misc 压缩包密码破解和图片隐写

原创

1n0r 于 2020-08-09 02:08:54 发布 3079 收藏 10
版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。
本文链接：https://blog.csdn.net/inryyy/article/details/107888704
版权

通常misc题目压缩包带有的密码要不就是真加密，要不就是伪加密。

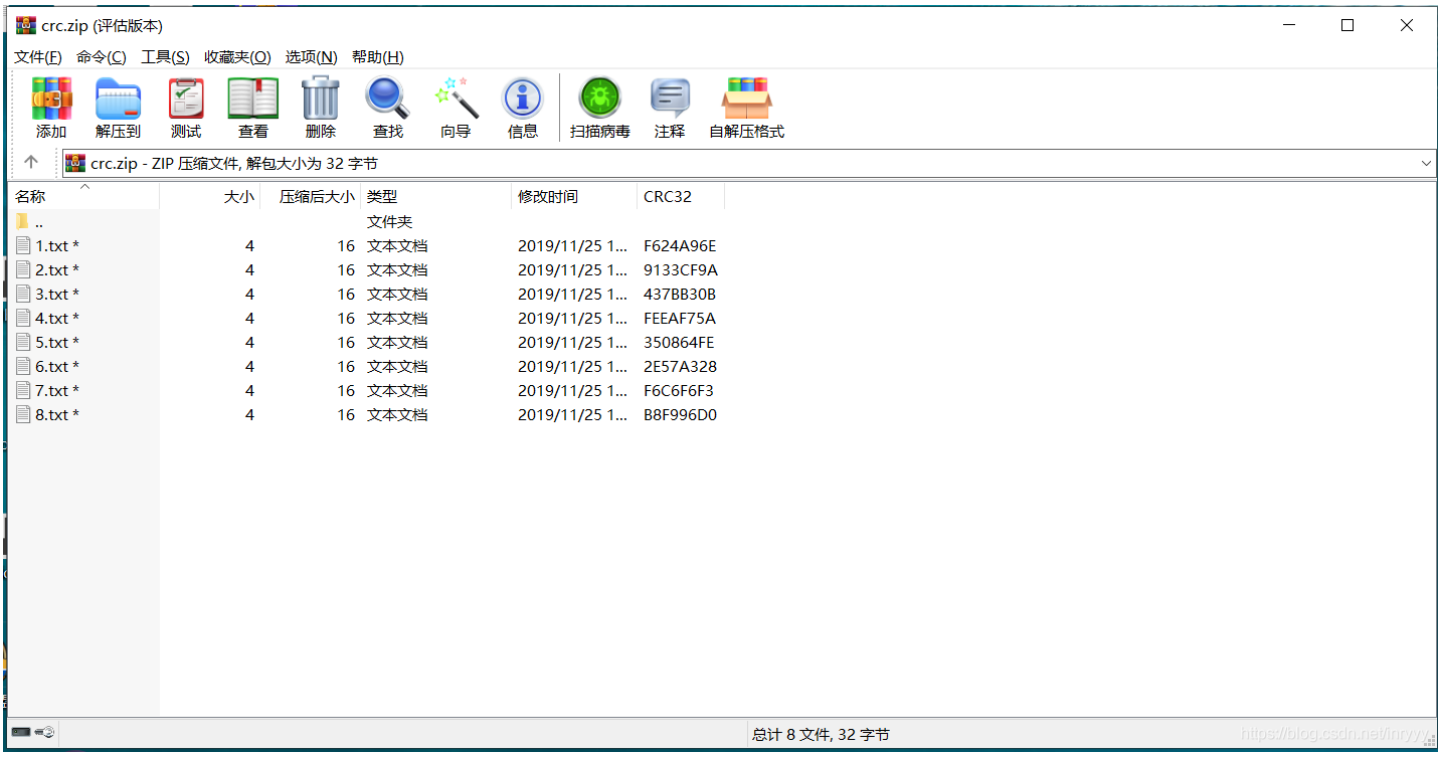
zip的伪加密：http://blog.csdn.net/wclxyn/article/details/7288994

说简单点就是目录中文件文件头标记（50 4B 01 02）后4字节的全局方式位标记是不是00 00 若不是，若为00 01或00 09那么zip进行了伪加密。只要将其修改为00 00即可。

