steganography-master>java Extract FLAG_IN_PICTURE.jpg -p N11D7Cqon6dBsFLr
Huffman decoding starts
Permutation starts
10911744 indices shuffled
Extraction starts
Length of embedded file: 222 bytes
(1, 127, 7) code used

C:\Users\Director\Desktop\F5\F5-steganography-master>
```

获取文档内容 猜测为十六进制编码

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	52	61	72	21	1A	07	01	00	33	92	B5	E5	0A	01	05	06	Rar!....3'pã....
0010h:	00	05	01	01	80	80	00	B9	52	7A	EA	24	02	03	0B	A7	....ëë.'Rzê\$...\$
0020h:	00	04	A7	00	20	CB	5B	DC	2D	80	00	00	08	66	6C	61	..\$. Ě[Ü-ě...fla
0030h:	67	2E	74	78	74	0A	03	02	9A	9D	6C	65	DF	CE	D5	01	g.txt...š.leßîŎ.
0040h:	68	67	61	6D	65	7B	34	30	38	37	5E	7A	23	6D	73	77	hgame{4087^z#msw
0050h:	33	34	45	52	74	6E	46	55	79	71	70	4B	55	6B	32	64	34ERtnFUyqpKuk2d
0060h:	6D	4C	50	57	36	30	7D	1D	77	56	51	03	05	04	00		mLPW60}.wVQ....

hgame{4087^z#msw34ERtnFUyqpKuk2dmLPW60}

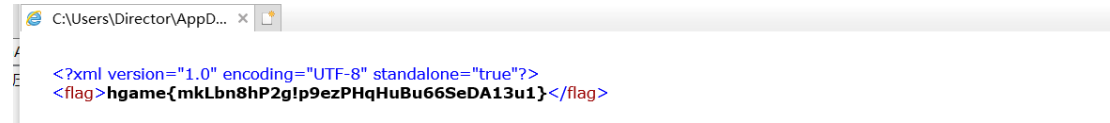
地球上最后的夜晚

打开压缩包一个 pdf 和一个 zip 解压密码隐写在 pdf 中

工具 wbstego43open

获取 zip password: OmR#O12#b3b%s\*IW

用 7.zip 打开 docx 在 secret.xml 里找到 flag

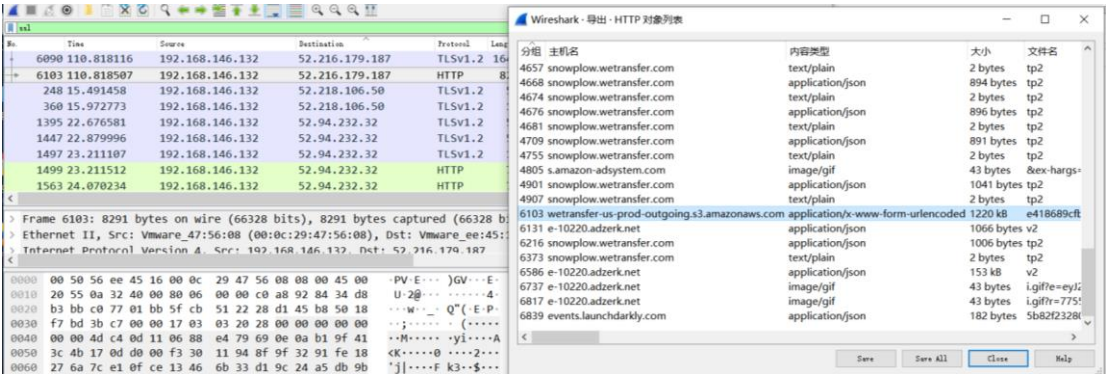
A screenshot of a text editor window. The title bar shows the file path 'C:\Users\Director\AppData...'. The editor contains two lines of XML code. The first line is a standard XML declaration: `<?xml version="1.0" encoding="UTF-8" standalone="true"?>`. The second line is a flag element: `<flag>hgame{mkLbn8hP2g!p9ezPHqHuBu66SeDA13u1}</flag>`. The text is color-coded: the opening and closing tags are blue, the attribute values are black, and the flag content is red.

```
C:\Users\Director\AppData... x
A
E
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
<flag>hgame{mkLbn8hP2g!p9ezPHqHuBu66SeDA13u1}</flag>
```

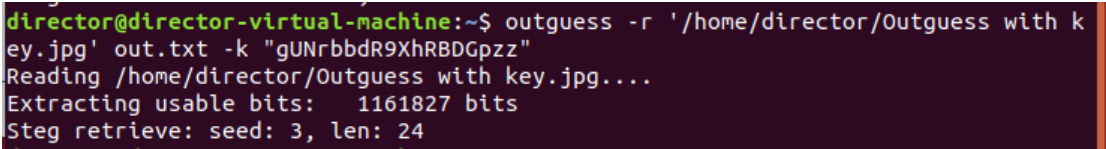
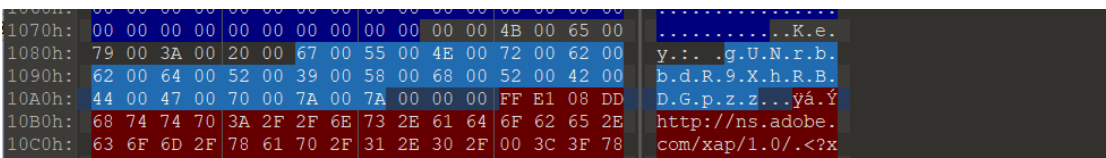
Cosmos 的午餐

Wireshark 导入 ssl

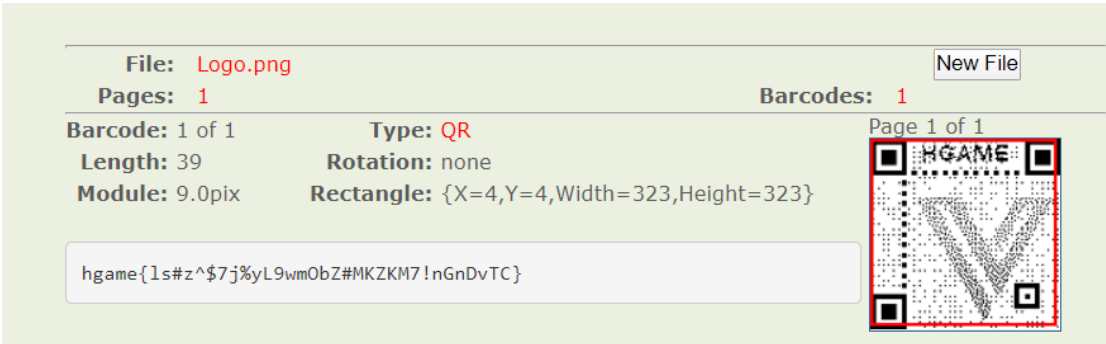
在里面找到压缩包文件 导出修改后缀



图片拿去 outguess key 在十六进制里找到



<https://dwz.cn/69rOREdu> 下载压缩包 扫一扫二维码



玩玩条码

根据提示解码 JPNPostcode 就是视频隐写的解密密码 1087627  
该编码为 Japanese Postal (Customer) Code

工具 VirtualDub2

得到 Zip Password: b8FFQcXsupwOzCe@

扫码可得

