2024Tangping Cup-冷鹋

博客：http://www.miaoaixuan.cn/

Misc

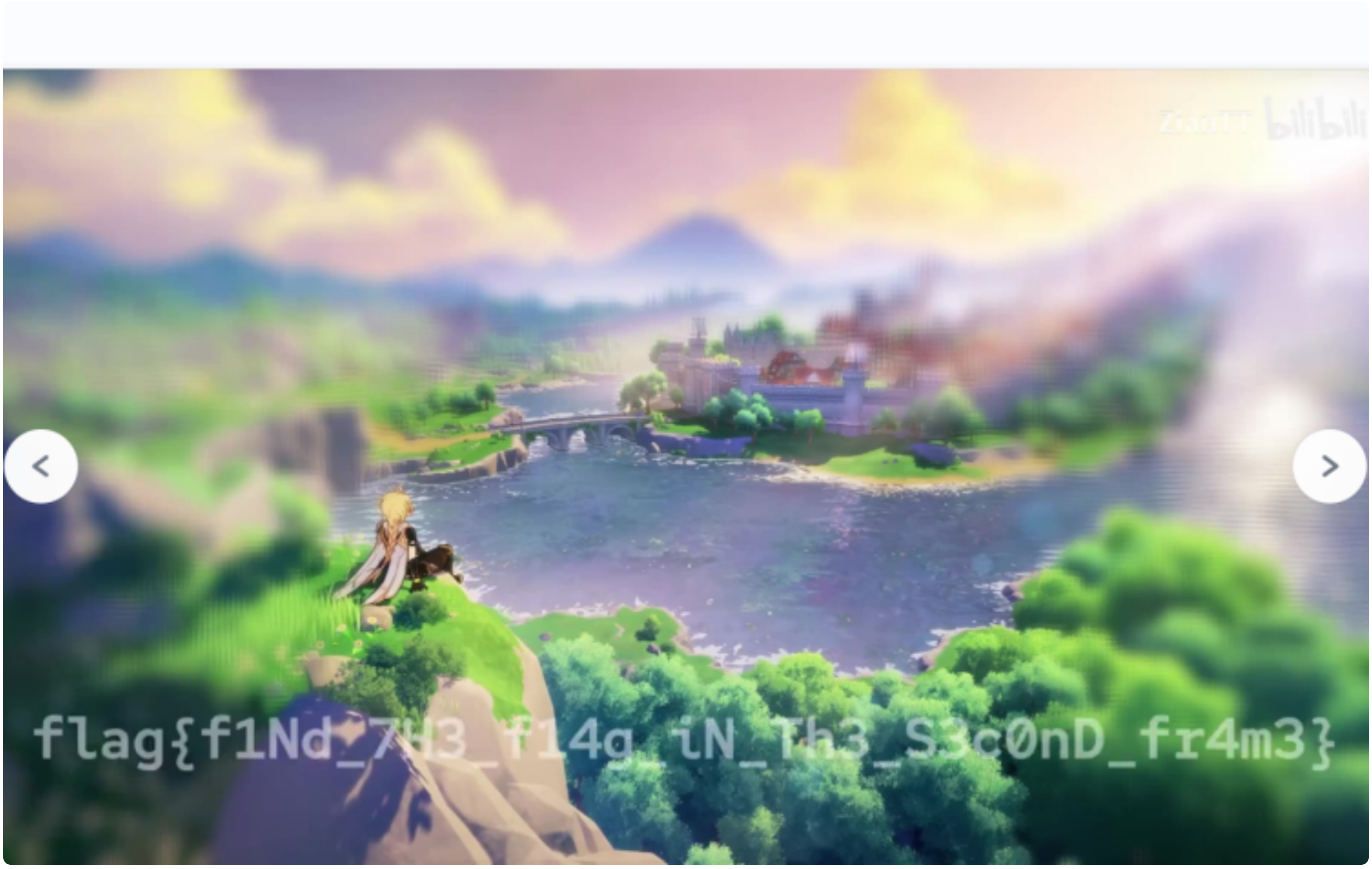
非常好忽悠混合

flag1

通过下载视频发现flag1藏在视频文件名称里

flag2

在视频的第二帧中发现有flag2



心中无码，自然高清

通过枚举分别可打印字符的马赛克图，然后将马赛克flag切片进行脚本比对，可得最终flag

Plain Text

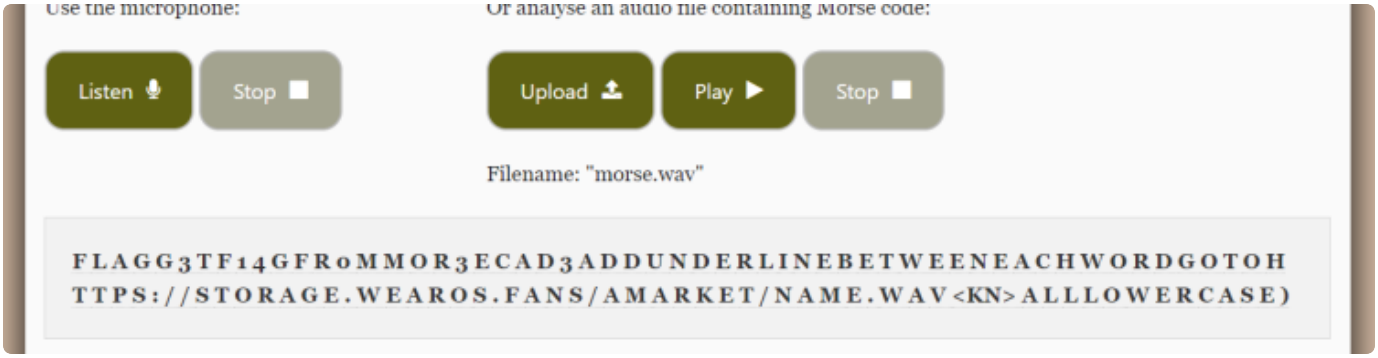
```
from PIL import Image, ImageDraw, ImageFont
import os
import string

# Ensure the output directory exists
output_dir = './mosaic_chars'
if not os.path.exists(output_dir):
    os.makedirs(output_dir)

flag = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz1234567890'

H = 68
W = 30

canvas = Image.new('RGB', (W * len(flag), H), (255, 255, 255))
# Ensure the font path is correct for your system
font = ImageFont.truetype('C:/Users/miaoaixuan/Desktop/JetBrainsMono-Regular.ttf', 50, encoding='utf-8')
pen = ImageDraw.Draw(canvas)
pen.text((0, 0), flag, 'black', font)

def mosaic_img(img: Image.Image, L, H, R, D):
    w, h = R - L, D - H
    a = [0, 0, 0]
    cnt = 0
    for x in range(w):
        for y in range(h):
            j = img.getpixel((L+x, H+y))
            for ch in range(len(a)):
                a[ch] += j[ch]
            cnt += 1
    b = [k//cnt for k in a]
    mosaic = Image.new('RGB', (w, h), tuple(b))
    img.paste(mosaic, (L, H, R, D))

for i in range(len(flag)):
    char = canvas.crop((W * i, 0, W * (i+1), H))
    if 0 <= i < len(flag) :  # Apply mosaic to specified characters
        mosaic_img(canvas, W*i, 0, W*i+W, H//2)
        mosaic_img(canvas, W*i, H//2, W*i+W, H)
    # Save the character image after potentially applying mosaic
    char = canvas.crop((W * i, 0, W * (i+1), H))  # Recrop to get the updated character
    char.save(f'{output_dir}/{flag[i]}_{char.tobytes().__len__()}.png')

