




攻防世界 Misc高手进阶区 6分题 北京地铁

原创

思源湖的鱼  于 2021-01-18 21:48:11 发布  290  收藏 1

分类专栏: [ctf](#) 文章标签: [ctf](#) [攻防世界](#) [misc](#)

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/weixin_44604541/article/details/112785198

版权

CTF

[ctf 专栏收录该内容](#)

200 篇文章 23 订阅

订阅专栏

前言

继续ctf的旅程

攻防世界Misc高手进阶区的6分题

本篇是北京地铁的writeup

发现攻防世界的题目分数是动态的

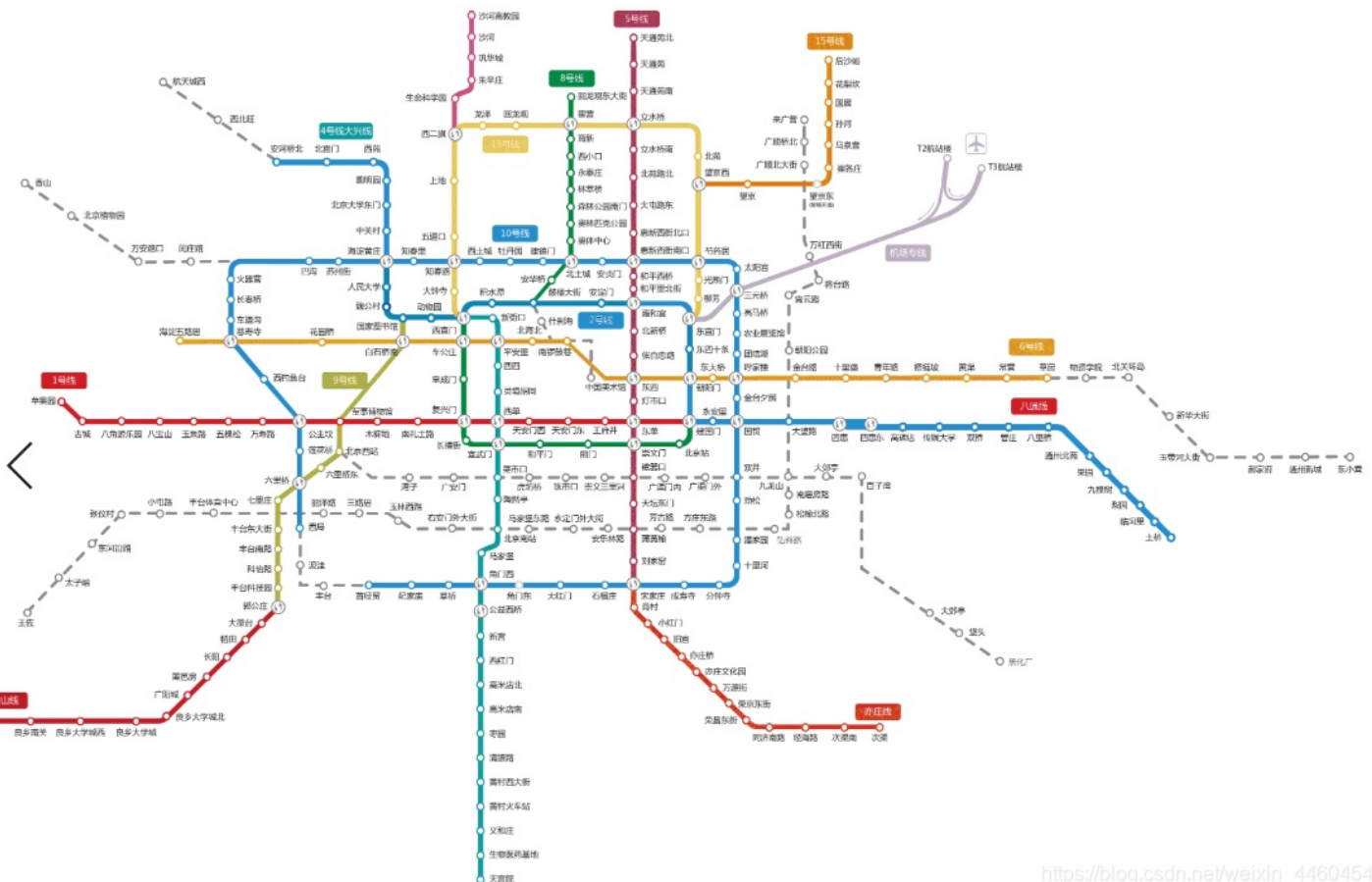
就仅以做题时的分数为准了

解题过程

题目描述

题目描述: Color Threshold 提示: AES ECB密钥为小写字母 提示2: 密钥不足位用斜杠0补全 提示3: 不要光记得隐写不看图片本身啊

拿到一个bmp图片



https://blog.csdn.net/weixin_44604541

扔进stegsolve

发现lsb隐写

```

37537351576d5a35 3234692f7956576f 7sSQWmZ5 24i/yVWo
4d6541494a413d3d ffffffff ffffffff MeAIJA== .....
ffffffff ffffffff .....
ffffffff ffffffff .....
ffffffff ffffffff .....
ffffffff ffffffff .....
ffffffff ffffffff .....
ffffffff ffffffff .....
ffffffff ffffffff .....
ffffffff ffffffff .....
ffffffff ffffffff .....
ffffffff ffffffff .....
ffffffff ffffffff .....
ffffffff ffffffff .....

```

Bit Planes

Alpha 7 6 5 4 3 2 1 0

Red 7 6 5 4 3 2 1 0

Green 7 6 5 4 3 2 1 0

Blue 7 6 5 4 3 2 1 0

Preview Settings

Include Hex Dump In Preview

Order settings

Extract By Row Column

Bit Order MSB First LSB First

Bit Plane Order

RGB GRB

RBG BRG

GBR BGR

https://blog.csdn.net/weixin_44604541

这应该是密文

7sSQWmZ524i/yVWoMeAIJA==

根据提示是AES
密钥应该在图片里

仔细看
发现魏公村的点颜色不一样



估摸着key是weigongcun
解密

AES加密模式: ECB 填充: zeropadding 数据块: 128位 密钥: weigongcun 偏移量: iv偏移量, ecb模式不用 输出: base64 字符集: gb2312编码 (简体)

待加密、解密的文本

```
7SsQVWmZ524i/yVWoMeAIJA==
```

↑ 将你电脑文件直接拖入试试^^

AES加密 AES解密

AES加密、解密转换结果(base64了)

```
DDcITi(Q*2!x@B0)
```

https://blog.csdn.net/weixin_44604541

得到flag

结语

提示给的很足