第四周做题记录

原创

打酱油的杯具 于 2020-08-09 18:22:33 发布 251 收藏 1

分类专栏： 做题记录 文章标签： 信息安全

本文链接：https://blog.csdn.net/weixin_45710230/article/details/107897799

做题记录 专栏收录该内容

8 篇文章 0 订阅

订阅专栏

[BJDCTF2020]纳尼

打开发现一个gif文件和一个txt文件，gif无法打开，txt中一句废话

使用notepad++查看发现无头文件，补齐后的动图中含有一串base64的密码，使用Stegsolve分离得到

Q1RGe3dhbmdfYmFvX3FpYW5nX2lzX3NhZH0=

在线找个解密网站解密后得到flag

flag：flag{wang_bao_qiang_is_sad}

---

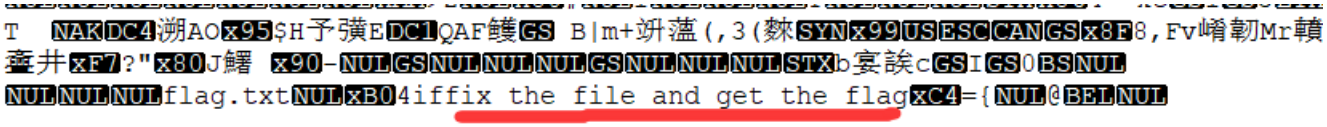
zip

打开后是一堆zip包，都需要密码解压，压缩包大小较小可以使用crc爆破

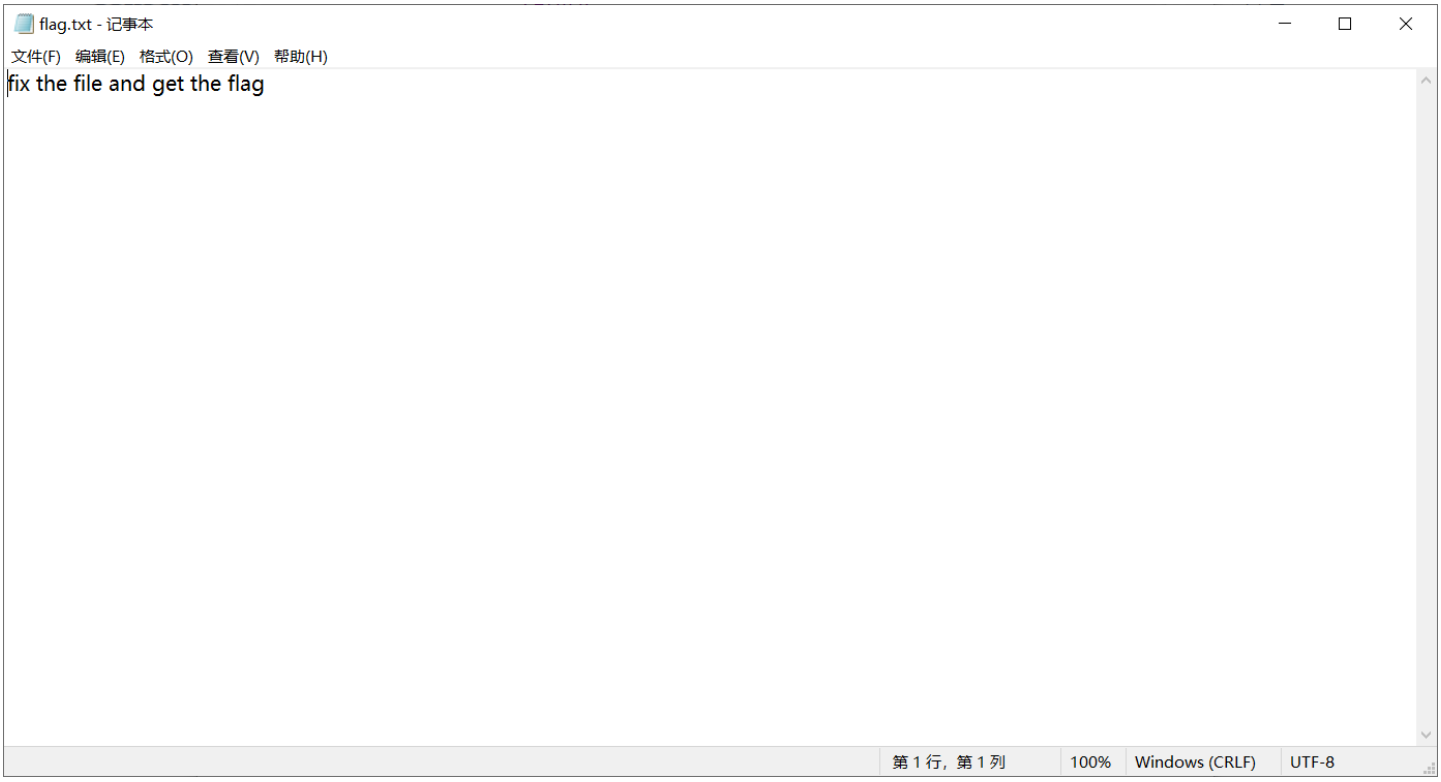
使用网上大佬的一个脚本进行爆破

```
import zipfile
import string
import binascii

def CrackCrc(crc):
    for i in dic:
        for j in dic:
            for k in dic:
                for h in dic:
                    s = i + j + k + h
                    if crc == (binascii.crc32(s.encode())):
                        f.write(s)
                        return

def CrackZip():
        for i in range(0,68):
            file = 'out'+str(i)+'.zip'
            crc = zipfile.ZipFile(file,'r').getinfo('data.txt').CRC
            CrackCrc(crc)

dic = string.ascii_letters + string.digits + '+/='

f = open('out.txt','w')
CrackZip()
print("CRC32碰撞完成")
f.close
```

