MRCTF writeup

原创

abtgu 于 2020-03-30 15:23:37 发布 892 收藏 2

分类专栏： CTF

本文链接：https://blog.csdn.net/weixin_43790779/article/details/105200038

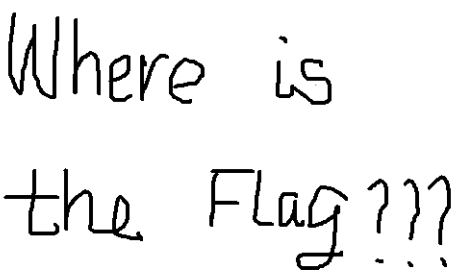
文章目录

MISC

eamisc

题目： Flag到底在哪嘞？

解题思路： 打开发现png格式图片，猜测高度被改写，写脚本进行CRC爆破，得到高度。



MRCTF{1ts_vEryyyyyy_ez!}

CyberPunk

题目： Hacking_security!

解题思路： 打开执行文件，发现需要的运行时间是2020年9月17日，直接更改系统时间，即可得到flag，MRCTF{We1cOm3_70_cyber_security}

千层套路

题目： 套娃题 淦！

解题思路： 套娃题，直接上脚本

```
import zipfile,os
def unzip(zipname):
    while True:
        passwd = zipname.split('.')[0]
        zf = zipfile.ZipFile(zipname,'r')
        zf.extractall(pwd=passwd.encode())
        os.remove(zipname)
        zipname = zf.namelist()[0]
        zf.close()
unzip("qctl.zip")
```

得到qr.txt，打开发现是rgb值，想到rgb转成二维码，上脚本

```
from PIL import Image

x = 200    #x坐标  通过对txt里的行数进行整数分解
y = 200    #y坐标  x * y = 行数

im = Image.new("RGB", (x, y))   #创建图片
file = open('qr.txt')    #打开rbg值的文件

#通过每个rgb点生成图片

for i in range(0, x):
    for j in range(0, y):
        line = file.readline()  #获取一行的rgb值
        line = line.replace("(","")
        line = line.replace(")\n","")
        rgb = line.split(", ")  #分离rgb，文本中逗号后面有空格
        im.putpixel((i, j), (int(rgb[0]), int(rgb[1]), int(rgb[2])))    #将rgb转化为像素

im.show()   #也可用im.save('flag.jpg')保存下来
```

得到一张二维码图片扫描，得flag。

MRCTF{ta01uyout1nreet1n0usandtimes}。

你能看懂音符吗

题目： 希望你可以参透这音符的奥秘。

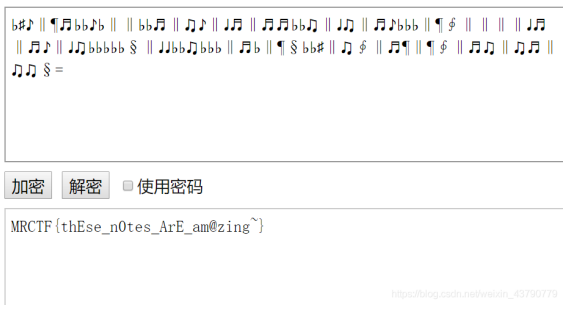
解题思路： 打开压缩包，发现压缩包损坏，用winhex查看，发现文件头错误，将前两个数字与第三第四个数据互换即可。

Address	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	Dump
00000000	52	61	72	21	1a	07	01	00	94	e6	41	f6	0b	01	05	07	Rar!....旅A?...□□
00000010	00	06	01	01	95	ce	80	00	f4	00	98	0d	38	02	03	0b	....睫€.?..8...□□
00000020	c8	cd	00	04	86	da	00	20	bf	3a	fe	97	80	03	00	1a	韧..嗒. ?膳€...□□
00000030	e4	bd	a0	e8	83	bd	e7	9c	8b	e6	87	82	e9	9f	b3	e7	浣.鑾界涞鎳傞煜?□
00000040	ac	a6	e5	90	97	2e	64	6f	63	78	0a	03	02	df	f6	91	玢??docx...喏?□□
00000050	8b	31	f9	d5	01	cc	74	c4	26	50	66	34	54	23	55	4f	? .蘴?Pf4T#UO□□
00000060	14	40	53	09	b0	92	4c	14	cc	18	cc	04	cc	1a	cb	4c	.@S.跑L.???蓁□□勇
00000070	b8	cb	2c	bc	d9	80	59	83	d8	32	cb	30	23	30	23	2d	杆,假€Y冒2?#0#-□□