```

```
44  canvas.save('flag_censored.png', format='png')
```

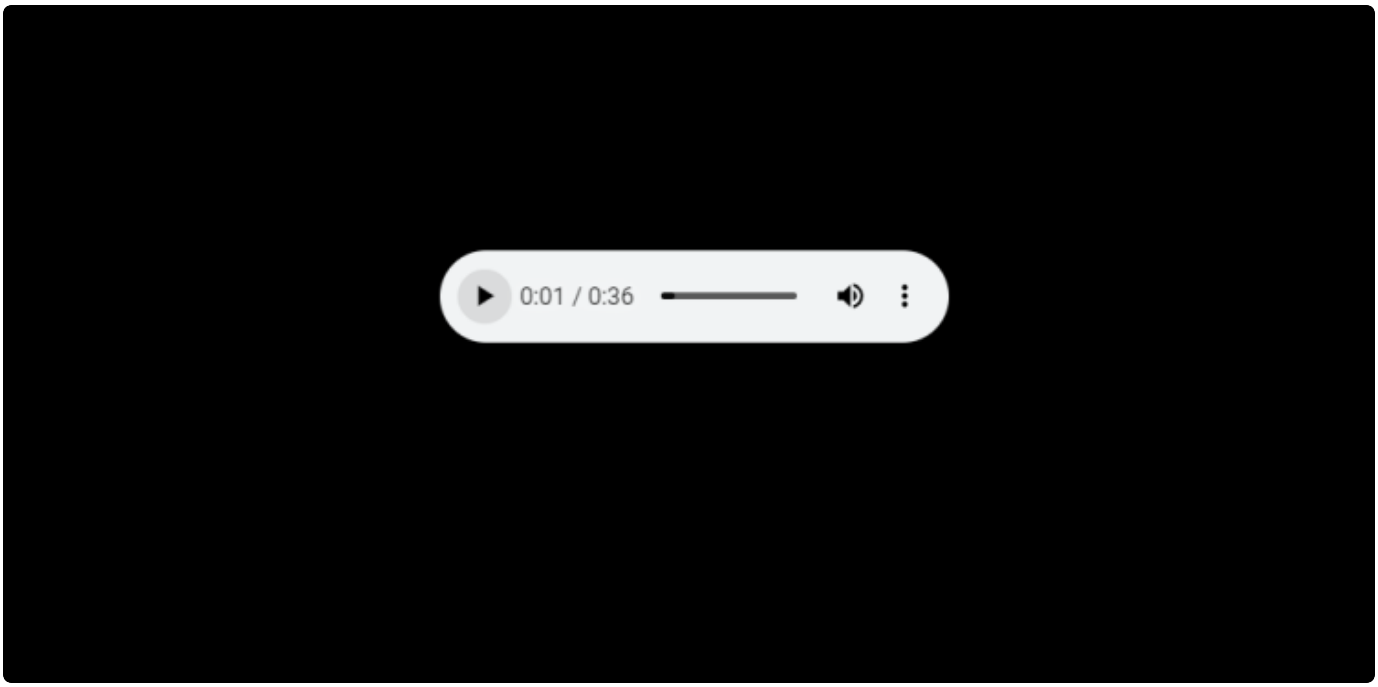
```
import os


def files_are_identical(file1_path, file2_path):
    """逐字节比较两个文件，检查它们是否完全相同"""
    with open(file1_path, 'rb') as file1, open(file2_path, 'rb') as file2:
        while True:
            chunk1 = file1.read(4096)
            chunk2 = file2.read(4096)

            if chunk1 != chunk2:
                return False

            if not chunk1:  # 如果chunk1为空，意味着文件已到末尾
                break

    return True

def compare_file_with_folder(target_file_path, folder_path):
    """比较指定文件与文件夹内所有文件，找出内容完全相同的文件"""
    identical_files = []

    for root, _, files in os.walk(folder_path):
        for filename in files:
            file_path = os.path.join(root, filename)
            if files_are_identical(target_file_path, file_path):
                identical_files.append(file_path)

    return identical_files

def print_identical_files(identical_files):
    """打印所有相同文件的路径"""
    if identical_files:
        print("找到以下相同的文件：")
        for file_path in identical_files:
            print(file_path)
    else:
        print("在文件夹中没有找到相同的文件。")

target_file_path = 'C:/Users/miaoaixuan/Desktop/1/char_23.png'
folder_path = 'C:/Users/miaoaixuan/mosaic_chars'
identical_files = compare_file_with_folder(target_file_path, folder_path)
print_identical_files(identical_files)
```

