week1

MISC

签到

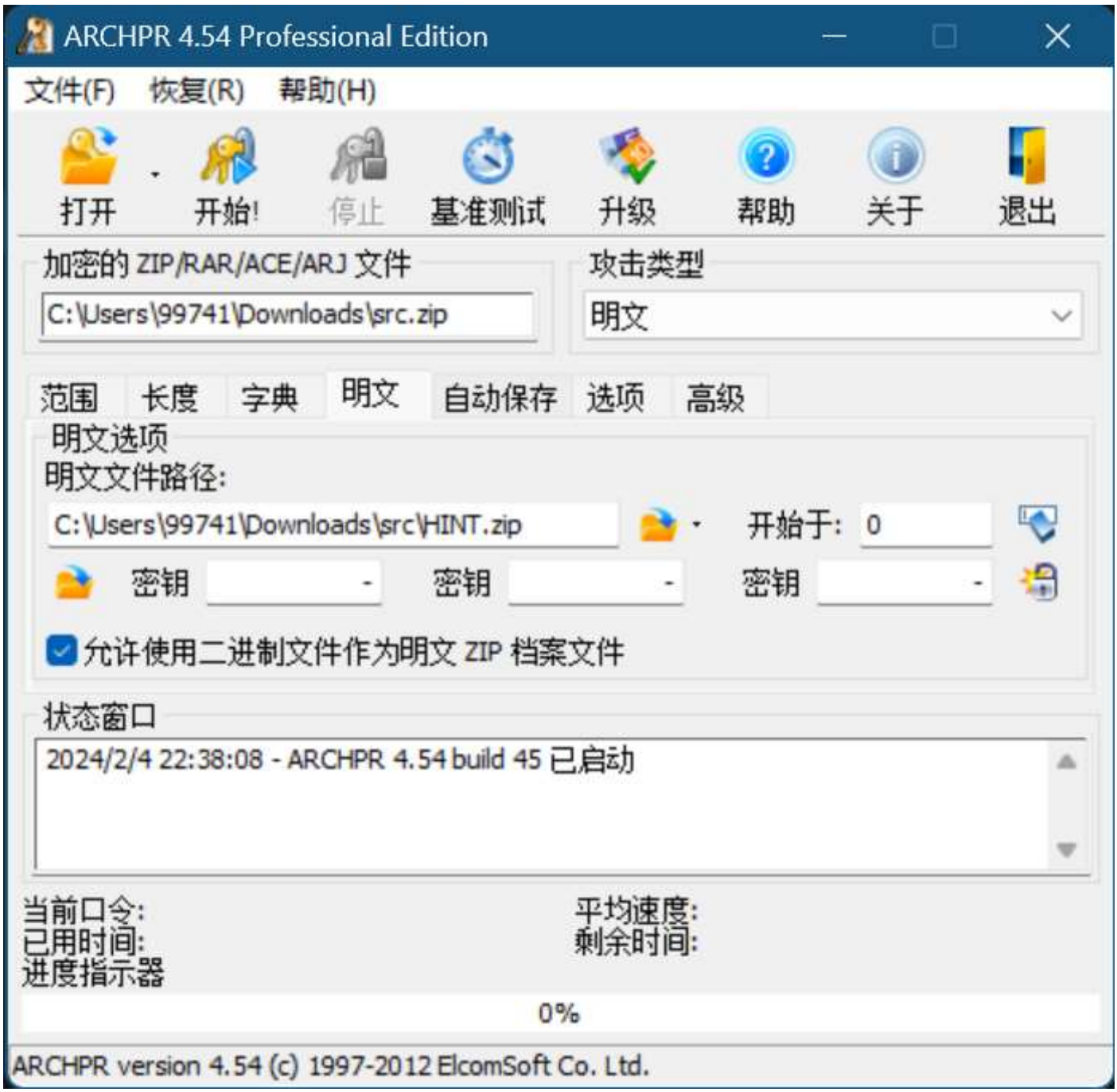
这没什么好说的吧

希尔希尔

通过得到的图片，初步推测IHAR可能被改了所以直接通过010editor打开，通过010editor的信息提示可得，图片的CRC码错误，同时可以在图片末尾发现一个多余的文件尾（50 4B，很明显的zip文件）。
同时，再通过脚本检验可得
所以直接同过CRC爆破脚本修复图片的IHAR，可得到一下图片
然后再通过多次不同隐写方法试探，可以从过LSB隐写的到一个key *(KEY:8 7][3 8;A=0)*。通过希尔加密的提示和这个key即可得出zip文件中希尔加密后的flag。

simple_attack

下载得到的是一个加密的压缩包，同时可以看到加密的压缩包中有两张图片的名字是一样的，所以可以判断是明文攻击类型的。但是直接将图片压缩成压缩包好像大小不太对。所以观察一下，发现直接下下来的压缩包就是一样的大小，所以直接将他当做明文进行攻击



接下来就可以得到一个被解密的zip文件然后查看里面的photo.txt,从名称上就可以知道是张照片，写base64的照片所以，方到浏览器网址栏中就可以的到flag

来自星尘

通过许多检测隐写的手段发现是steghide，同时，经过题目提示的弱密码可得到，隐写于其中的密文图片。通过来自星尘的官网可知是来自星尘上的游戏内文字，通过搜索可以找到对应表，然后翻译出来就好了。

Signin

仔细看能看到一个被拉伸的SEE所以，通过PS将图片在反拉回来就能得到flag

REVERSE

ezIDA

用IDA打开好像就有 没记错的话

ezUPX

搜索一下，UPX就是个壳，跟着教程脱一下壳，再用IDA打开，就可以得到一个程序，然后分析代码。可知将一串字符与0x32做了异或运算，所以将程序中的字符数组提取出来，然后，再写个程序对每一个字符进行一次异或运算就能得到flag

ezASM

通过阅读代码可以看到数据段（data段）有串数字，推测为密文，同时在阅读汇编代码可以找到 `orx 0x22` ，所以可知做了一次异或运算，同时通过 `cmp` 语句可知比较的是字符串的长度 `33` 所以写个程序将每个字符异或一遍就可以得到flag *(关键在于能够看懂一定的汇编语言代码)*

~~ps.临近要交的时候补的wp，漏了很多的细节上的东西~~

同时非常感谢各位出题人的耐心回答和爱的敲打