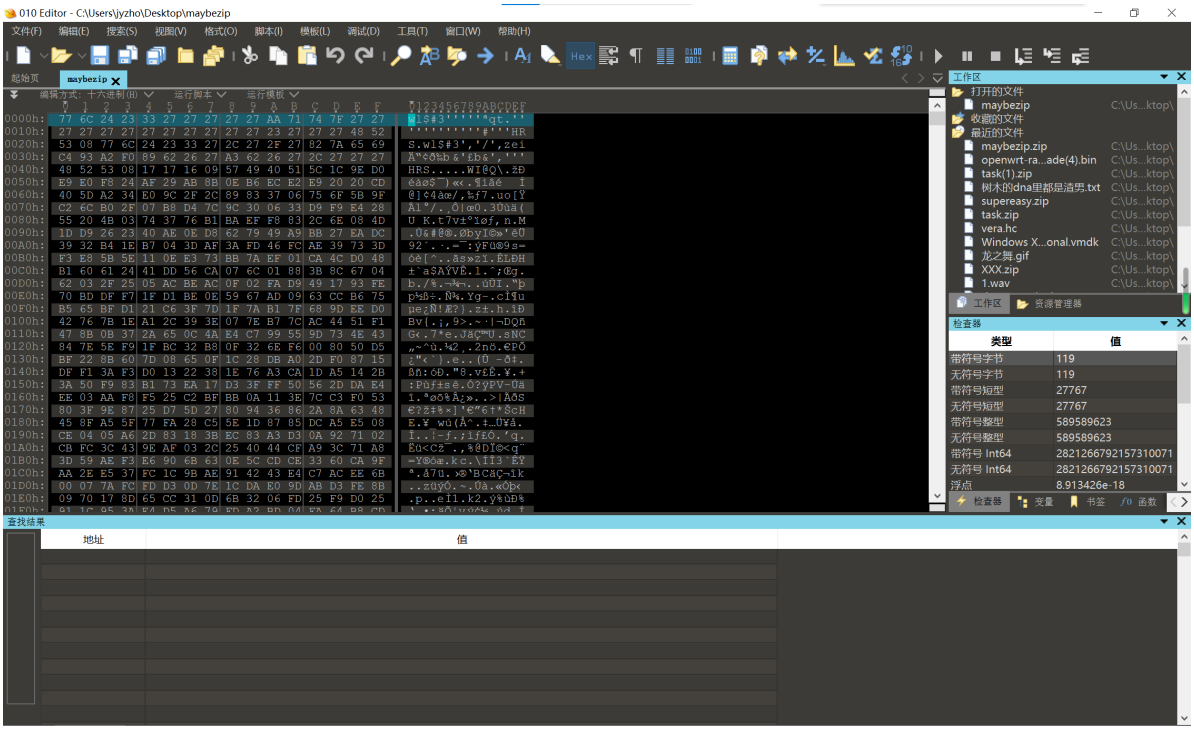
St4rr HGame2024 Week4 Writeup

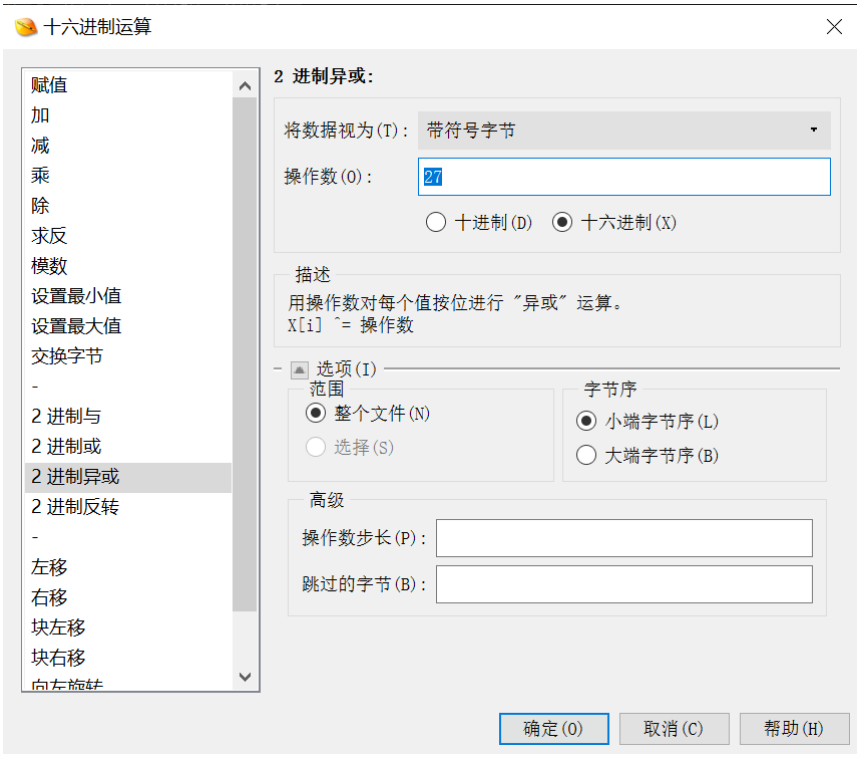
