XCTF-转轮机加密-WP

原创

lqvir 于 2020-12-22 18:49:02 发布 97 收藏

文章标签： 密码学

本文链接：https://blog.csdn.net/weixin_46227016/article/details/111563898

转轮机加密

首先查看附件信息，一种神奇的加密方式

```
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
```

题目中给出的是 提示转轮机 杰弗逊 经过查询可知未杰弗逊转轮机加密方法，

大佬给的解密原理

利用原理写出朋友python脚本。

```
a=[ 'ZWAXJGDLUBVIQHKYPNTCRMOSFE',
'KPBELNACZDTRXMJQOYHGVSFUWI',
'BDMAIZVRNSJUWFHTEQGYXPLOCK',
'RPLNDVHGFCUKTEBSXQYIZMJWAO',
'IHFRLABEUOTSGJVDKCPMNZQWXY',
'AMKGHIWPNYCJBFZDRUSLOQXVET',
'GWTHSPYBXIZULVKMRAFDCEONJQ',
'NOZUTWDCVRJLXKISEFAPMYGHBQ',
'XPLTDSRFHENYVUBMCQWAOIKZGJ',
'UDNAJFBOWTGVRSCZQKELMXYIHP',
'MNBVCXZQWERTPOIUYALSKDJFHG',
'LVNCMXZPQOWEIURYTASBKJDFHG',
'JZQAWSXCDERFVBGTYHNUMKILOP']

key=[2,3,7,5,13,12,9,1,8,10,4,11,6]
table=[]
for i in key:
    table.append(list(a[i-1]))
s=list('NFQKSEVOQOFNP')
for i in range(0,len(s)):
    index=table[i].index(s[i])
    temp=table[i][0:index]
    table[i][0:index]=[]
    table[i]+=temp
    print(table[i])
for i in table:
    print(chr(ord(i[17])+32),end='')
```

```
['N', 'A', 'C', 'Z', 'D', 'T', 'R', 'X', 'M', 'J', 'Q', 'O', 'Y', 'H', 'G', 'V', 'S', 'F', 'U', 'W', 'I', 'K', 'P', 'B', 'E', 'L']
['F', 'H', 'T', 'E', 'Q', 'G', 'Y', 'X', 'P', 'L', 'O', 'C', 'K', 'B', 'D', 'M', 'A', 'I', 'Z', 'V', 'R', 'N', 'S', 'J', 'U', 'W']
['Q', 'G', 'W', 'T', 'H', 'S', 'P', 'Y', 'B', 'X', 'I', 'Z', 'U', 'L', 'V', 'K', 'M', 'R', 'A', 'F', 'D', 'C', 'E', 'O', 'N', 'J']
['K', 'C', 'P', 'M', 'N', 'Z', 'Q', 'W', 'X', 'Y', 'I', 'H', 'F', 'R', 'L', 'A', 'B', 'E', 'U', 'O', 'T', 'S', 'G', 'J', 'V', 'D']
['S', 'X', 'C', 'D', 'E', 'R', 'F', 'V', 'B', 'G', 'T', 'Y', 'H', 'N', 'U', 'M', 'K', 'I', 'L', 'O', 'P', 'J', 'Z', 'Q', 'A', 'W']
['E', 'I', 'U', 'R', 'Y', 'T', 'A', 'S', 'B', 'K', 'J', 'D', 'F', 'H', 'G', 'L', 'V', 'N', 'C', 'M', 'X', 'Z', 'P', 'Q', 'O', 'W']
['V', 'U', 'B', 'M', 'C', 'Q', 'W', 'A', 'O', 'I', 'K', 'Z', 'G', 'J', 'X', 'P', 'L', 'T', 'D', 'S', 'R', 'F', 'H', 'E', 'N', 'Y']
['O', 'S', 'F', 'E', 'Z', 'W', 'A', 'X', 'J', 'G', 'D', 'L', 'U', 'B', 'V', 'I', 'Q', 'H', 'K', 'Y', 'P', 'N', 'T', 'C', 'R', 'M']
['Q', 'N', 'O', 'Z', 'U', 'T', 'W', 'D', 'C', 'V', 'R', 'J', 'L', 'X', 'K', 'I', 'S', 'E', 'F', 'A', 'P', 'M', 'Y', 'G', 'H', 'B']
['O', 'W', 'T', 'G', 'V', 'R', 'S', 'C', 'Z', 'Q', 'K', 'E', 'L', 'M', 'X', 'Y', 'I', 'H', 'P', 'U', 'D', 'N', 'A', 'J', 'F', 'B']
['F', 'C', 'U', 'K', 'T', 'E', 'B', 'S', 'X', 'Q', 'Y', 'I', 'Z', 'M', 'J', 'W', 'A', 'O', 'R', 'P', 'L', 'N', 'D', 'V', 'H', 'G']
['N', 'B', 'V', 'C', 'X', 'Z', 'Q', 'W', 'E', 'R', 'T', 'P', 'O', 'I', 'U', 'Y', 'A', 'L', 'S', 'K', 'D', 'J', 'F', 'H', 'G', 'M']
['P', 'N', 'Y', 'C', 'J', 'B', 'F', 'Z', 'D', 'R', 'U', 'S', 'L', 'O', 'Q', 'X', 'V', 'E', 'T', 'A', 'M', 'W', 'I', 'K', 'H']
```


有意义的明文为：fireinthehole

就是flag