Xctf-转轮机加密

原创

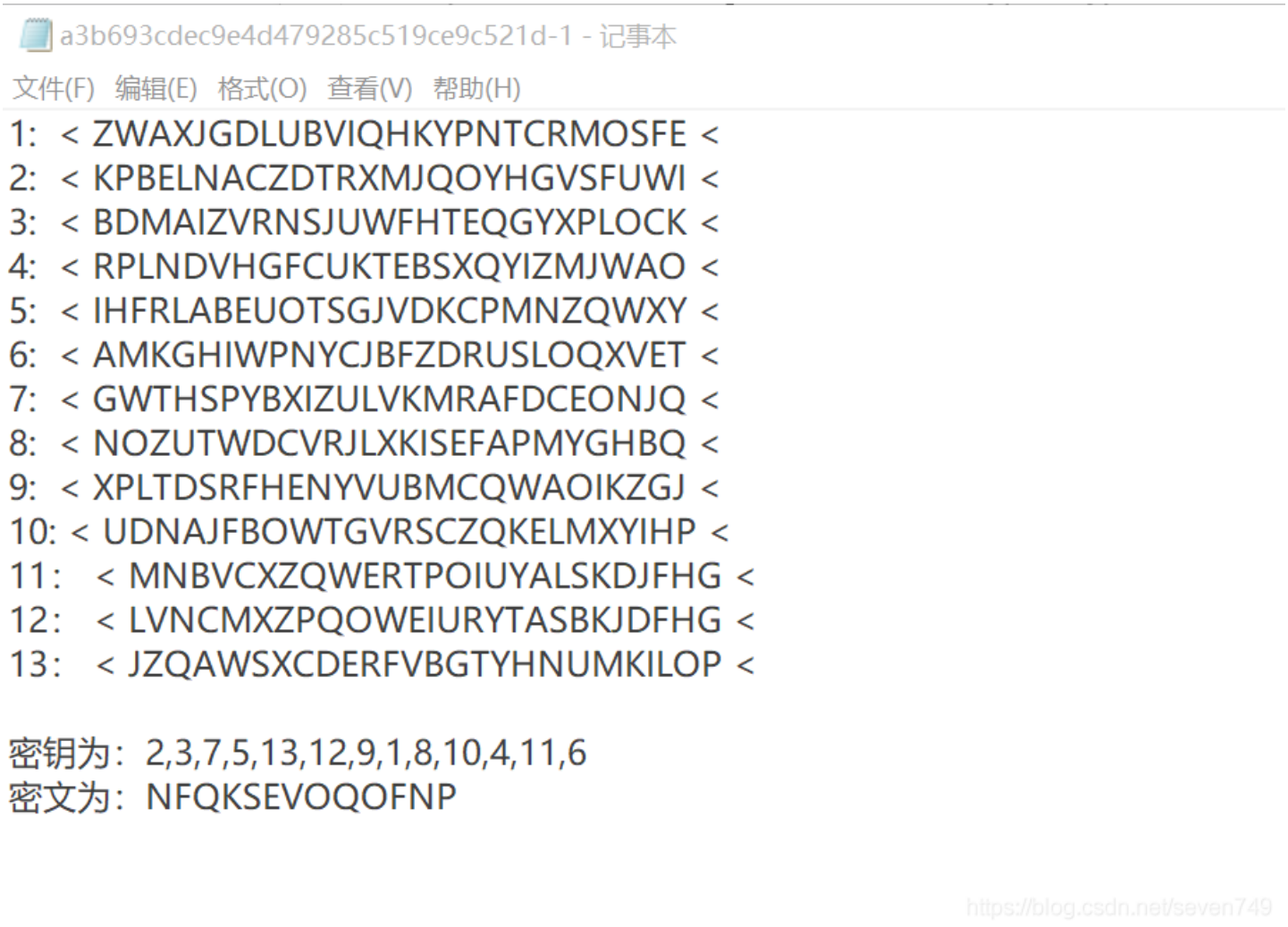
seven749 于 2020-10-14 22:24:57 发布 447 收藏 1

