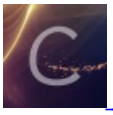
# bugku-writeup-Crypto-托马斯.杰斐逊

原创

dark2019 于 2021-06-24 21:44:01 发布 39 收藏
分类专栏： 信息安全 wp 文章标签： 密码学 wp



题目：托马斯.杰斐逊


**01—找线索**

```
托马斯.txt

1:  <ZWAXJGDLUBVIQHKYPNTCRMOSFE <
2:  <KPBELNACZDTRXMJQOYHGVSFUWI <
3:  <BDMAIZVRNSJUWFHTEQGYXPLOCK <
4:  <RPLNDVHGFCUKTEBSXQYIZMJWAO <
5:  <IHFRLABEUOTSGJVDKCPMNZQWXY <
6:  <AMKGHIWPNYCJBFZDRUSLOQXVET <
7:  <GWTHSPYBXIZULVKMRAFDCEONJQ <
8:  <NOZUTWDCVRJLXKISEFAPMYGHBQ <
9:  <QWATDSRFHENYVUBMCOIKZGJXPL <
10: <WABMCXPLTDSRJQZGOIKFHENYVU <
11: <XPLTDAOIKFZGHENYSRUBMCQWVJ <
12: <TDSWAYXPLVUBOIKZGJRFHENMCQ <
13: <BMCSRFHLTDENQWAOXPYVUIKZGJ <
14: <XPHKZGJTDSENYVUBMLAOIRFCQW <

密钥:  2,5,1,3,6,4,9,7,8,14,10,13,11,12

密文：HCBTSXWCRQGLES
```

通过百度发现这题为斐尔逊转转码加密，观察密钥密文，可能是按密钥顺序行排列，按密文顺序调整每一行首字母为该密文所对应的的字母。

先按密钥行排列：

```
2:  <KPBELNACZDTRXMJQOYHGVSFUWI <
5:  <IHFRLABEUOTSGJVDKCPMNZQWXY <
1:  <ZWAXJGDLUBVIQHKYPNTCRMOSFE <
3:  <BDMAIZVRNSJUWFHTEQGYXPLOCK <
6:  <AMKGHIWPNYCJBFZDRUSLOQXVET <
4:  <RPLNDVHGFCUKTEBSXQYIZMJWAO <
9:  <QWATDSRFHENYVUBMCOIKZGJXPL <
7:  <GWTHSPYBXIZULVKMRAFDCEONJQ <
8:  <NOZUTWDCVRJLXKISEFAPMYGHBQ <
14: <XPHKZGJTDSENYVUBMLAOIRFCQW <
10: <WABMCXPLTDSRJQZGOIKFHENYVU <
13: <BMCSRFHLTDENQWAOXPYVUIKZGJ <
11: <XPLTDAOIKFZGHENYSRUBMCQWVJ <
12: <TDSWAYXPLVUBOIKZGJRFHENMCQ <
```

再按密文调整每行顺序：

```
2:  <HGVSFUWIKPBELNACZDTRXMJQOY<
5:  <CPMNZQWXYIHFRLABEUOTSGJVDK<
1:  <BVIQHKYPNTCRMOSFEZWAXJGDLU<
3:  <TEQGYXPLOCKBDMAIZVRNSJUWFH<
6:  <SLOQXVETAMKGHIWPNYCJBFZDRU<
4:  <XQYIZMJWAORPLNDVHGFCUKTEBS<
9:  <WATDSRFHENYVUBMCOIKZGJXPLQ<
7:  <CEONJQGWTHSPYBXIZULVKMRAFD<
8:  <RJLXKISEFAPMYGHBQNOZUTWDCV<
14: <QWXPHKZGJTDSENYVUBMLAOIRFC<
10: <GOIKFHENYVUWABMCXPLTDSRJQZ<
13: <LTDENQWAOXPYVUIKZGJBMCSRFH<
11: <ENYSRUBMCQWVJXPLTDAOIKFZGH<
12: <SWAYXPLVUBOIKZGJRFHENMCQTD<
```

发现比较特别的一行，XSXSBUGKUADMIN，输入尝试，flag错误，再换小写试试，正确。

tips：

看来转转码加密核心就在于“**转**”，依据密钥和密文转，密钥控制每行位置，密文控制每行顺序。