打开发现word中提示“呀！一不小心把文档里的东西弄没了”，猜测文字被隐藏，点击选项，找到显示，勾选隐藏文字，发现一串音符，进行音符在线解密。

♭♯♪‖¶♬♭♭♪♭‖‖♭♭♬‖♫♪‖♩♬‖♫♬♪♭♭♭‖¶♯‖‖‖‖♩♬‖♫♬♪‖♩♫♭♭♭♭§‖♩♩♭♭♫♭♭♭‖♬♭‖¶§♭♭♯‖♫♯‖♬¶‖¶♯‖♬♫‖♫♬‖♫♫§=

解密地址：https://www.qqxiuzi.cn/bianma/wenbenjiami.php?s=yinyue



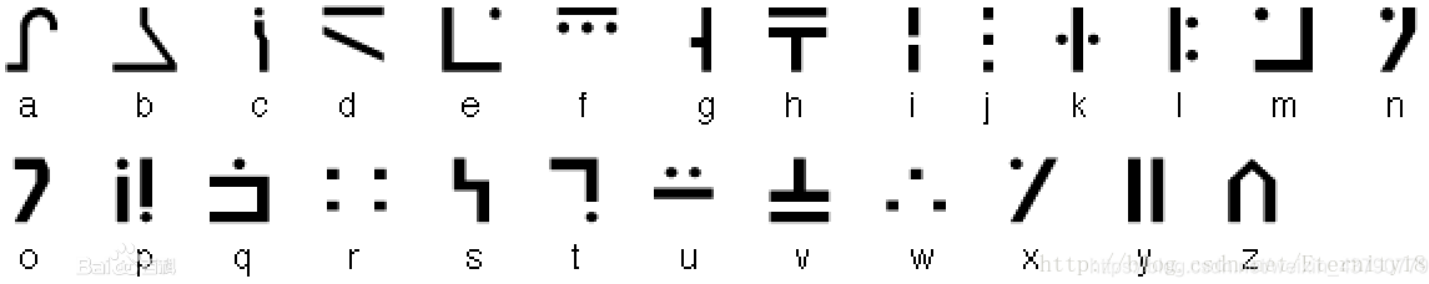
得到flag。MRCTF{thEse_n0tes_ArE_am@zing~}

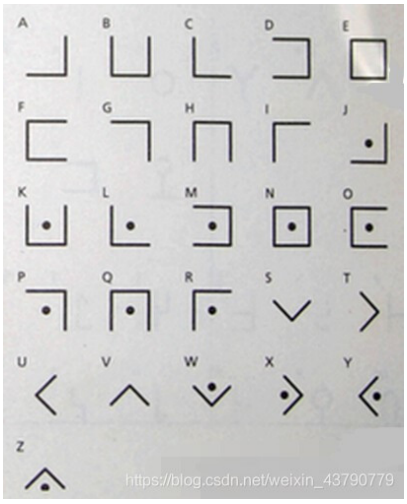
Crypto

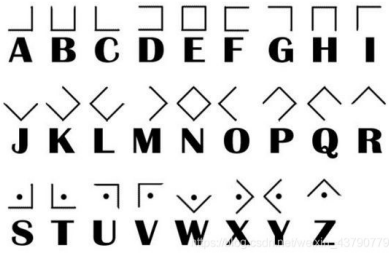
古典密码知多少

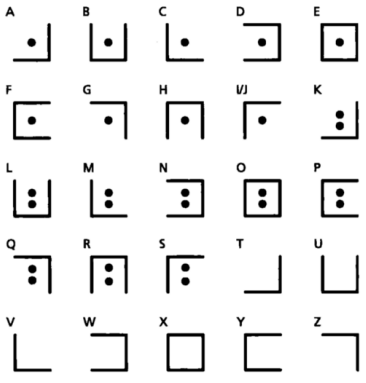
题目： 佛曰：迦呐那侄耨盡切訶呐帝梵竟缽密俱彌穆曳罰呼迦孕諳婆

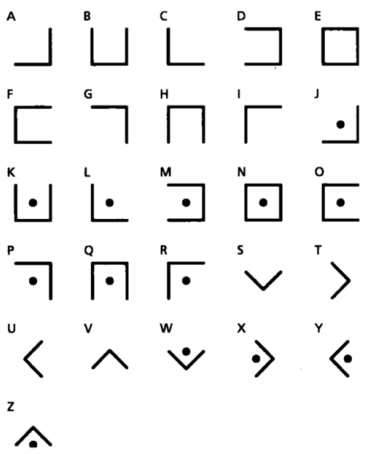
解题思路： 打开图片，发现是猪圈密码，圣堂武士密码，标准银河字母，对照密码表解密，











得到FGCPFLIRTUASYON，图中提到栅栏，想到栅栏密码。当每组数字为3时，得到FLAGISCRYPTOFUN，故flag为MRCTF{CRYPTOFUN}