Misc

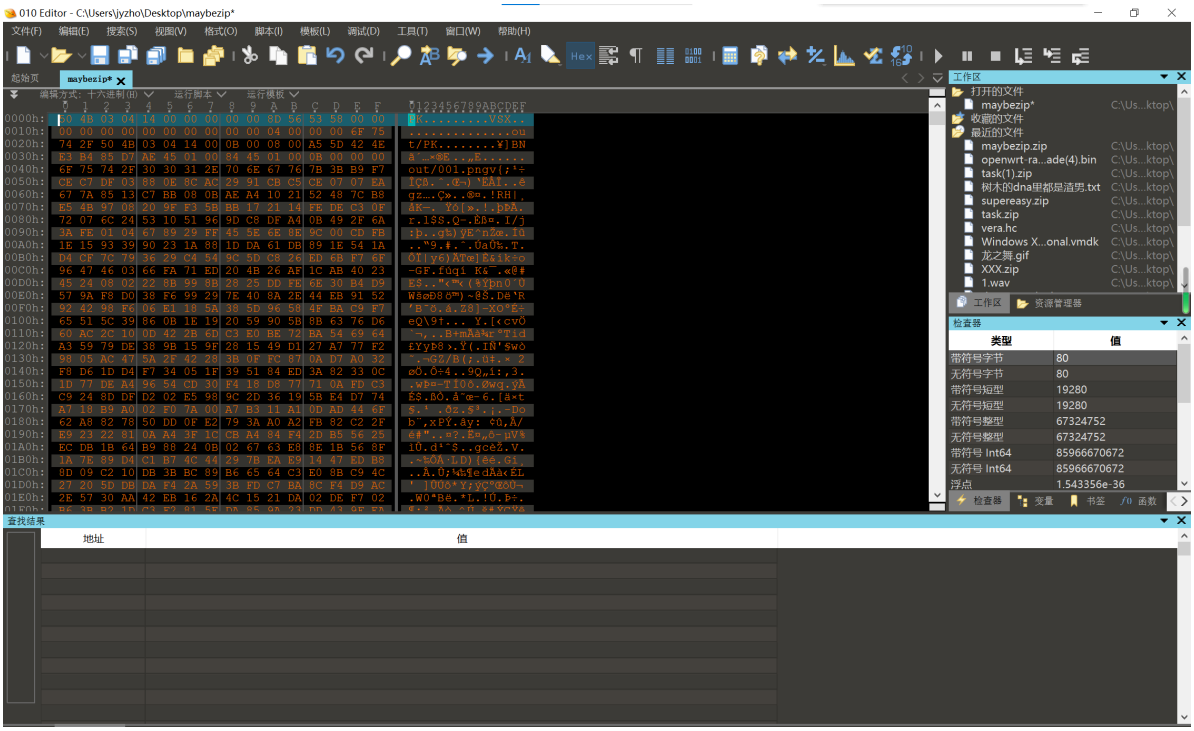
Maybezip

> 一个让人步步惊心的套娃题

