攻防世界练习题

原创

goblin shelly 于 2020-06-06 23:24:02 发布 570 收藏 2

文章标签： 密码学

本文链接：https://blog.csdn.net/rreally/article/details/106534515

幂数加密

最近在攻防世界里面写了一题，叫幂数加密，我就搜索学习了一边幂数加密，例如E是第五个字母5=2^0+2^2 所以E加密过之后是02；O是第十五个15=2^0+2^1+2^2+2^3所以O加密后是0123。

一打开题目：884210122048022440401422420 24 80122。傻了。哪来的8嘛。后来了解到了一种加密方式叫云影加密。云影密码是01248密码，与二进制幂加密不同，这个加密法采用的是0作间隔，其他非0数隔开后组合起来相加表示序号1-26之一的字母，例如18 = 1+8 = 9 = I，1248 = 1+2+4+8 = 15 = O这样。

特点：密文中仅存在01248,加密对象仅有字母。

所以答案就出来了。

题目：884210122048022440401422420248 0122

改一下：88421/122/48/2244/4/142242/248/122

加一下：23/5/12/12/4/15/14/5

换字母：W/E/L/L/D/O/N/E

所以flag是cyberpeace{WELLDONE}。

Railfence

这是个奇葩类型，用常规工具从2试到20 都不对，但一看就感觉应该是栅栏密码啊。后来查到了一个特殊的栅栏密码叫做WWW的变种

例如：密文为1 2 3 4 5 6 key=3 Rail-fence Cipher

1 . . . 5 . ↘ ↗ ↘

. 2 . 4 . 6 ↘ ↗

. . 3 . . . ↘ ↗

结果为 1 5 2 4 6 3

长见识了。

附解密网站：http://www.atoolbox.net/Tool.php?Id=777

转轮机加密

题目：

1: < ZWAXJGDLUBVIQHKYPNTCRMOSFE <

2: < KPBELNACZDTRXMJQOYHGVSFUWI <

3: < BDMAIZVRNSJUWFHTEQGYXPLOCK <

4: < RPLNDVHGFCUKTEBSXQYIZMJWAO <

5: < IHFRLABEUOTSGJVDKCPMNZQWXY <

6: < AMKGHIWPNYCJBFZDRUSLOQXVET <

7: < GWTHSPYBXIZULVKMRAFDCEONJQ <

8: < NOZUTWDCVRJLXKISEFAPMYGHBQ <

9: < XPLTDSRFHENYVUBMCQWAOIKZGJ <

10: < UDNAJFBOWTGVRSCZQKELMXYIHP <

11： < MNBVCXZQWERTPOIUYALSKDJFHG <

12： < LVNCMXZPQOWEIURYTASBKJDFHG <

13： < JZQAWSXCDERFVBGTYHNUMKILOP <

密钥为：2,3,7,5,13,12,9,1,8,10,4,11,6

密文为：NFQKSEVOQOFNP

这个他有提示：托马斯·杰斐逊

所以直接搜索到了杰斐逊转轮密码。按照这个密码体系来就好了，第二行放到第一栏，第三行放到第二栏，以此类推。得到下表。

2: < KPBELNACZDTRXMJQOYHGVSFUWI <

3: < BDMAIZVRNSJUWFHTEQGYXPLOCK <

7: < GWTHSPYBXIZULVKMRAFDCEONJQ <

5: < IHFRLABEUOTSGJVDKCPMNZQWXY <

13： < JZQAWSXCDERFVBGTYHNUMKILOP <

12： < LVNCMXZPQOWEIURYTASBKJDFHG <

9: < XPLTDSRFHENYVUBMCQWAOIKZGJ <

1: < ZWAXJGDLUBVIQHKYPNTCRMOSFE <

8: < NOZUTWDCVRJLXKISEFAPMYGHBQ <

10: < UDNAJFBOWTGVRSCZQKELMXYIHP <

4: < RPLNDVHGFCUKTEBSXQYIZMJWAO <

11： < MNBVCXZQWERTPOIUYALSKDJFHG <

6: < AMKGHIWPNYCJBFZDRUSLOQXVET <

密钥为：2,3,7,5,13,12,9,1,8,10,4,11,6

然后把重新

2: < NACZDTRXMJQOYHGVSFUWIKPBEL <

3: < FHTEQGYXPLOCKBDMAIZVRNSJUW <

7: < QGWTHSPYBXIZULVKMRAFDCEONJ <

5: < KCPMNZQWXYIHFRLABEUOTSGJVD <

13: < SXCDERFVBGTYHNUMKILOPJZQAW <

12: < EIURYTASBKJDFHGLVNCMXZPQOW <

9: < VUBMCQWAOIKZGJXPLTDSRFHENY <

1: < OSFEZWAXJGDLUBVIQHKYPNTCRM <

8: < QNOZUTWDCVRJLXKISEFAPMYGHB <

10: < OWTGVRSCZQKELMXYIHPUDNAJFB <

4: < FCUKTEBSXQYIZMJWAORPLNDVHG <

11: < NBVCXZQWERTPOIUYALSKDJFHGM <

6: < PNYCJBFZDRUSLOQXVETAMKGHIW <

密文为：NFQKSEVOQOFNP

排序后的表的排头按密文排列，像这样：

然后为了方便，将每一竖列写出来，因为题目要求小写字母提交，所以我誊的时候就将它转化成了小写字母，如下：

1: nfqksevoqofnp
2: ahgcxuusnwcbn
3: ctwpcubfotuvy
4: zetmdrmezgkcc
5: dqhneyczuvtxj
6: tgszrtqwtrezb
7: rvpgfawawsbgf

8: xxywvsaxdcswz
9: mpbxbbojczxed
10: jlxygkigvqqrr
11: qoiitjkdrkytu
12: oczhydzljeips
13: ykufhfgullzol
14: hblrnhjbxmmio
15: gdvlugxvkxjuq
16: vmkamlpiiywyx
17: sambkvlqsiaav
18: fireinthehole
19: uzaulcdkfprst
20: wvfoomsyaupka
21: irdtpxrppdldm
22: kncsjzfnmnnjk
23: psegzphtyadfg
24: bjojqqecgjvhh
25: eunvaonrhfhgi
26: lwjdwwymbbgmw

可以看出唯一一个有意义的是第18个，提交就好了，本题不需要格式，提交小写字母串即可。

本题没有多大难度，就是有耐心即可。

本周总结：不要轻信标题，要保持耐心，多学学传统题型的变种，出题人喜欢变种。