

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](#)

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/seven749/article/details/109085121>

版权

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-杰斐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。

a3b693cdec9e4d479285c519ce9c521d-1 - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
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: < JZQAWSXCDEFVVBGTYHNUMKILOP <
```

密钥为: 2,3,7,5,13,12,9,1,8,10,4,11,6

密文为: NFQKSEVOQOFNP

<https://blog.csdn.net/seven749>

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

```
< KPBELNACZDTRXMJQOYHGVSFUWI <  
< BDMAIZVRNSJUWFHTEQGYXPLOCK <  
< GWTHSPYBXIZULVKMRAFDCEONJQ <  
< IHFRLABEUOTSGJVDKCPMNZQWXY <  
< JZQAWSXCDERFVBGTYHNUMKILOP <  
< LVNCMXZPQOWEIURYTASBKJDFHG <  
7 XPLTDSRFHENYVUBMCQWAOIKZGJ  
< ZWAXJGDLUBVIQHKYPNTCRMOSFE <  
< NOZUTWDCVRJLXKISEFAPMYGHBQ <  
< UDNAJFBOWTGVRSCZQKELMXYIHP <  
< RPLNDVHGFUCUKTEBSXQYIZMJWAO <  
< MNBVCXZQWERTPOIUYSKDJFHG <  
< AMKGHIWPNYCJBFZDRUSLOQXVET <
```

<https://blog.csdn.net/seven749>

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

```
NACZDTRXMJQOYHGVSFUWIKPBEL  
FHTEQGYXPLOCKBDMAIZVRNSJUW  
QGWTSPYBXIZULVKMRAFDCEONJ  
KCPMNZQWXYIHFRLABEUOTSGJVD  
SXCDEFVBGTYHNUMKILOPJZQAW  
EIURYTASBKJDFHGLVNCMXZPQOW  
VUBMCQWAOIKZGJXPLTDSRFHENY  
OSFEZWAXJGDLUBVIQHKYPNTCRM  
QNOZUTWDCVRJLXKISEFAPMYGHB  
OWTGVRSCZQKELMXYIHPUDNAJFB  
FCUKTEBSXQYIZMJWAO RPLNDVHG  
NBVCXZQWERTPOIUYSKDJFHGM  
PNYCJBFZDRUSLOQXVETAMKGHIW
```

<https://blog.csdn.net/seven749>

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: < GWTSPYB
XIZULVKMRAFDCENJQ < 8: < NOZUTWDCVRJLXKISEFAPMYGHBQ < 9: < XPLTDSRFHENYVUBMCQWAOIKZGJ < 10: < UDNAJFBOWTGVRSCZQ
KELMXYIHP < 11 < MNBVCXZQWERTPOIUAYLSKDJFHG < 12 < LVNCMXZPQWEIURYTASBKJDFHG < 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
JLXYGKIGVQQR
QOIITJKDRKYTU
OCZHYDZLJEIPS
YKUFHFGULLZOL
HBLRNHJBXMMIO
GDVLUGXVKXJUQ
VMKAMLPIIYWYX
SAMBKVLQSIAAV
FIREINTHEHOLE
UZAULCDKFPRST
WVFOOMSAYAUPKA
IRDTPXRPPDLDM
KNCSJZFNMMNJK
PSEGZPHTYADFG
BJOJQQECCGJVHH
EUNVAONRHFHGI
LWJDWWYMBBGMW

```

发现只有第18列有译义，即可得到flag，注意提交格式。