文章标签： cryptoapi 加密解密

本文链接：https://blog.csdn.net/seven749/article/details/109085121

Xctf-转轮机加密

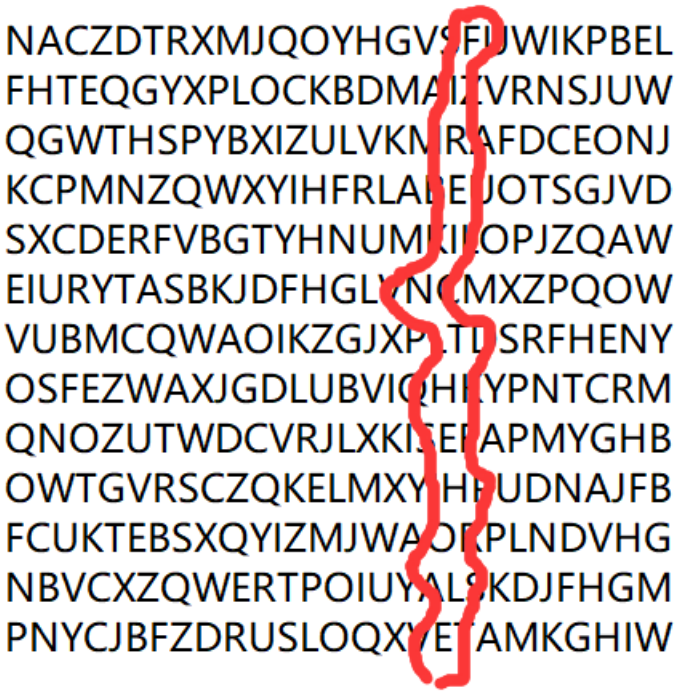
题目给的提示是托马斯·杰斐逊，是转轮加密。我们先了解一下转轮加密的原理：托马斯-杰弗逊转轮加密由三串字符串组成，第一部分为加密表，第二部分为密钥，第三部分为密文。加密表就是我们需要利用密钥和密文来进行加密。



方法1：手动解密

通过观察得到这是一个26*13的字母表，它的密钥一共有13个数，故可联想到行数，首先来看第二行，也就是重新排列，将第二行作为新的第一行；第三行作为新的第二行；依次类推，得到一个新的字母表

通过寻找密文来对其进行旋转，即重新排列，密文共有13个字母，即在每一行中寻找相应的字母进行旋转
密文为：NFQKSEVOQOFNP
即在第一行内寻找字母N作为首字母，对其进行旋转，以此类推，即可得到新的字母表



对应每一列来看发现只有第18列有译义，fire in the hole ，即为flag

方法二：利用代码来解
（来自别人的代码）

```
import re
sss='''1: < ZWAXJGDLUBVIQHKYPNTCRMOSFE < 2: < KPBELNACZDTRXMJQOYHGVSFUWI < 3: < BDMAIZVRNSJUWFHTEQGYXPLOCK < 4:
< RPLNDVHGFCUKTEBSXQYIZMJWAO < 5: < IHFRLABEUOTSGJVDKCPMNZQWXY < 6: < AMKGHIWPNYCJBFZDRUSLOQXVET < 7: < GWTHSPYB
XIZULVKMRAFDCEONJQ < 8: < NOZUTWDCVRJLXKISEFAPMYGHBQ < 9: < XPLTDSRFHENYVUBMCQWAOIKZGJ < 10: < UDNAJFBOWTGVRSCZQ
KELMXYIHP < 11 < MNBVCXZQWERTPOIUYALSKDJFHG < 12 < LVNCMXZPQOWEIURYTASBKJDFHG < 13 < JZQAWSXCDERFVBGTYHNUMKILOP
<
'''
m="NFQKSEVOQOFNP"
content=re.findall(r'< (.*?) <',sss,re.S)
iv=[2,3,7,5,13,12,9,1,8,10,4,11,6]
vvv=[]
ans=""
for i in range(13):
   index=content[iv[i]-1].index(m[i])
   vvv.append(index)
for i in range(0,26):
   flag=""
   for j in range(13):
       flag+=content[iv[j]-1][(vvv[j]+i)%26]
   print flag
```

运行得到结果

NFQKSEVOQOFNP
AHGCXIUSNWCBN
CTWPCUBFOTUVY
ZETMDRMEZGKCC
DQHNEYCZUVTXJ
TGSZRTQWTREZB
RYPQFAWAWSBQF
XXYWVSAXDCSWZ
MPBXBBOJCZXED
JLXYGKIGVQQRR
QOIITJKDRKYTU
OCZHYDZLJEIPS
YKUFHFGULLZOL
HBLRNHJBXMMIO
GDVLUGXVKXJUQ
VMKAMLPIIYWYX
SAMBKVLQSIAAV
FIREINTHEHOLE
UZAULCDKFPRST
WVFOOMSYAUPKA
IRDTPXRPPDLDM
KNCSJZFNMNNJK
PSEGZPHTYADFG
BJOJQQECGJVHH
EUNVAONRHFHGI
LWJDWWYMBBGMW

发现只有第18列有译义，即可得到flag，注意提交格式。