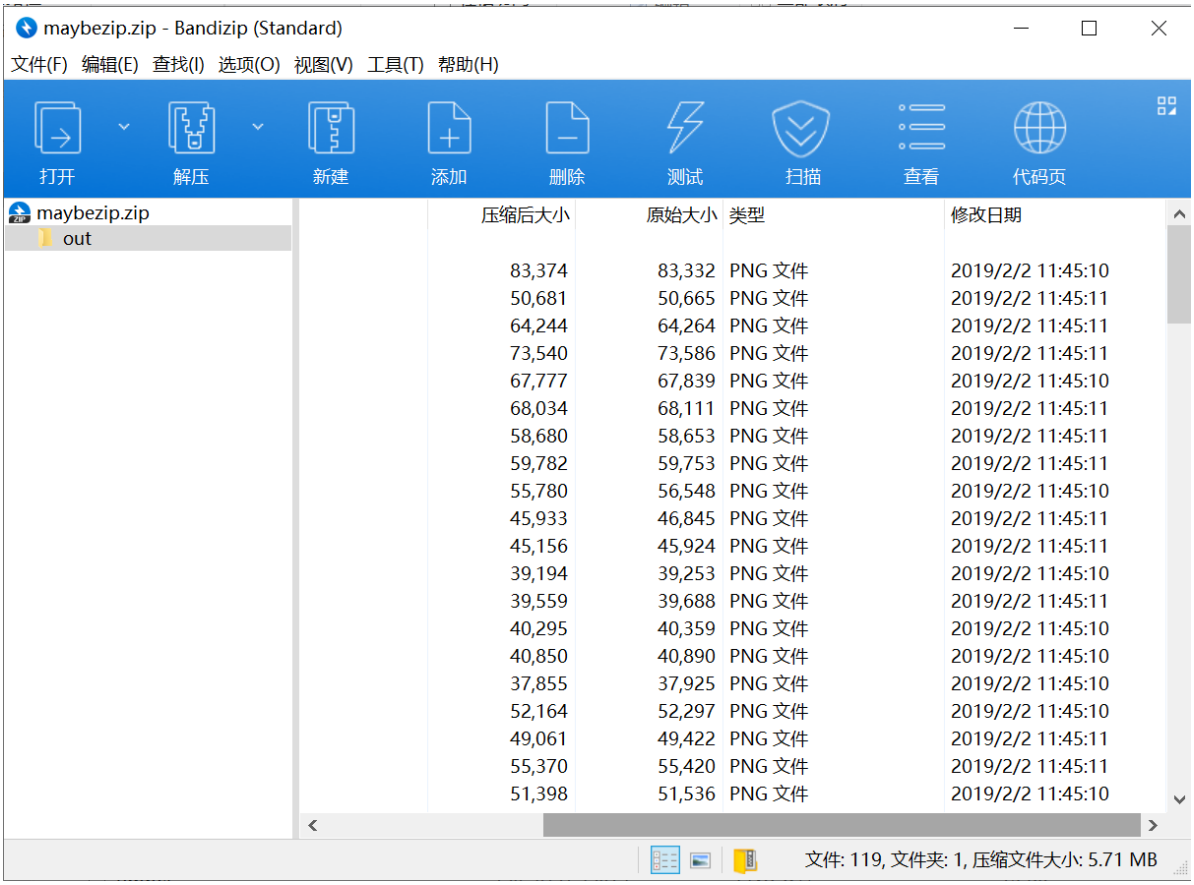
把下载下来的文件放进010里面看一下，发现有很多的27，于是对文件整体异或0x27，看到了zip的格式