bepbep

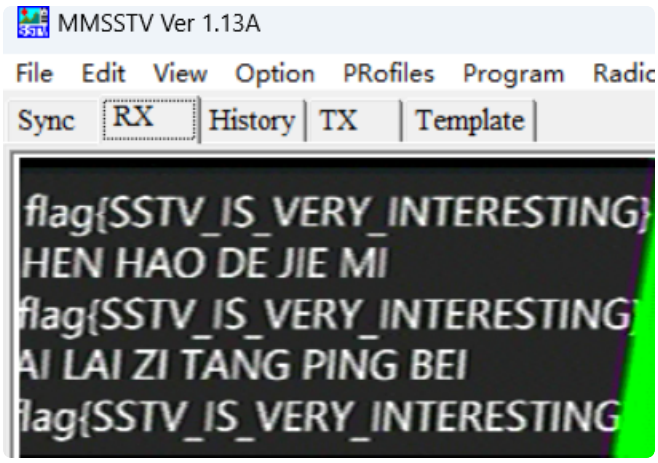
通过摩斯自动网站解密摩斯电码Morse Code Adaptive Audio Decoder | Morse Code World根据要求需要转小写，还要加下划线，得到flag1



Flag1末尾有一网址可得第二段音频,易得sstv解密



sstv解密得flag2



我朝，大盒

通过这几条信息可判断列车的行驶轨迹和旁边高速，再通过路路通程序查询可得车次号

1月25日12:50中国电信 中国沙棘之乡、中国蚕豆之乡、中国绿色名县——“天下贵清康养漳县”欢迎您!微信搜索畅游漳县小程序，了解更多旅游资讯。 [漳县文体广电和旅游局]

1月25日13:40中国电信 “畅游生态陇南乐享康养胜地热情好客的陇南人民欢迎您!更多旅游资讯，请关注“陇南文旅”微信公众号获取。

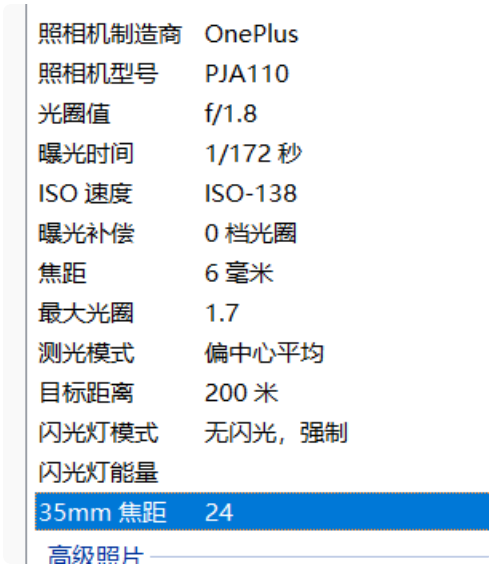
1月25日16:39中国电信 [广元市农民工暨返乡下乡创业工作领导小组办公室]乡亲朋友们您好!为传递省委省政府对全川返乡乡亲们的关心关爱，省农民工办公室牵头首届“天府惜动，向川籍老乡送上新春福利。请通过微信关注“四川农民工服务平台”领取，或登录网址【数据删除】领取，并到就近农民工服务站兑换!。

2:09

D206 动车 共15站　　兰州局兰州段 担当

车站名称	车次	到点	开点	停时	里程
兰州	D206	--:--	11:35	0分	0
岷县	D206	13:19	13:21	2分	216
哈达铺	D206	13:38	13:40	2分	241
陇南	D206 ←	14:37	14:41	4分	28分钟 370 公里
广元	D206	15:42	15:48	6分	509
阆中	D206	16:42	16:44	2分	615
南部	D206	16:57	16:59	2分	636
南充北	D206	17:29	17:31	2分	697
武胜	D206	18:00	18:02	2分	754
重庆西	D207	19:01	19:12	11分	867
綦江东	D207	19:42	19:44	2分	928
赶水东	D207	20:02	20:04	2分	959
桐梓东	D207	20:43	20:45	2分	1035
遵义	D207	21:13	21:15	2分	1088
贵阳北	D207	22:20	--:--	0分	1214

图片exif中有iso信息



照相机制造商	OnePlus
照相机型号	PJA110
光圈值	f/1.8
曝光时间	1/172 秒
ISO 速度	ISO-138
曝光补偿	0 档光圈
焦距	6 毫米
最大光圈	1.7
测光模式	偏中心平均
目标距离	200 米
闪光灯模式	无闪光，强制
闪光灯能量	
35mm 焦距	24

高级照片

可得答案

Flag1

问题1：图片中的位置附近有一条高速公路 请给出高速公路编号[G+两位数字]

G75

问题2：图片所在位置最近的市是哪个[XX(X)市]

