

攻防世界-转轮机加密

原创

m0_62094846 于 2022-03-18 15:28:40 发布 100 收藏

文章标签: [安全](#)

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/m0_62094846/article/details/123575585

版权

转轮机加密

最佳Writeup由 [Viking · ZERO_Nu1L](#) 提供

难度系数: ★★★★ 4.0

题目来源: [ISCC2017](#)

题目描述: 你俩继续往前走, 来到了前面的下一个关卡, 这个铺面墙上写了好多奇奇怪怪的 英文字母, 排列的的整整齐齐, 店面前面还有一个大大的类似于土耳其旋转烤肉的架子, 上面一圈圈的 也刻着很多英文字母, 你是一个小历史迷, 对于二战时候的历史刚好特别熟悉, 一拍大腿: “嗨呀! 我知道 是什么东西了! ”。提示: 托马斯·杰斐逊。flag, 是字符串, 小写。

题目场景: 暂无

题目附件: [附件1](#)

CSDN @m0_62094846

```
*a3b693cdec9e4d479285c519ce9c521d.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
1: < ZWAXJGDLUBVIQHKYPNTCRMOSFE <zkwyapxnjtgcdrlmuobsvfieq h
2: < KPBELNACZDTRXMJQOYHGVSFUWI <kcvzpdstbrfxemujlqwonyihag
3: < BDMAIZVRNSJUWFHTEQGYXPLOCK <bwcdufokmjhl astpinexzrqyvg
4: < RPLNDVHGFUCUTEBSXQYIZMJWAO <rfoxapgsqwolhubyj nvkeimdtz
5: < IHFRLABEUOTSGJVDKCPMNZQWXY <ifautgvkpnqx ywzmcjdsobrhle
6: < AMKGGHIWPNYCJBFZDRUSLOQXVET <akinjzrsoxe tvqludbywgmhpcf
7: < GWTHSPYBXIZULVKMRAFDCOEONJQ <gtpxukaefomliyhwsbzvrdn jc
8: < NOZUTWDCVRJLXKISEFAPMYGHBQ <
9: < XPLTDSRFHENYVUBMCQWAOIKZGJ <xbpumlvc tyjdnwgseazrhokfi
10: < UDNAJFBOWTGVRSCZQKELMXYIHP <uedklnqmazjcyfsibrhovpwg t
11: < MNBVCXZQWERTPOIUAYLSKDJFHG <mxifuznqyhawbelgsrvtk dpcoj
12: < LVNCMXZPQOWEIURYTASBKJDFHG <lnxqerakdh gfsyiozcvmpwutb
13: < JZQAWSXCDEFVGBGYHNUMKILOP <jadbnougewzsrmpkyfxqcvhi l

密钥为: 2,3,7,5,13,12,9,1,8,10,4,11,6
密文为: NFQKSEVOQOFNP
```

看题目描述一直用栅栏密码, 也没个结果

但是遗漏了一个重要信息: 托马斯·杰斐逊 (查了下这个人发现没什么用就放弃了)

这是一个加密名杰斐逊转轮密码, 没有解密器

查了下解密方式:

第一部分为加密表，第二部分为密钥，第三部分为密文

按照密钥的数字，第一个是2，选择加密表2: < KPBELNACZDTRXMJQOYHGVSFUWI <

密文第一个是N，把N后面的提前，N前面的放后面NACZDTRXMJQOYHGVSFUWIKPBEL

其他的也是一样

```
< NACZDTRXMJQOYHGVSFUWIKPBEL <
< FHTEQGYXPLOCKBDMALZVRNSJUW <
< QGWITHSPYBXIZULVKMRAFDCEONJ <
< KCPMNZQWXYIHFRLABEUOTSGJVD <
< SXCDERFVBGTYHNUMKILOPJZQAW <
< EIURYTASBKJDFHGLVNCMXZPQOW <
< VUBMCQWAOIKZGJXPLTOSRFHENY <
< OSFEZWAXJGDLUBVIQHKYPNTCRM <
< QNOZUTWDCVRJLXKISEFAPMYGHB <
< OWTGVRSCZQKELMXYIHPUDNAJFB <
< FCUKTEBSXQYIZMJWAORPLNDVHG <
< NBVCXZQWERTPOIUYSKDJFHGM <
< PNYCJBFZDRUSLOQXVETAMKGHIW <
```

(这是别人的图片，不想一个个转了)

发现倒数第九列的字母可以拼出意思

fireinthehole (这个就是flag了，不用加其他的东西)