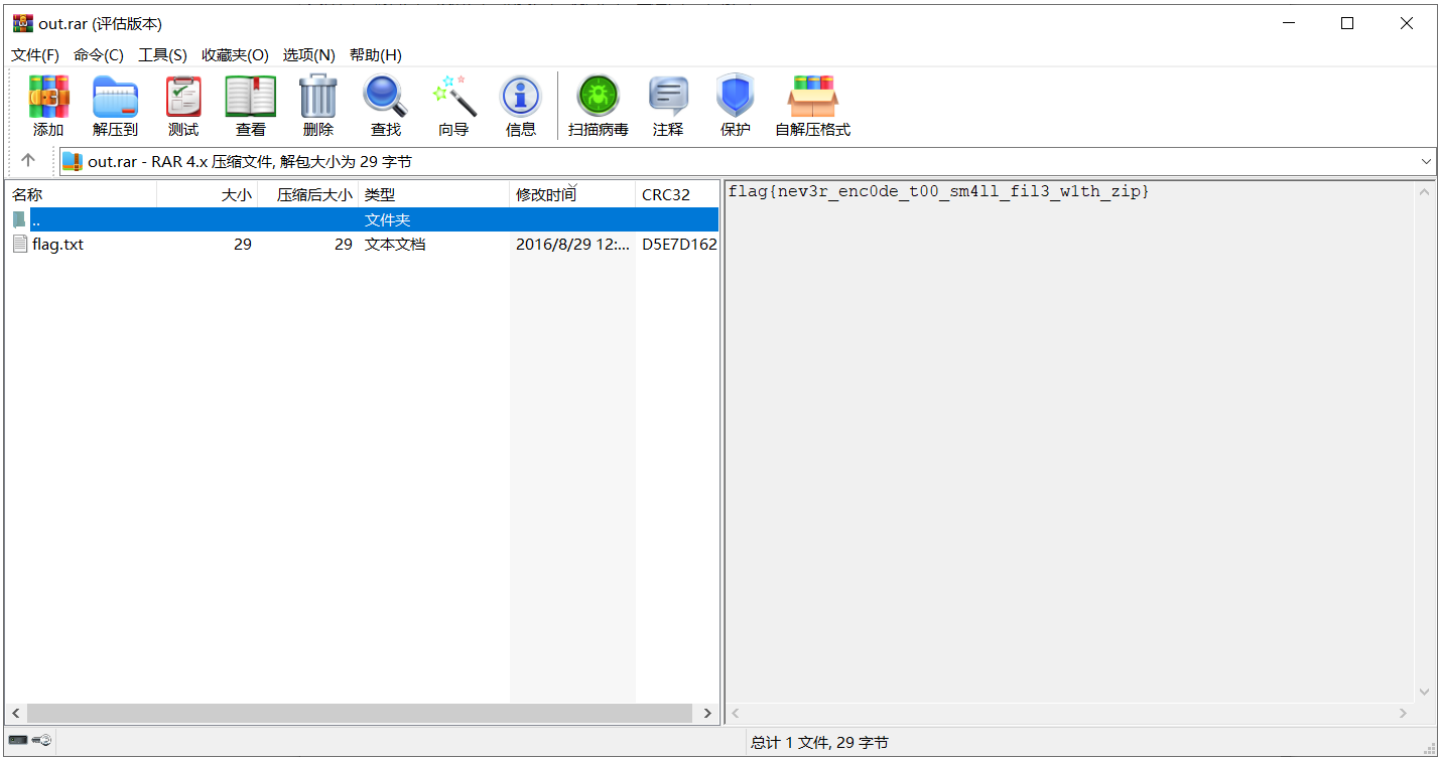
得到一串base64编码，使用notepad++自带的插件转化，打开发现



查看文件尾发现是rar，在头部补全，打开发现



wtf，使用winrar打开后，在旁边发现flag



flag：flag{nev3r_enc0de_t00_sm4ll_fil3_w1th_zip}

谁赢了比赛？

打开发现一张png图片，在文件尾发现rar文件尾

```
) 11 9d 03 90 8b e6 70 3f 8e 20 b4 43 18 02 fc 78 ....嫩p??碲..黿□[
) df f4 c3 db 84 bb bb e1 ab 0c 0f 61 50 e9 e3 d5 唪蜜券会?.aP殂?□[
) 7e ef 79 61 a8 0a 08 13 c6 a5 a1 f0 41 59 cc 8c ~飝a?..匹○AY虎□□[
) 4a ce 97 cf 8c a3 32 f2 36 c7 03 56 d4 ba 5e a0 J螚蠶???V院^.□□□[
) 2f 36 5b 8b 04 39 fc 0f 13 e5 1f 08 13 bc 56 c0 /6[?9?.?..糌?□□□[
) 8d d5 3e 71 2b b3 4c 2b 9a 85 c8 fa 49 36 b8 47 .?q+砣+殏鳃I6窯□[
) 34 a2 bb e1 27 42 19 76 5b 8b 09 73 87 4e ab 35 4ₙ.?B.v[?s喟?□□□□[
) 32 74 55 b4 d5 ac 0a 25 9e 5b 78 96 6c 88 68 03 2tU凑?%溻x杶坐.□[
) 56 ba 07 e1 91 db 1a 74 20 90 2d 00 1f 00 00 00 V?釕?t .-.....□□[
) 1f 00 00 00 02 37 01 89 bd 1d 71 13 47 1d 30 08 .....7.墠.q.G.0.[
) 00 20 00 00 00 66 6c 61 67 2e 74 78 74 00 b0 f1 . ...flag.txt.榜[
) ac 1a 77 68 65 72 65 20 64 6f 20 79 6f 75 20 74 ?where do you t□
) 68 69 6e 6b 20 74 68 65 20 66 6c 61 67 20 69 73 hink the flag is
) 3f c4 3d 7b 00 40 07 00                         ??{.@..□
```