阆中市

问题3：图片采用的ISO感光度是多少

138

提交答题区1

Flag2

问题4：出题人所乘车的的车次号是

D206

提交答题区2

这是flag2flag{A1_lA1_zl_gU0_Tie}

躺平问答

通过百度等搜索引擎搜索易得（bushi

上周，身为2024届英才计划培养对象的出题人ZianTT参加了一次冬令营，请问他的活动大致地点是？（七个汉字）

哈尔滨工业大学

在2023年，Cloudflare因为机房停电导致大量服务不可用，Cloudflare官方博客记载此时的英文版链接是：

https://blog.cloudflare.com/post-mortem-on-cloudflare-control-plane-and-analytics-outage

QQ上线了新春活动，但糟糕的体验显然引发了一些用户的困扰，关闭该功能的链接是？（一个由https://开始的链接）

https://docs.qq.com/form/page/DUWl2cXN2WktZVWlB

HTCPCP是一种类似HTTP的协议，用于控制咖啡壶，其中，当发送了BREW请求来冲泡的时候，如果服务认为请求的添加项组合违背了饮酒者对所述种类的共识，返回的状态码是：

403

OpenAI在2024年1月发生了多少运行事件(以公示数据为准)：

11

比赛平台域名tpcup.org的Registry Domain ID 是：

6de68c6722e84ac0a541745e94b7dca0-LROR

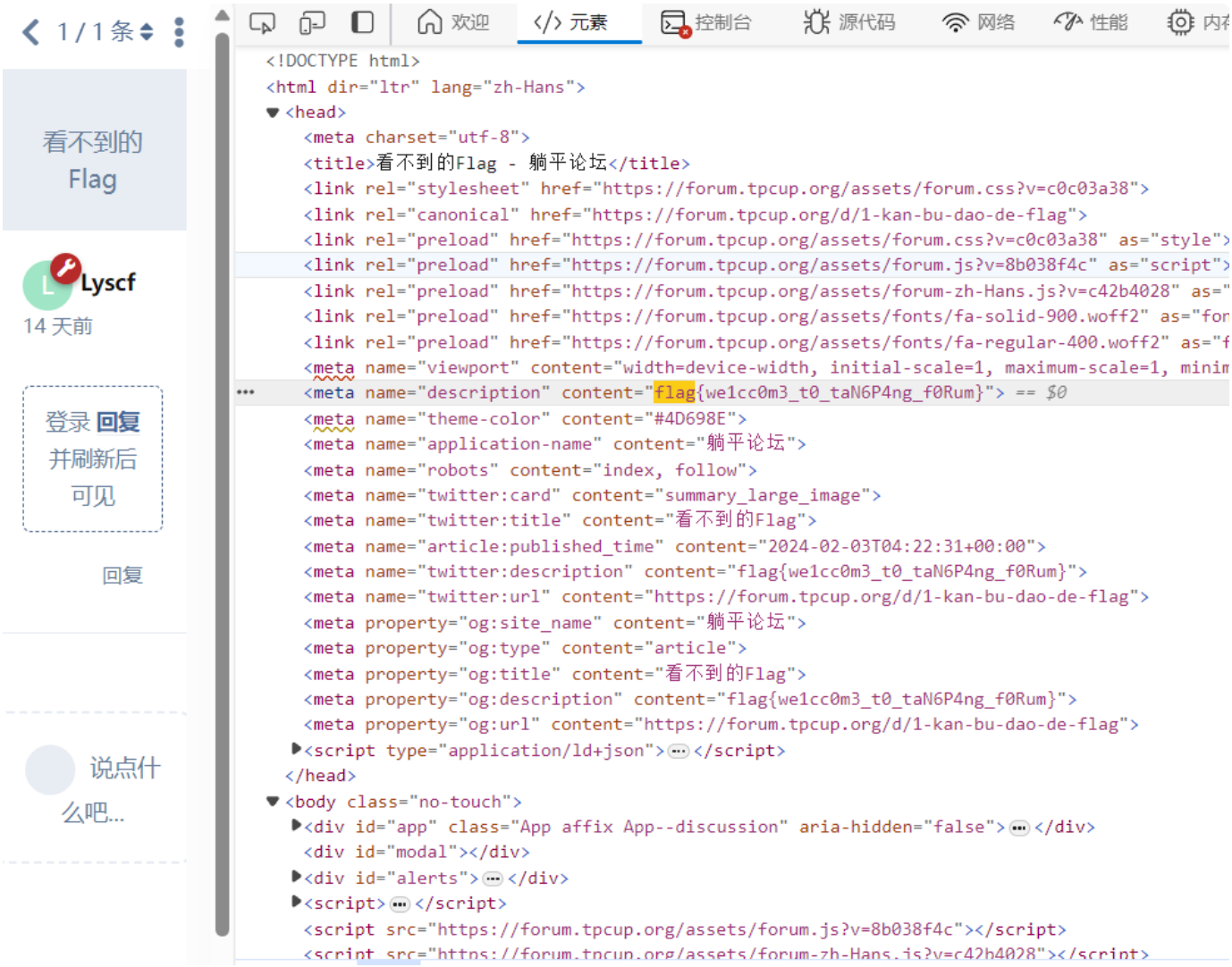
本次比赛计算服务提供商所在主体纳税人识别号是：（18位由数字和大写字母组成的字符串）

