Crypto
RSA?

Rabin 算法的一小部分 n 是素数

```
#-*- coding:utf-8 -*-

from Crypto.Util.number import *

n = 72368347860939160093254172353442842843910502872734220583482413607701314232408072597178646868850123012939213283973911
e = 2
c = 21669064089653901164377611856030756990863152466469821325207928683016154627327076959430587832112335896021624828478742
plaintext = pow(c, (n + 1) // 4, n)
plaintext = long_to_bytes(plaintext)
print (plaintext)
```

hgame{eaa5262c-4631-46ef-a97b-53277ab7e1d8}

ToyCipher_XorShift

反向推导

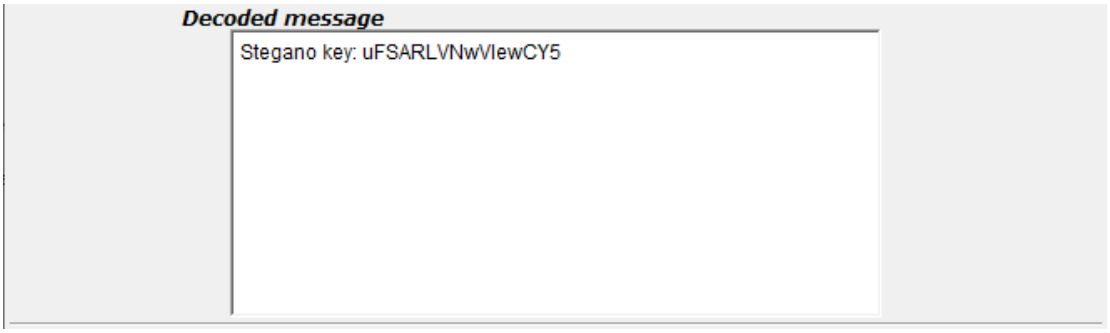
```
MASK = (1 << BITSLENGTH) - 1

BLOCKS = lambda data: [ bytes(data[i*BLOCKSIZE:(i+1)*BLOCKSIZE]) for i in range(len(data)//BLOCKSIZE) ]
XOR = lambda s1, s2: bytes([x^y for x,y in zip(s1, s2)])

def d(x, a, shr=True):
    x = x & MASK
    a = a % BITSLENGTH
    M = (1 << a) - 1
    if shr:
        M = M << (BITSLENGTH - a)
        for i in range((BITSLENGTH // a) + 1):
            x ^= (x & M) >> a
            M = M >> a
    else:
        for i in range((BITSLENGTH // a) + 1):
            x ^= (x & M) << a
            M = M << a
    return x & MASK

def dec(block):
    block = int.from_bytes(block, byteorder='big')
    block = d(block, 17, shr=False)
    block = d(block,  7, shr=True )
    block = d(block, 13, shr=False)
    return block.to_bytes(BLOCKSIZE, byteorder='big')

def decrypt(cipher, iv, unpad=False):
    plaintext = b''
    mid = iv
    for block in BLOCKS(cipher):
        plaintext += XOR(mid, dec(block))
        mid = block
    return plaintext

IV = b'c8C~M0d3'
cipher = binascii.unhexlify(b'15eb80358fe6f89b1802a5f3eb5a6ec6c33dc4f35822fb6e97e0b22be860a28602b35e2930a93ac5')
plaintext = decrypt(cipher, IV)
print (plaintext)
```

hgame{tHi$+4lgOr1thM_i5_3@sY-t0~b2EaK}

Misc

三重隐写

工具：silenteye 文件：You know LSB

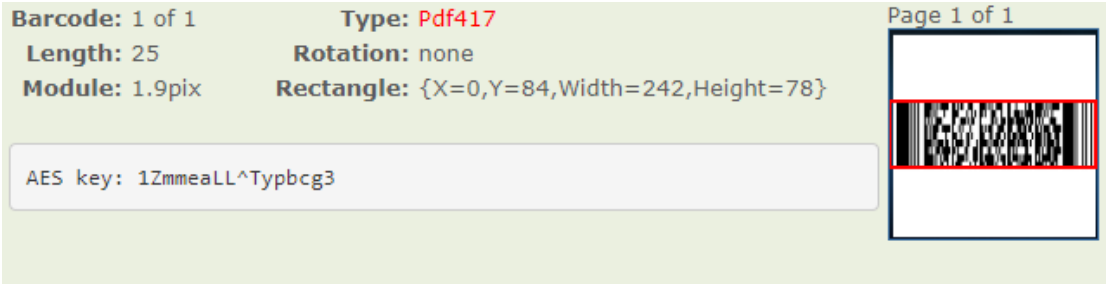


工具：MP3Stego 文件：上裹与手抄卷

```
C:\Users\Director\Desktop\MP3Steg\MP3Stego_1_1_19\MP3Stego>Decode.exe -X C:\Users\Director\Desktop\HGAME\M32\
上裹与手抄卷.mp3 -P uFSARLVNwVIewCY5
MP3StegoEncoder 1.1.19
See README file for copyright info
Input file = 'C:\Users\Director\Desktop\HGAME\M32\上裹与手抄卷.mp3'  output file = 'C:\Users\Director\Desktop\
HGAME\M32\上裹与手抄卷.mp3.pcm'
Will attempt to extract hidden information. Output: C:\Users\Director\Desktop\HGAME\M32\上裹与手抄卷.mp3.txt
The bit stream file C:\Users\Director\Desktop\HGAME\M32\上裹与手抄卷.mp3 is a BINARY file
HDR: s=FFF, id=1, l=1, ep=on, br=2, sf=2, pd=0, pr=1, m=1, js=1, c=1, o=0, e=1
lg.=MPEG-1, layer=I, tot bitrate=64, sfrq=32.0
mode=j-stereo, sblim=32, jsbd=8, ch=2
[Frame     0]Got 1048 bits = 32 slots plus 24
[Frame     1]Got 324424 bits = 10138 slots plus 8
[Frame 9822]Frame cannot be located
Input stream may be empty
Avg slots/frame = 422.031; b/smp = 2.93; br = 129.247 kbps
Decoding of "C:\Users\Director\Desktop\HGAME\M32\上裹与手抄卷.mp3" is finished
The decoded PCM output file name is "C:\Users\Director\Desktop\HGAME\M32\上裹与手抄卷.mp3.pcm"
```

Zip Password: VvLvmGjpJ75GdJDP

文件：Unlasting 封面扫码



工具：Encrypto 文件：flag.crypto key: 1ZmmeaLL^Typbcg3

hgame{i35k#zlewynLC0zfQur!*H9V$JiMVWmL}