当然也会有真加密的，假如密码简单可以尝试爆破，工具archpr。

不过也会有密码过长的，爆破难顶，得一年的时间才能爆破出来。

例如下面这道题



强硬破解密码行不通，我们可以发现这些txt文件都很小，估计密码藏在这些txt文本当中，我们可以通过crc32爆破出txt文件的内容。

4位的crc32脚本如下：

```
import binascii
import string

crc=0xF624A96E
dic=string.ascii_letters+'0123456789+-_{}'

for a in dic:
 for b in dic:
  for c in dic:
   for d in dic:
    s=a+b+c+d
    if (binascii.crc32(s)&0xffffffff)==crc:
       print(s)
```

密码出来后，解压出来了两个一模一样的图片。

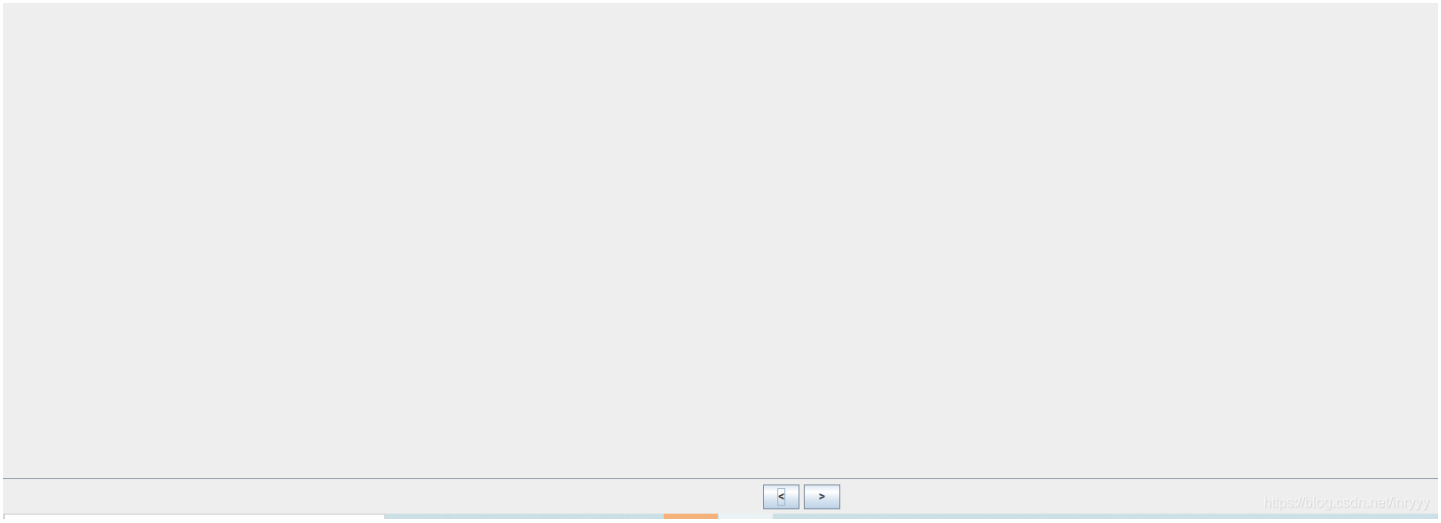
接下来这是图片隐写，而且还给出了两张一样的图片，估计是盲水印。
接下来就是直接到github上找盲水印脚本，然而我发现解不出来。之后才知道是用了另外一种方式来加密。

```
python decode.py --original <original image file> --image <image file> --result <result file>
```

github上盲水印加密解密方法：
https://github.com/chishaxie/BlindWaterMark/blob/master/README.md

steghide隐写
它可以将想要隐藏的信息藏入图片中
将txt文件隐藏并加密
steghide embed -cf 1.jpg -ef Flag.txt -p 123456
解密
steghide extract -sf 1.jpg

stegsolve：
可以发现图片下隐藏的东西，
可以查看动图的帧数
例如攻防世界的give_you_flag



或者通过箭头能发现意外的东西

还有通过修改图片宽和高获得图片下隐藏的信息，工具用winhex来修改
宽和高的数据在第二行，前四位为宽，后四位为高。

LSB隐写：
原理：https://blog.csdn.net/weixin_34075268/article/details/88744599