拖进kali分离，得到一个rar文件，打开发现密码

使用ARCHPR爆破得到密码1020，得到一个废话的flag文件，和一张动图

看了好久发现一张一闪而过的图片，使用StegSolve分离得到，结果是假的flag

查完wp后，把flag图片使用StegSolve查看0通道发现二维码

扫码的flag

flag:flag{shanxiajingwu_won_the_game}

[ACTF新生赛2020]outguess

打开题目发现一堆文件，在jpg文件备注下发现一段奇怪的文字

为核心价值观编码，使用网页http://ctf.ssleye.com/cvencode.html解码得到abc

看到题目提示为outgess，使用得到的密码尝试分离，得到flag

flag：flag{gue33_Gu3Ss!2020}

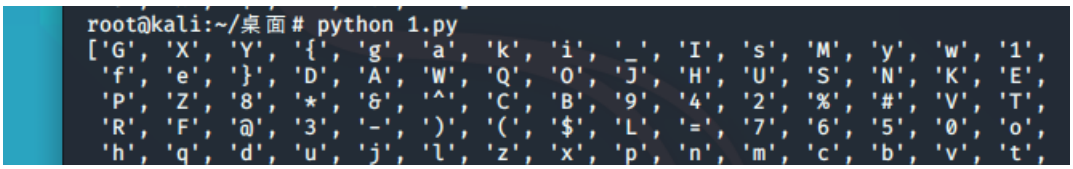
[GXYCTF2019]gakki

打开得到一张图片，拖进kali分分离得到一个带密码的rar压缩包，使用ARCHPR暴力破解得到密码8864

得到一份乱七八糟的txt文件，使用字频统计脚本

```
alphabet = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890!@#$%^&*()_+- ={}[]"
f = open("flag.txt", "r")
data = f.read()