然后就卡住了。。。问了一下学长知，这里的时间存在隐写。看了一下，什么11451。。。（警撅）

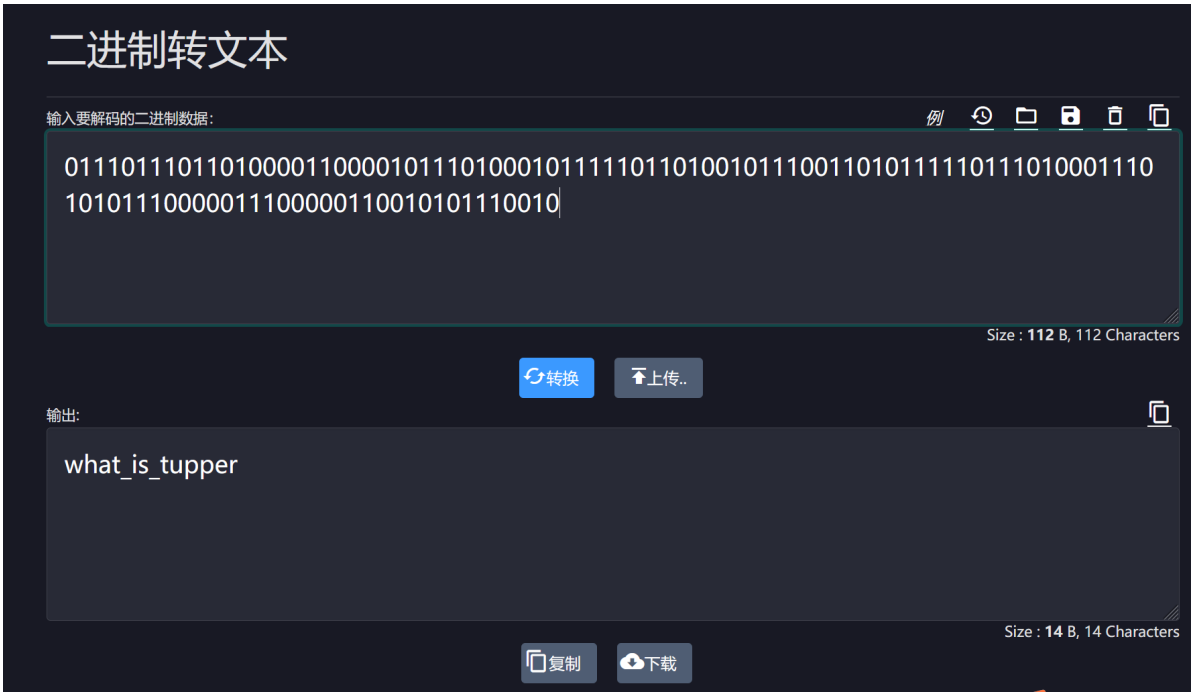


这里的时间只有两种，分别对应0和1，写个脚本提取一下。

```
import zipfile
# 打开ZIP文件
zip_file = zipfile.ZipFile("maybezip.zip")
# 创建一个空列表来存储修改时间
modification_times = []
# 遍历ZIP文件中的所有文件
for info in zip_file.infolist():
    # 获取文件的修改时间并添加到列表中
```

```
    modification_time = info.date_time
    modification_times.append(modification_time)
s=''
for time in modification_times:
    if time==(2019,2,2,11,45,10):
        s+='0'
    elif time==(2019, 2, 2, 11, 45, 12):
        s+='1'
print(s)
# 关闭ZIP文件
zip_file.close()
```

