




BUUCTF 还原大师

原创

宁嘉  于 2020-05-14 13:35:40 发布  2011  收藏

分类专栏: [BUUCTF Crypto](#) 文章标签: [md5](#)

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/MikeCoke/article/details/106118054>

版权



[BUUCTF Crypto](#) 专栏收录该内容

34 篇文章 2 订阅

订阅专栏

还原大师

1

我们得到了一串神秘字符串：TASC?O3RJMV?WDJKX?ZM,问号部分是未知大写字母，为了确定这个神秘字符串，我们通过了其他途径获得了这个字符串的32位MD5码。但是我们获得它的32位MD5码也是残缺不全，E903???4DAB????08?????51?80??8A?,请猜出神秘字符串的原本模样，并且提交这个字符串的32位MD5码作为答案。注意：得到的flag请包上flag{}提交

Flag

Submit

<https://blog.csdn.net/MikeCoke>

MD5爆破：

python3爆破脚本：

```
# -*- coding: utf-8 -*-
#!/usr/bin/env python
import hashlib

#print hashlib.md5(s).hexdigest().upper()
k = 'TASC?O3RJMV?WDJKX?ZM'          #要还原的明文
for i in range(26):
    temp1 = k.replace('?',str(chr(65+i)),1)
    for j in range(26):
        temp2 = temp1.replace('?',chr(65+j),1)
        for n in range(26):
            temp3 = temp2.replace('?',chr(65+n),1)
            s = hashlib.md5(temp3.encode('utf8')).hexdigest().upper()#注意大小写
            if s[:4] == 'E903':      #检查元素
                print (s)          #输出密文
```

得到flag{E9032994DABAC08080091151380478A2}



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)