1. 听听音乐？

听听音乐? [已完成]

描述

一首MP3,好好听哦，flag由大写英文字母、数字以及下划线组成，记得添加hgame{}

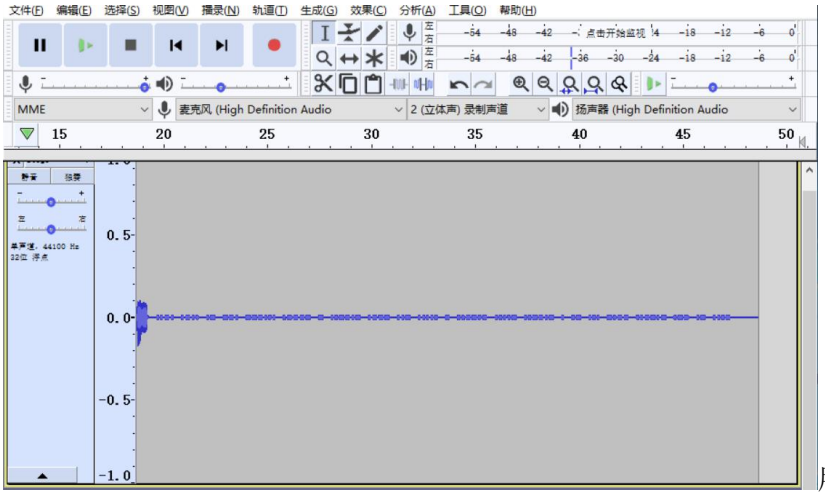
URL http://plir4axuz.bkt.clouddn.com/hgame2019/a80509c91f30027ca21b069e7d94fa7718ab2e40684628c41943bf647f3d7c6a/stego.mp3

基准分数 150

当前分数 150

完成人数 79

先获取文件 听了一下这首歌 最后面的很奇怪



用 Audacity 打开看到了最后面的波形

初步认为应该是摩斯密码 拿去网站上翻译一下就得到了 flag

..-./.-../.-/--./---.../.----/-/..--.-/.---/..-/...../-/..--.-/....-/..--.-/./.-/.../-.--/..--.-/.--/.-/...-

加密摩斯密码 解密摩斯密码

FLAG:1T_JU5T_4_EASY_WAV

2.至少像那雪一样

至少像那雪一样[已完成]

描述

出题人想不好题目描述了

URL http://plqfgjy5a.bkt.clouddn.com/%E8%87%B3%E5%B0%91%E5%83%8F%E9%82%A3%E9%9B%AA%E4%B8%80%E6%A0%B7.jpg

基准分数 150

当前分数 150

完成人数 42

下载得到了一张图片 先用 stegsolve 查看图片发现啥都没有 binwalk 分析一下发现后面合并一个 zip 压缩包

用 binwalk 进行分离然后就陷入僵局。。。 以下省略漫长的 py 学长过程 发现 binwalk 分离有问题

后选择用 foremost 进行分离 打开压缩包发现里面也压缩着一个图片文件很明显应该是明文解密

解密后解压文件一篇空白。。。 百度 ing 机缘巧合之下用 vim 打开文件十六进制查看

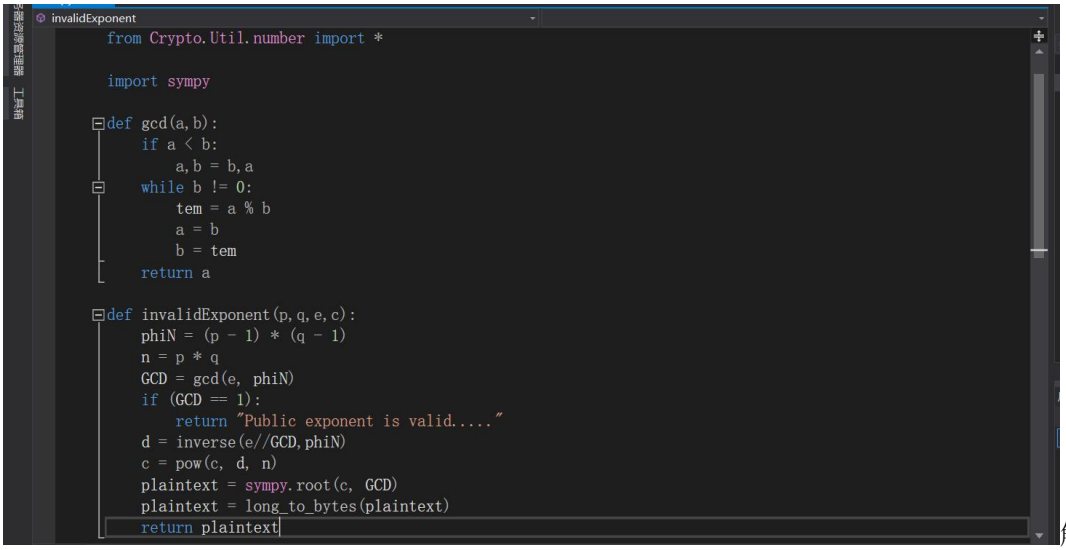
应该是二进制 那就转换一下得到 flag

3.旧时记忆

看到提示直接百度 存储器的发展历史 发现所给图片是打孔卡 对着 Google 查的打孔卡和字符的对照表直接获得 flag

4.babyRSA

先去网上了解一下 RSA 加密 发现题中的 e 与 pin 不互质 很难受无法算出 d Google 了一波找到了一个解密程序好像适用这个题目 复制这个程序改一波数据跑一下得到了 flag


invalidExponent
from Crypto.Util.number import *
import sympy
def gcd(a,b):
if a < b:
a,b = b,a
while b != 0:
tem = a % b
a = b
b = tem
return a
def invalidExponent(p,q,e,c):
phiN = (p - 1) * (q - 1)
n = p * q
GCD = gcd(e, phiN)
if (GCD == 1):
return "Public exponent is valid....."
d = inverse(e//GCD,phiN)
c = pow(c, d, n)
plaintext = sympy.root(c, GCD)
plaintext = long_to_bytes(plaintext)
return plaintext
解密程序