然后二进制转ascii（即每八位转成一个ascii字符），把最后几位多余的舍掉，得到压缩包密码，也是一个hint

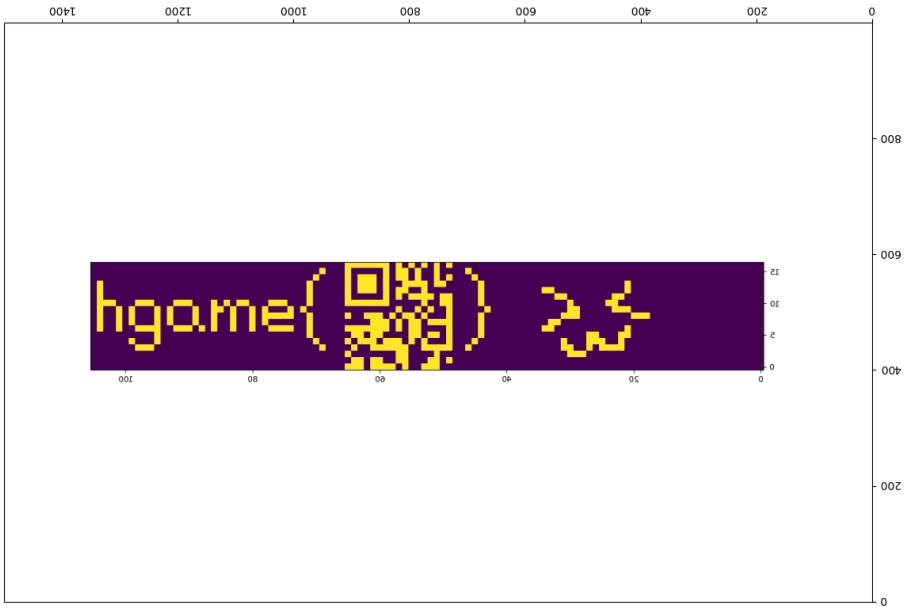


根据hint得知解压出来的文本里那是tupper自指公式的k，脚本画一下图：

```
import numpy as np
import matplotlib.pyplot as plt
from PIL import Image

def Tupper_self_referential_formula(k):
    aa = np.zeros((17,106))
    def f(x, y):
        y += k
        a1 = 2**-(-17*x - y%17)
        a2 = (y // 17) // a1
        return 1 if a2 % 2 > 0.5 else 0
    for y in range(17):
        for x in range(106):
            aa[y, x] = f(x, y)
    return aa[:,::-1]
```

```
k =
727873297223509985235745114810257416958169646355583844422026929393432483103763270305717217904843200256395854960198272246024712870077614739801490049407777475167263979475703878471976846121233972212756378959068016267707257810595403465055834472079348426107367805991580117432922660798728799330070029895439493782746278803718601214016257571571501022474151606674490479186209269816535400587854557894864771334918000721731117447400847754543719414752676119838872
aa = Tupper_self_referential_formula(k)
plt.figure(figsize=(15,10))
plt.imshow(aa,origin='lower')
plt.savefig("tupper.png")
img = Image.open('tupper.png')
#翻转
dst1 = img.transpose(Image.FLIP_LEFT_RIGHT).rotate(180)
plt.imshow(dst1)
plt.show()
```