天干地支+甲子

题目： 我是精通周易的旷世奇才。

解题思路： 根据天干地支纪年法找到txt中所给组合的数字编码，然后分别加上60，转换成ASSII码，得到flag。

```
>>> l = [71, 111, 111, 100, 106, 111, 98]
>>> for i in l:
        print(chr(i), end="")

Goodjob
```

keyboard

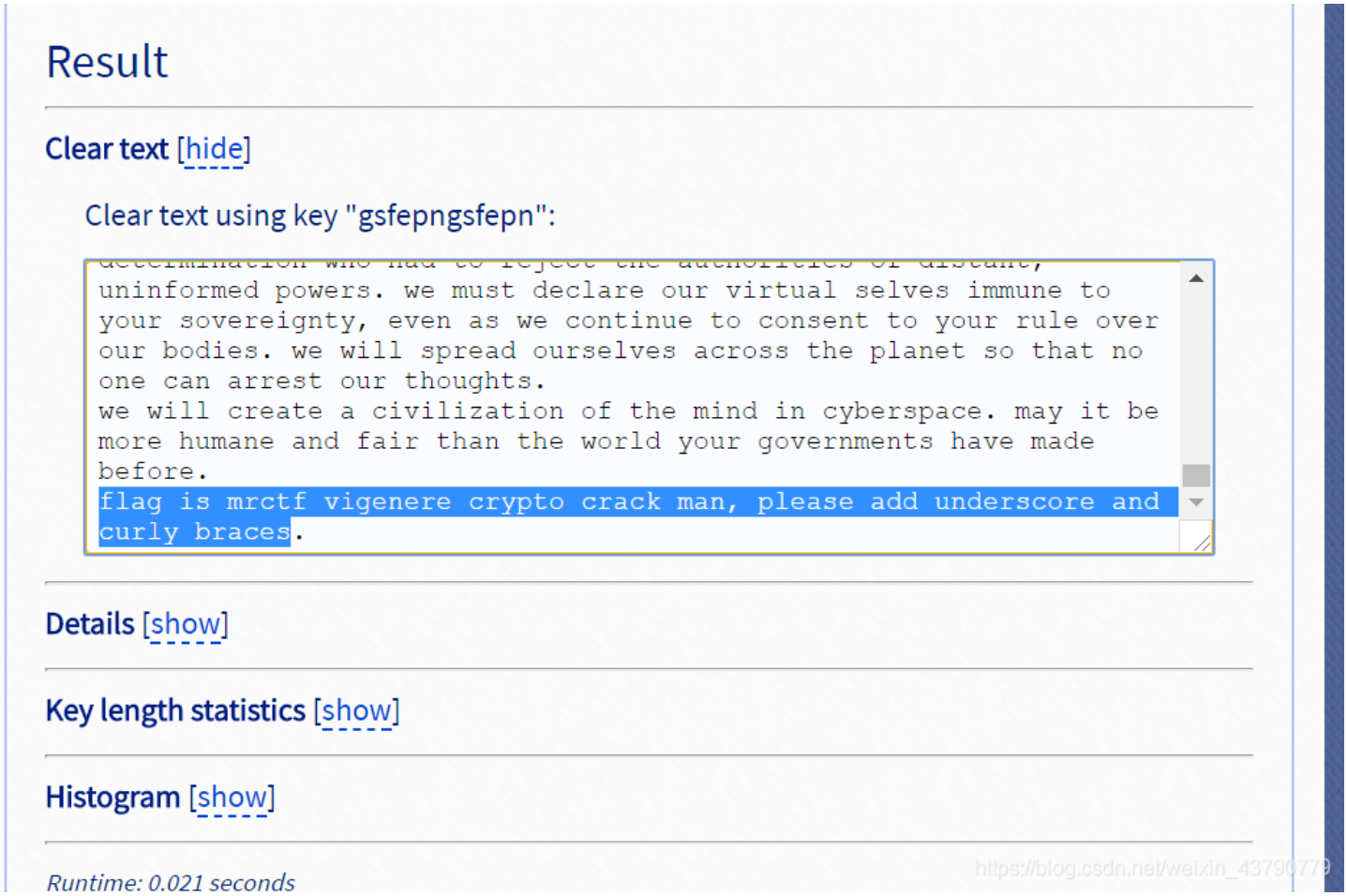
题目： 你很了解这个□？？？

解题思路： 根据题目想到键盘密码，打开txt，发现全是数字，想到九键，每一行的数字个数对应该数字下字母的位置，得到mobilephone，故flag为MRCTF{mobilephone}。

vigenere

题目： 听说你很会密码。

解题思路： 由题目可知是维多尼亚密码，在线解密TXT中的内容，可以发现最后一段提示flag，加上下划线，大括号即可。



由题目可知是维多尼亚密码，在线解密TXT中的内容，可以发现最后一段提示flag，加上下划线，大括号即可。mrctf{vigenere_crypto_crack_man}。