result = {d:0 for d in alphabet}

def sort_by_value(d):
    items = d.items()
    backitems = [[v[1],v[0]] for v in items]
    backitems.sort(reverse=True)
    return [ backitems[i][1] for i in range(0,len(backitems))]

for d in data:
    for alpha in alphabet:
        if d == alpha:
            result[alpha] = result[alpha] + 1

print(sort_by_value(result))
```

执行得到flag

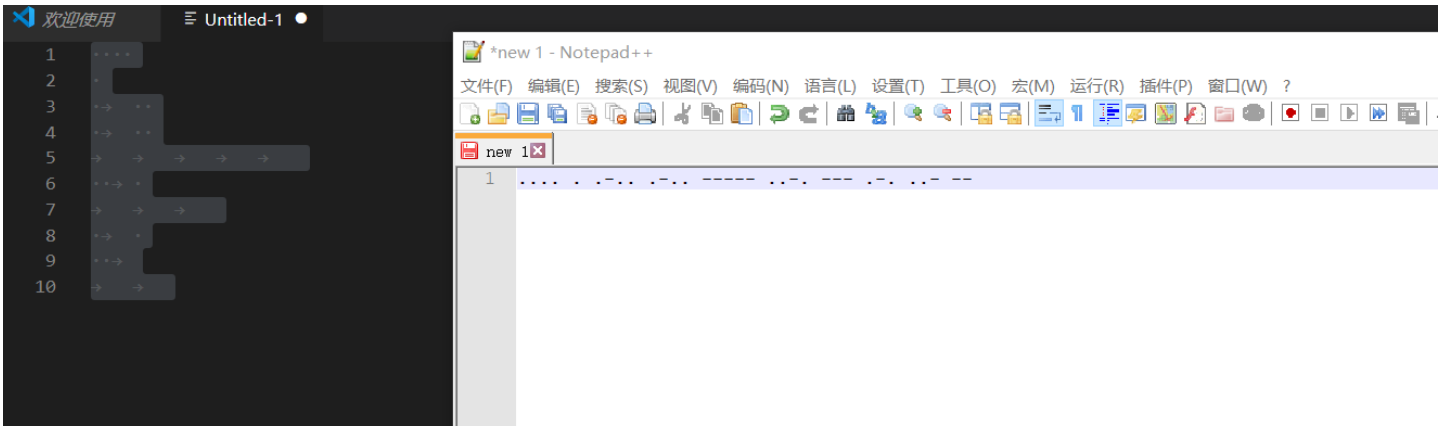


flag：GXY{gaki_IsMyw1fe}

弱口令

打开发现有密码，使用WinRAR打开后发现旁白有些看不见的文字

复制到vscode中发现是摩斯密码



通关网站解密得到压缩包密码HELL0FORUM

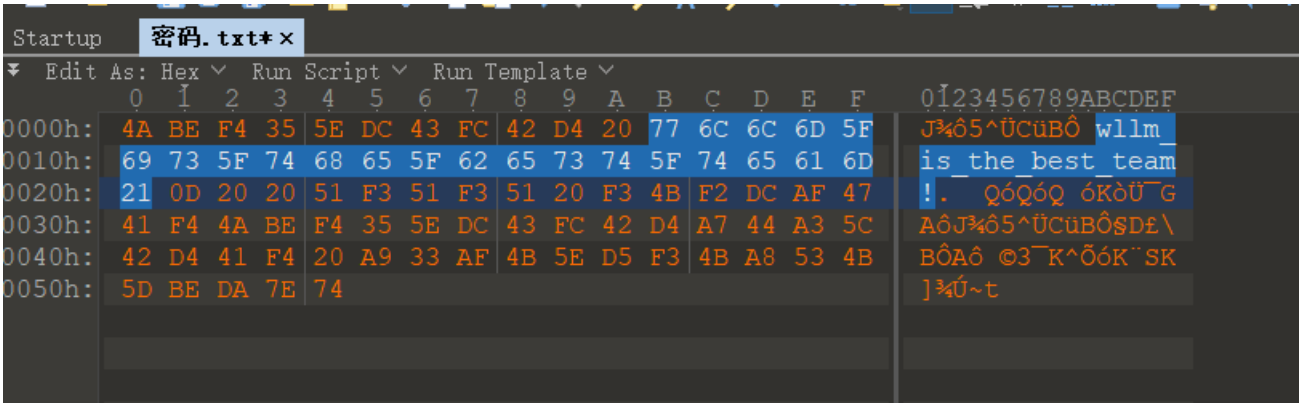
打开得到一张图片，然后不会做了，查看大佬wp后，发现使用lsb脚本使用弱口令即可

```
python lsb.py extract 1.png new 123456
```