又在这里卡住了。。。问了一下学长，得知这是个micro qrcode，用μ QR Scanner扫一下得到flag

hgame{Matryo5hk4_d01l}

IOT

ez7621

下载下来的这个名字超长的文件可以用binwalk分离

```
┌──(root㉿DESKTOP-LQMRD0K)-[~]
└─# binwalk -e 1.bin --run-as=root

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0×0             uImage header, header size: 64 bytes, header CRC: 0×4E6924EB, created: 2023-11-14 13:38:11, image size: 2843650 bytes, Data Address: 0×80001000, Entry Po
int: 0×80001000, data CRC: 0×7FC9D6F, OS: Linux, CPU: MIPS, image type: OS Kernel Image, compression type: lzma, image name: "MIPS OpenWrt Linux-5.15.137"
64            0×40            LZMA compressed data, properties: 0×6D, dictionary size: 8388608 bytes, uncompressed size: 9467008 bytes

WARNING: Symlink points outside of the extraction directory: /root/_1.bin.extracted/squashfs-root/usr/bin/scp → /usr/sbin/dropbear; changing link target to /dev/null for security pur
poses.

WARNING: Symlink points outside of the extraction directory: /root/_1.bin.extracted/squashfs-root/usr/bin/ssh → /usr/sbin/dropbear; changing link target to /dev/null for security pur
poses.

WARNING: Symlink points outside of the extraction directory: /root/_1.bin.extracted/squashfs-root/usr/bin/wget → /usr/bin/uclient-fetch; changing link target to /dev/null for securit
y purposes.

WARNING: Symlink points outside of the extraction directory: /root/_1.bin.extracted/squashfs-root/etc/mtab → /proc/17108/mounts; changing link target to /dev/null for security purpos
es.

WARNING: Symlink points outside of the extraction directory: /root/_1.bin.extracted/squashfs-root/etc/resolv.conf → /tmp/resolv.conf; changing link target to /dev/null for security p
urposes.

WARNING: Symlink points outside of the extraction directory: /root/_1.bin.extracted/squashfs-root/etc/localtime → /tmp/localtime; changing link target to /dev/null for security purpo
ses.

WARNING: Symlink points outside of the extraction directory: /root/_1.bin.extracted/squashfs-root/etc/TZ → /tmp/TZ; changing link target to /dev/null for security purposes.

WARNING: Symlink points outside of the extraction directory: /root/_1.bin.extracted/squashfs-root/etc/ssl/cert.pem → /etc/ssl/certs/ca-certificates.crt; changing link target to /dev/
null for security purposes.

WARNING: Symlink points outside of the extraction directory: /root/_1.bin.extracted/squashfs-root/etc/ppp/resolv.conf → /tmp/resolv.conf.ppp; changing link target to /dev/null for se
curity purposes.

WARNING: Symlink points outside of the extraction directory: /root/_1.bin.extracted/squashfs-root/sbin/rmmod → /usr/sbin/kmodloader; changing link target to /dev/null for security pu
rposes.

WARNING: Symlink points outside of the extraction directory: /root/_1.bin.extracted/squashfs-root/sbin/insmod → /usr/sbin/kmodloader; changing link target to /dev/null for security p
urposes.

WARNING: Symlink points outside of the extraction directory: /root/_1.bin.extracted/squashfs-root/sbin/modinfo → /usr/sbin/kmodloader; changing link target to /dev/null for security
purposes.

WARNING: Symlink points outside of the extraction directory: /root/_1.bin.extracted/squashfs-root/sbin/modprobe → /usr/sbin/kmodloader; changing link target to /dev/null for security
 purposes.

WARNING: Symlink points outside of the extraction directory: /root/_1.bin.extracted/squashfs-root/sbin/lsmod → /usr/sbin/kmodloader; changing link target to /dev/null for security pu
rposes.
2843714       0×2B6442        Squashfs filesystem, little endian, version 4.0, compression:xz, size: 3818212 bytes, 1356 inodes, blocksize: 262144 bytes, created: 2023-11-14 13:38:11
```