91440403MACK9P7J40

Web

躺平论坛

easy的F12



Crypto

主唱太拼命了

看题目的意思，估计是要爆破p+q的后60位，刚好在网上找到一篇文章：
https://blog.csdn.net/weixin_52640415/article/details/130415368

直接拿里边的脚本来改了下

Python

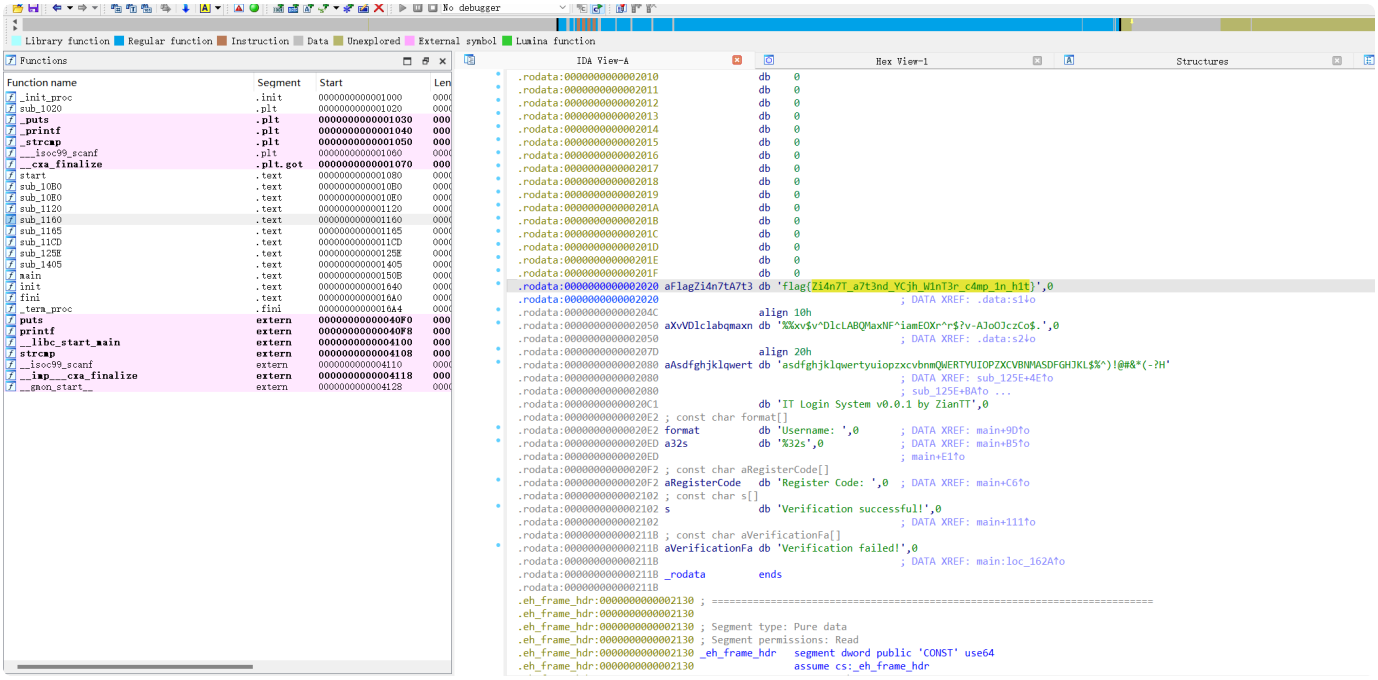
```python
from Crypto.Util.number import *
from gmpy2 import *
ct = 184408724864033236225108070129785071805299414261066431154569808379562953257641925954858207297728454287539535903017137050783992018693651937080573278488999040746718328075966653675506149190551195090738124993160194470700774724197391162379524862601796129845824968624416098490356038421618390694071152182456814233 69
n = 990435771821184443784396422856400479583949713121020353009836340021848496582243738732680608868337286124945651708032263596414682715371553854580290526329839808374493781596713747489260319218837733051895942993586947240697287935191646322289509985455058076406049562508326923442263825731210148429532750203537435873 93
gift = 199082962971542611936037844766389311235162407040253062445619309358334639717991281104899674484609133115805473897433672609025228650732008259177230581083668 48


PR.<x> = PolynomialRing(Zmod(n))
ok = False
p = 0
def pq_add(tp,tq,tgift,idx, kbit):
    global ok
    global p
    if ok:
        return
    if tp*tq>n:
        #print('>')
        return

    if (tp+(2<<idx))*(tq+(2<<idx))<n:
        #print('<', hex((tp+(1<<(idx+2))))[:20], hex(tq+(2<<idx))[:20], hex(N)[:20])
        return

    if idx<=kbit:
        try:
            f = tp + x
            rr = f.monic().small_roots(X=2^kbit, beta=0.44)
            if rr != []:
                """print(rr)
                print(tp)
                print('p = ',f(rr[0]))"""
                p = int(f(rr[0]))
                ok = True
                return
```

```
            except:
                pass

            return

        idx -=1
        b = tgift >>idx
        one = 1<<idx

        #print(hex(tp)[:20],hex(tq)[:20],hex(tgift)[:20],idx,b)

        if b==0 or b==1:
            pq_add(tp,tq,tgift,idx, kbit)
        if b==1 or b==2:
            pq_add(tp+one,tq,tgift-one,idx, kbit)
            pq_add(tp,tq+one,tgift-one,idx, kbit)
        if b==2 or b==3:
            pq_add(tp+one,tq+one,tgift-(one<<1),idx, kbit)

tp = 1<<511
tq = 1<<511
tgift = gift -tp -tq
kbit = 60
pq_add(tp,tq,tgift,511, kbit)
print(p)
q = n // p
e = bytes_to_long(b"too desperate!")
phi = (p-1)*(q-1)
d = invert(e, phi)
print(long_to_bytes(int(pow(ct, d, n))))
```