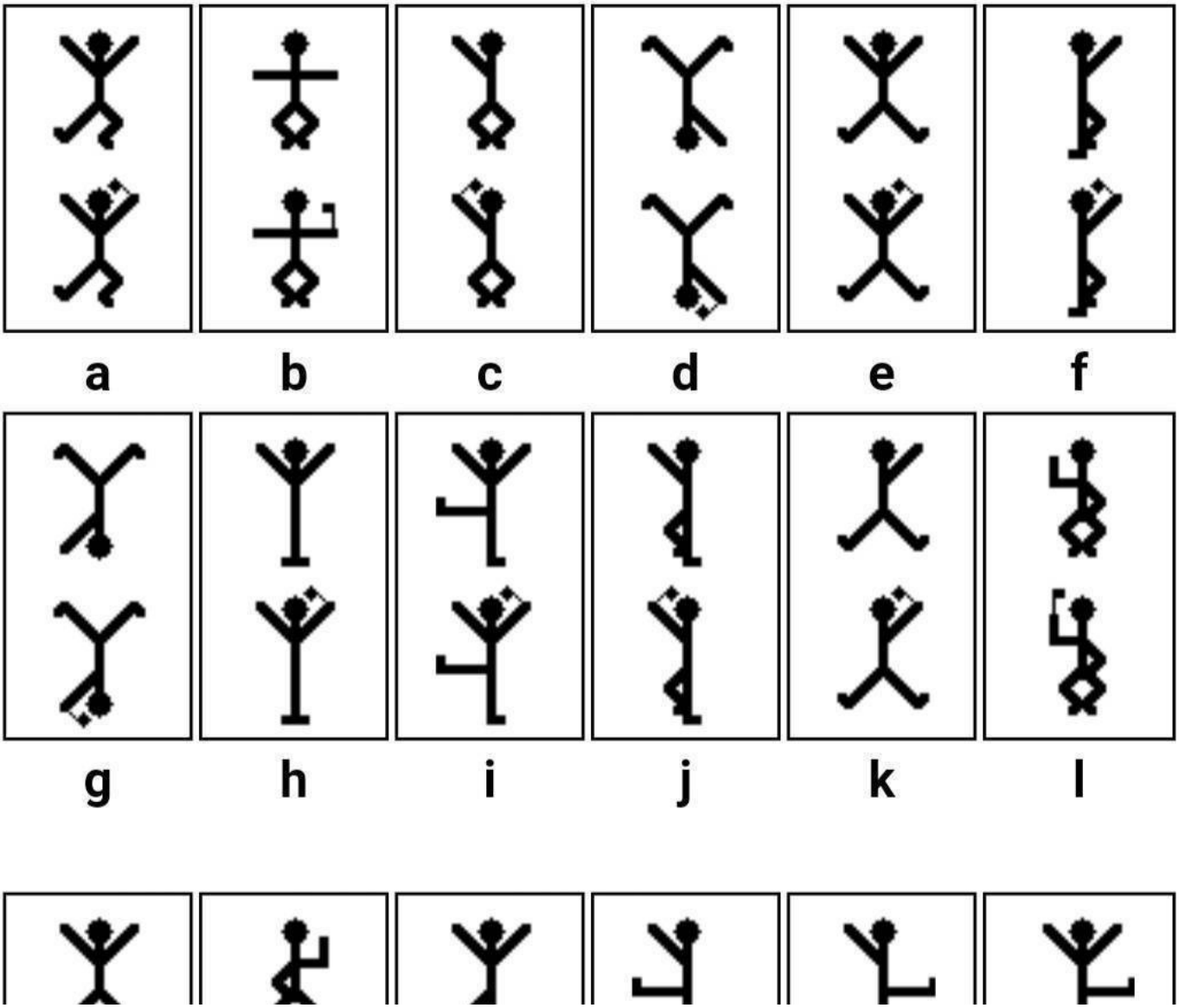
flag：flag{jsy09-wytg5-wius8}

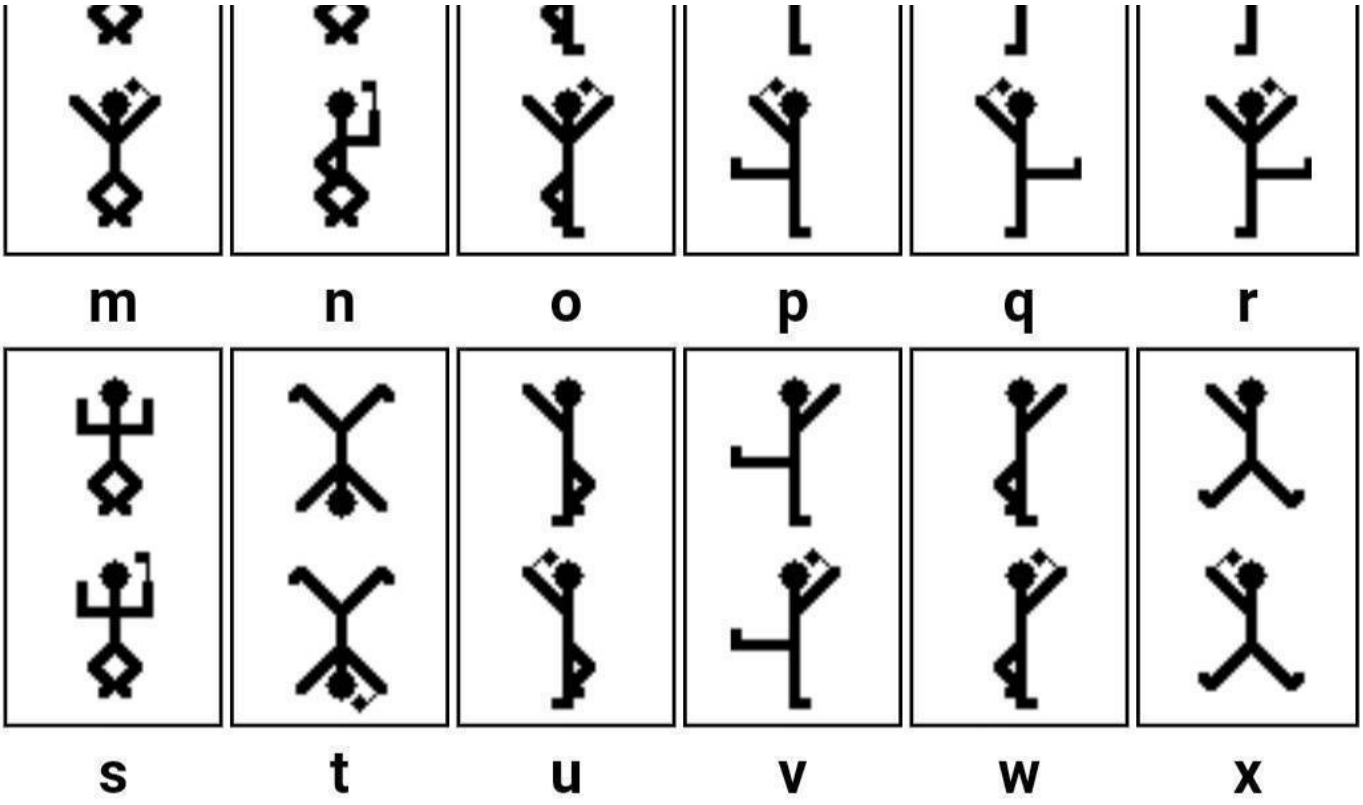
[SWPU2019]伟大的侦探

打开发现一个加密的文件夹和一个未加密的txt文件，txt提示编码，使用01edito修改为EBCDIC编码得到密码



打开文件夹发现一堆小人图片，是福尔摩斯里面跳舞的小人加密





得到flag：iloveholmesandwllm