在分离得到的文件中搜索一下flag，找到一个ko文件看起来有点东西

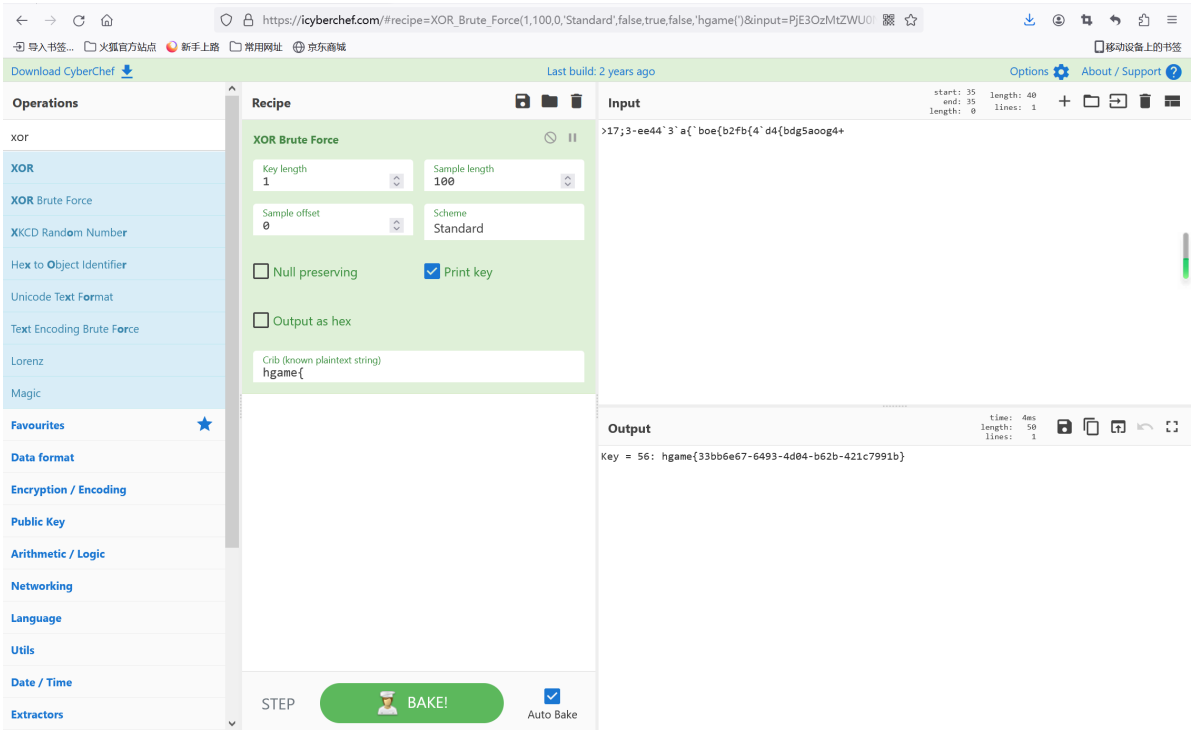
用IDA看一下逻辑，是个异或，整个字符串对0x56异或回去就行

```
addiu   $sp, -0x88
lui     $v0, %hi($LC0)    # ">17;3-ee44`3`a{`boe{b2fb{4`d4{bdg5aoog4"...
sw      $s0, 0x7C+var_s0($sp)
lui     $s0, %hi(__stack_chk_guard)
addiu   $v0, %lo($LC0)    # ">17;3-ee44`3`a{`boe{b2fb{4`d4{bdg5aoog4"...
lw      $a0, __stack_chk_guard
addiu   $v1, $sp, 0x7C+var_68
sw      $s1, 0x7C+var_s4($sp)
sw      $a0, 0x7C+var_8($sp)
sw      $ra, 0x7C+var_s8($sp)
addiu   $a0, $v0, ($LC0+0x20 - 0x148)  # "g5aoog4d44+"
move    $s1, $v1
```

```
addu    $a0, $s1, $v1
lbu     $a1, 0($a0)
addiu   $a0, $sp, 0x7C+var_3C
addu    $a0, $v1
xori    $a1, 0x56
sb      $a1, 0($a0)
b       loc_D0
addiu   $v1, 1
```

```
st=">17;3-ee44`3`a{`boe{b2fb{4`d4{bdg5aoog4+"
s=""
for i in st:
    s+=chr(ord(i)^0x56)
print(s)
```

或者看到这个字符串凭经验可以直接猜测是异或，用cyberchef可以爆破之


https://icyberchef.com/#recipe=XOR_Brute_Force(1,100,0,'Standard',false,true,false,'hgame{')&input=PjE3OzMtZWU0
Download CyberChef
Last build: 2 years ago
Options
About / Support
Operations
xor
XOR
XOR Brute Force
XKCD Random Number
Hex to Object Identifier
Unicode Text Format
Text Encoding Brute Force
Lorenz
Magic
Favourites
Data format
Encryption / Encoding
Public Key
Arithmetic / Logic
Networking
Language
Utils
Date / Time
Extractors
Recipe
XOR Brute Force
Key length
1
Sample length
100
Sample offset
0
Scheme
Standard
Null preserving
Print key
Output as hex
Crib (known plaintext string)
hgame{
STEP
BAKE!
Auto Bake
Input
>17;3-ee44`3`a{`boe{b2fb{4`d4{bdg5aoog4+
Output
Key = 56: hgame{33bb6e67-6493-4d04-b62b-421c7991b}