Reverse

HIT! 准入认证!

IDA打开搜索即得


No debugger
Library function
Regular function
Instruction
Data
Unexplored
External symbol
Lumina function
Functions
Function name
Segment
Start
IDA View-A
Hex View-1
Structures
.rodata:0000000000002020 aFlagZi4n7tA7t3 db 'flag{Zi4n7T_a7t3nd_YCjh_W1nT3r_c4mp_1n_h1t}',0
.rodata:0000000000002050 aXvVDlclabqmaxn db '%%xv$v^DlcLABQMaxNF^iamEOXr^r$?v-AJoOJczCo$.',0
.rodata:0000000000002080 aAsdfghjklqwert db 'asdfghjklqwertyuiopzxcvbnmQWERTYUIOPZXCVBNMASDFGHJKL$%^)!@#&*(-?H'
.rodata:00000000000020C1 db 'IT Login System v0.0.1 by ZianTT',0
.rodata:00000000000020E2 format db 'Username: ',0
.rodata:00000000000020ED a32s db '%32s',0
.rodata:00000000000020F2 aRegisterCode db 'Register Code: ',0
.rodata:0000000000002102 s db 'Verification successful!',0
.rodata:000000000000211B aVerificationFa db 'Verification failed!',0
.rodata:000000000000211B _rodata ends
.eh_frame_hdr:0000000000002130 _eh_frame_hdr segment dword public 'CONST' use64
.eh_frame_hdr:0000000000002130 assume cs:_eh_frame_hdr