

bugku 密码学题目writeup整理（1）

原创

[Void&Exists](#) 于 2019-06-25 23:34:33 发布 1820 收藏 6

分类专栏: [CTF](#) 文章标签: [CTF](#) [Writeup](#) [Bugku](#) [网络安全](#) [密码学](#)

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/a1004070060/article/details/93634603>

版权



[CTF 专栏收录该内容](#)

16 篇文章 0 订阅

订阅专栏

1.滴答~滴

Challenge 4873 Solves ×

滴答~滴

20

答案格式KEY{xxxxxxxx}

<https://blog.csdn.net/a1004070060>

如图, 很简单, 摩斯电码解码即可

2.聪明的小羊

Challenge 4612 Solves ×

聪明的小羊

20

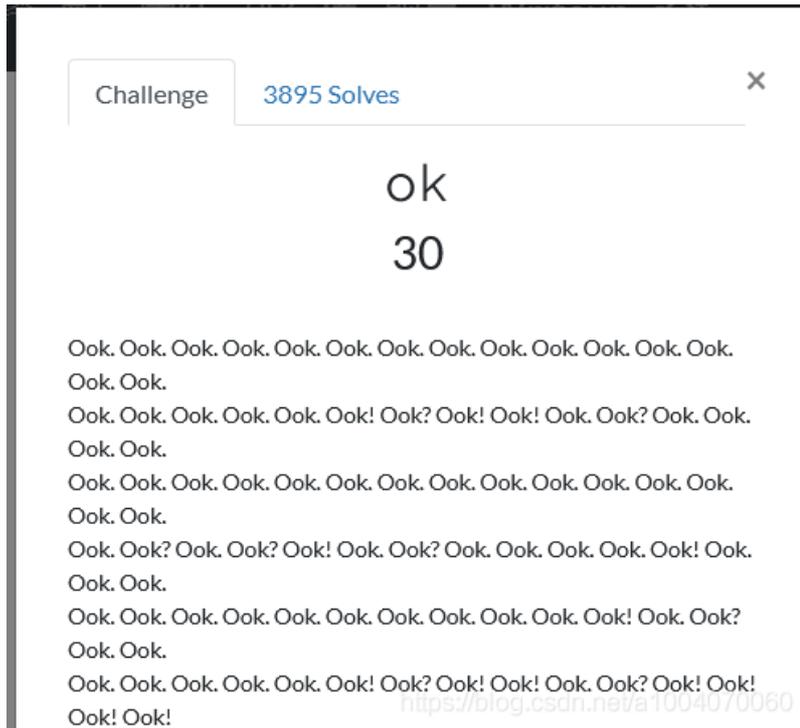
一只小羊翻过了2个栅栏

KYsd3js2E{a2jda}

<https://blog.csdn.net/a1004070060>

根据提示猜测为栅栏密码，随便找个工具解码即可，实在没工具自己手解也很快

3.OK



第一次见到，如果是线下赛见到这种题估计会蒙圈，猜测是Brainfuck的变种，直接百度搜Ook!?解码，找到一个在线网站<https://www.splitbrain.org/services/ook>，复制进去即可。

4.这不是摩斯电码



明显的brainfuck，直接解码即可

5.easy_crypto

Challenge 824 Solves ×

easy_crypto 30

```
0010 0100 01 110 1111011 11 11111 010 000 0 001101 1010 111  
100 0 001101 01111 000 001101 00 10 1 0 010 0 000 1 01111 10  
11110 101011 1111101
```

Flag Submit
<https://blog.csdn.net/a1004070060>

刚开始看到分割的二进制数下意识地转成16进制拿去解码，解完发现不对。观察密文后发现01的分布有点像莫斯密码，于是查表发现F对应的莫斯码正是 ..-，把这串密文复制到记事本里，0用.替换，1用-替换，之后莫斯解码即可。注意：提交之前需要将字符串转为小写，并补上括号。

6.简单加密

Challenge 2267 Solves ×

简单加密 60

```
e6Z9i~]8R~U~QHE{RnY{QXg~QnQ{^XV1RX1p^XI5Q6Q6SKY8jUAA
```

Flag Submit
<https://blog.csdn.net/a1004070060>

刚看到这道题目的时候是有点懵的，不过看这个结构应该是一种ASCII的加法密码，遂写脚本尝试破解：

```
st="e6Z9i~]8R~U~QHE{RnY{QXg~QnQ{^XV1RX1p^XI5Q6Q6SKY8jUAA"  
for i in range(100):  
    stt=""  
    for j in st:  
        stt+=chr(ord(j)-i)  
    print(stt)
```

运行后发现结果里有一串像是base64的东西，拿去解码即可得到flag

```
e6Z9i~]8R~U~QHE {RnY {QXg~QnQ { ^XV1RX1p~XI5Q6Q6SKY8jUAA
d5Y8h} \7Q} T} PGDzQmXzPWf} PmPz] WUkQWko] WH4P5P5RjX7i T@@
c4X7g | [6P | S | OFCyP1Wy0Ve | 010y \VTjPVjn \VG30404QIW6hS??
b3W6f {Z50 {R {NEBxOkVxNUd {NkNx [USiOUim [UF2N3N3PHV5gR>>
a2V5ezY4NzQzMDAwNjUwMTczMjMwZTRhNThlZTE1M2M2OGU4fQ==
1U4dyX3MyPyLC@vMiTvLSbyLiLvYSQgMSgkYSD0L1L1NFT3eP<<
_0T3cxW2Lx0xKB?uLhSuKRaxKhKuYnpSLh0gRcdt0k0MA3004070060
```

7.散乱的密文

Challenge 1991 Solves x

散乱的密文

60

If5{ag024c483549d7fd@@1}
一张纸条上凌乱的写着2 1 6 5 3 4

Flag Submit

<https://blog.csdn.net/a1004070060>

题目意思应该是按照2 1 6 5 3 4的顺序置换列后读出来，但这样读出来的第一行是"flga5{"，估计得出结果还要再栅栏，倒不如直接根据"flag{5"的顺序置换，置换结果横着读出来删掉末尾的@@就是答案

If5{ag
024c48
3549d7
fd@@1}

flag{5
2048c4
53d794
df1}@@

<https://blog.csdn.net/a1004070060>

8.凯撒部长的奖励

Challenge

1491 Solves



凯撒部长的奖励

60

就在8月，超师傅出色地完成了上级的特遣任务，凯撒部长准备给超师傅一份特殊的奖励，兴高采烈的超师傅却只收到一长串莫名的密文，超师傅看到英语字符串便满脸黑线，帮他拿到这份价值不菲的奖励吧。密文：MSW{byly_Cm_sloI_IYqUlx_yhdls_Cn_Wuymul_il_wuff_bcg_pCwnll_cr
题目来源：第七季极客大挑战

Flag

Submit

<https://blog.csdn.net/a1004070060>

凯撒密码，解码即可

这道题的问题在于没有参加过极客挑战赛的人可能不知道flag的提交格式是SYC{}，所可能会采坑

9.一段base64

Challenge

1673 Solves



一段Base64

80

flag格式：flag{xxxxxxxxxxxx}

1.txt

Flag

Submit

<https://blog.csdn.net/a1004070060>

这道题看起来简单，实际做起来异常繁琐。。。长度超限了，下一篇见