Misc

Tools

当我看到那个套娃的图片的时候 我就有点不详的预感了

果真是一些图片隐写工具的套娃

使用的隐写工具依次是F5->steghide->Outguess->JPHS 密码都是在图片的简介里

每次解压都得到一个二维码的一角 拼起来就可以了 ~~其实有三个脚就可以扫了~~

Telegraph：1601 6639 3459 3134 0892

先是看题目的那几个数字 是中文电报码 翻译下来就是`带通滤波器`

然后上Audacity康康音频的频谱图 上边写了个850hz

那基本很明显了 打开Au处理一下音频 ~~一定要选好滤波器的种类 不然眼睛能看瞎~~

发现这个音频成了一场段长短点 那基本是莫斯电码了

然后看频谱翻译 ~~如果你是鬼子电报员可以直接听~~

Hallucigenia

怪诞虫？？？ 一个让科学家分不清上下左右的虫子2333

一张图片 先binwalk一下 发现没东西 然后拖到Stegsolve里康康

发现里边有藏一个二维码 扫一扫 感觉好像是base64 解密一下

好家伙这是什么东西 怎么还是乱码

想了好久 发现结尾的GNP有点熟悉 不就是PNG倒过来的 还真的是分不清左右

倒一下 得到一张图片 镜像后的flag 2333 ps翻一下就好了

DNS

先是得到一个网络数据包 上Wireshark

结合题目名字 先筛选udp.port==53或者DNS 然后就找到了一个网址 `flag.hgame2021.cf`

先访问一下 发现一直蹦弹窗`flag is here but not here` 不一会网页就崩溃了

az 那强行用view-source康康网页原代码 ~~好家伙while(true) 连延迟都不设置的吗~~

结尾写了一个SPF 暗示满明显的了

cmd nslooks一下查看网页的SPF服务 发现返回的就是flag

Crypto

signin

看python先 发现加密过程是这样的

$$c \mod p = a^p \times m$$

`m`就是flag通过`s2n`转化来的 同理就可以用`n2s`逆回去

然后`a` `m` `p`都是质数

~~那就枚举下`*`吧(但是还真的行) 虽然算蛮久的 真的好久 好孩子千万不要试~~

最主要的问题是`a`的`p`次方太大了 查了一查和幂运算相关的定理 找到了费马大道理的弟弟费马小定理

$$a^{p-1} \mod p = 1$$

这样式子就可以化简到一个不定方程

$$ax \mod p = c$$

那就是解这个关于`x'`和`m`的不定方程的正整数解

又因为有整数解的条件是`c`能被`p`,`a`的最大公约数整除 所以等效于求

$$a' * m + p' * x' = Gcd(a, m)$$

刚好libnum里边有这个函数

```
x, y, gcd = xgcd(a, p)
m = ((x * c // gcd) % p + p) % p
FLAG = n2s(m)
```

gcd or more?

有py代码可得

$$flag^2 \mod n = chiper$$

这化简一下不是和上一道题差不多吗

$$chiper = flag^2 + n * x$$

此外`x^2=y(mod n)`是`二次剩余问题`~~弓我知道它的名字~~`libnum`好像有直接求解的函数

WhitegiveRSA

幸好这几个数都不大 可以直接暴力破解

先对n分解质因数得n=2^137 * 3 * 1648981883189819

然后写三个for循环枚举出p和q

p = 857504083339712752489993810777

q = 10292249479429980750803486472l9

然后就可以推出d

d = 12183288670241573157707396295737778019551049996539846984328l

最后找一个在线工具解密一下就好了

The Password

az 有左移 右移 又有位运算 那么之前的左移和右移应该都是位运算吧 那么就该先找到这个东西是多少位啊

写个脚本大概比了一下 发现这堆数据应该在2^63到2^64之间 那么应该就是64位了吧

~~幸好一开始假设对了 不然裂开~~

每一条方程对应的参数都是`xi` `yi` `ni`

说明方程间是没有关系的 那么就一条条来解就好了

$$y = x \oplus n \oplus (x \ggg a) \oplus (x \lll b)$$

每一条方程都是这样的形式 那么意图就应该很明显了 把x给独立出来

先引入一个定理~~吧~~

如果

$$a = b \oplus c$$

那么

$$a \ggg x = (b \ggg x) \oplus (c \ggg x)$$

左移同理

然后就得到了

$$y \ggg a = (x \ggg a) \oplus (x \ggg 2a) \oplus (x \lll b - a)$$

$$y \lll b = (x \lll b) \oplus (x \lll a - b) \oplus (x \lll 2b)$$

然后三条式子异或一下

$$y \oplus (y \ggg a) \oplus (y \lll b) = x \oplus (x \ggg 2a) \oplus (x \lll 2b)$$

好家伙梦回第一条

这时候 左移右移的一个性质就起作用了 当n等于y的长度时

$$y \lll n = y$$

右移同理

所以只要我们迭代6次 就可以得到一个式子

$$y' = x \oplus x \oplus x$$

自己异或自己就是0

那么我们就如愿以偿的解出x了

然后把x按编号从头接到尾 再转化为字符串就好了

或者也可以用位来理解 每一位都是一个未知数 那么一共就有64条方程

左移右移就相当于未知数下标加或者减

然后也是迭代和消元 ~~但是看着会比这个复杂一些~~