

BugkuCTF-Crypto题杰斐逊

原创

彬彬有礼am_03 于 2021-08-31 15:03:17 发布 24 收藏

分类专栏: [# BugkuCTF-Crypto](#) 文章标签: [python](#)

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/am_03/article/details/120017453

版权



[BugkuCTF-Crypto 专栏收录该内容](#)

20 篇文章 1 订阅

订阅专栏

打开下载文件

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

密明: 2,5,1,3,6,4,9,7,8,14,10,13,11,12
密文: HCBTSXWCRQGLES
flag格式 flag[你解密的内容]
```

这是一类加密方式, 叫做轮转密码或者叫比尔密码, 解密的方式就是先通过密钥调整字符串的行号, 然后通过密文调整一行字符串的顺序, 例如, 密文的第一个字母是H, 第一行字符串是

```
1 | KPBELNACZDTRXMJQOYHGVSFUWI
```

则, 将H以前的所有字符放到该字符串的末尾

```
1 | HGVSFUWIKPBELNACZDTRXMJQOY
```

知道了解决方法, 下面开始写脚本, 我是先人工将字符串行号排序, 放到一个txt里, 然后才用脚本解密, 脚本如下:

```
#coding:utf-8
#秘钥
key="2,5,1,3,6,4,9,7,8,14,10,13,11,12"
#密文
cipher_text = "HCBTSXWCRQGLS"

f = open("file1.txt")
str_first_encry = []

for line in f:
    line = line.strip()
    str_first_encry.append(line)

key_index = key.split(",")
str_second_encry=[]
for k in key_index:
    str_second_encry.append(str_first_encry[int(k)-1])
    print(str_first_encry[int(k)-1])

for i,ch in enumerate(cipher_text):
    line = str_second_encry[i]
    split_index = line.index(ch)
    temp=[]
    temp[0:len(line)-split_index+1] = line[split_index:len(line)]
    temp[len(temp):] = line[0:split_index]
    str_second_encry[i] = "".join(temp)
print("-----")
for plain in str_second_encry:
    print(plain)
```

运行脚本，生成c.txt文件，仔细观察每一列，在倒数第六列有发现：

```
KPBELNACZDTRXMJQOYHGVSFUWI
IHFRLABEUOTSGJVDKCPMNZQWXY
ZWAXJGDLUBVIQHKYPNTCRMOSFE
BDMAIZVRNSJUWFHTEQGYXPLOCK
AMKGGHIWPNYCJBFZDRUSLOQXVET
RPLNDVHGFUCKTEBSXQYIZMJWAO
QWATDSRFHENYVUBMCOIKZGJXPL
GWTHTSPYBXIZULVKMRAFDCEONJQ
NOZUTWDCVRJLXKISEFAPMYGHBQ
XPHKZGJTDSENYVUBMLAOIRFCQW
WABMCXPLTDSRJQZGOIKFHENYVU
BMCSRFLTDENQWAOXPYVUIKZGJ
XPLTDAOIKFZGHENYSRUBMCQWVJ
TDSWAYXPLVUBOIKZGJRFHENMCQ
-----
HGVSFUWIKPBELNACZDTRXMJQOY
CPMNZQWXYIHFRLABEUOTSGJVDK
BVIQHKYPNTCRMOSFEZWAXJGDLU
TEQGYXPLOCKBDMAIZVRNSJUWFH
SLOQXVETAMKGGHIWPNYCJBFZDRU
XQYIZMJWAORPLNDVHGFUCKTEBS
WATDSRFHENYVUBMCOIKZGJXPLQ
CEONJQGWTHSPYBXIZULVKMRAFD
RJLXKISEFAPMYGHBQNOZUTWDCV
QWXPBKZGJTDSENYVUBMLAOIRFC
GOIKFHENYVUWABMCXPLTDSRJQZ
LTDENQWAOXPYVUIKZGJBMCSRFLH
ENYSRUBMCQWVJXPLTDAOIKFZGH
SWAYXPLVUBOIKZGJRFHENMCQTD
```

```
HGVSFUWIKPBELNACZDTRXMJQOY
CPMNZQWXYIHFRLABEUOTSGJVDK
BVIQHKYPNTCRMOSFEZWAXJGDLU
TEQGYXPLOCKBDMAIZVRNSJUWFH
SLOQXVETAMKGGHIWPNYCJBFZDRU
XQYIZMJWAORPLNDVHGFUCKTEBS|
WATDSRFHENYVUBMCOIKZGJXPLQ
CEONJQGWTHSPYBXIZULVKMRAFD
RJLXKISEFAPMYGHBQNOZUTWDCV
QWXPBKZGJTDSENYVUBMLAOIRFC
GOIKFHENYVUWABMCXPLTDSRJQZ
LTDENQWAOXPYVUIKZGJBMCSRFLH
ENYSRUBMCQWVJXPLTDAOIKFZGH
SWAYXPLVUBOIKZGJRFHENMCQTD
```

解密后为XSXSBUGKUADMIN

提交发现不对

改为小写，flag{xxsbugkuadmin}，成功。



[创作打卡挑战赛](#)

[赢取流量/现金/CSDN周边激励大奖](#)