

CTF密码学Crypto2

转载

宁嘉 于 2020-04-13 13:22:19 发布 674 收藏 1

分类专栏: [BUUCTF Crypto](#) 文章标签: [python](#) [密码学](#)

原文链接: <https://blog.csdn.net/BigRingKing/article/details/100991878>

版权



[BUUCTF Crypto](#) 专栏收录该内容

34 篇文章 2 订阅

订阅专栏

CTF密码学Crypto2

1.转轮加密（托马斯.杰斐逊密码）

1.转轮加密（托马斯.杰斐逊密码）

利用下面的python脚本进行转换解密:

代码来源: 原作者

```
#密钥
key="2,5,1,3,6,4,9,7,8,14,10,13,11,12"
#密文
cipher_text = "HCBTSXWCRQGLS"
f = open(r"C:\Users\MIKEYW\Desktop\mike.txt") #待解密文件的绝对文件名
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)

```

对于待解密文件的绝对文件名就是：绝对路径+文件名

托马斯·杰斐逊

100

```

1: <ZWAXJGDLUBVIQHKYPNTCRMOSFE <2:
<KPBELNACZDTRXMJQOYHGVSFUWI <3:
<BDMAIZVRNSJUWFHTEQGYXPLOCK <4:
<RPLNDVHGFUCUKTEBSXQYIZMJWAO <5:
<IHFRLABEUOTSGJVDKCPMNZQWXY <6:
<AMKGHIWPNYCJBFZDRUSLOQXVET <7:
<GWITHSPYBXIZULVKMRAFDCEONJQ <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

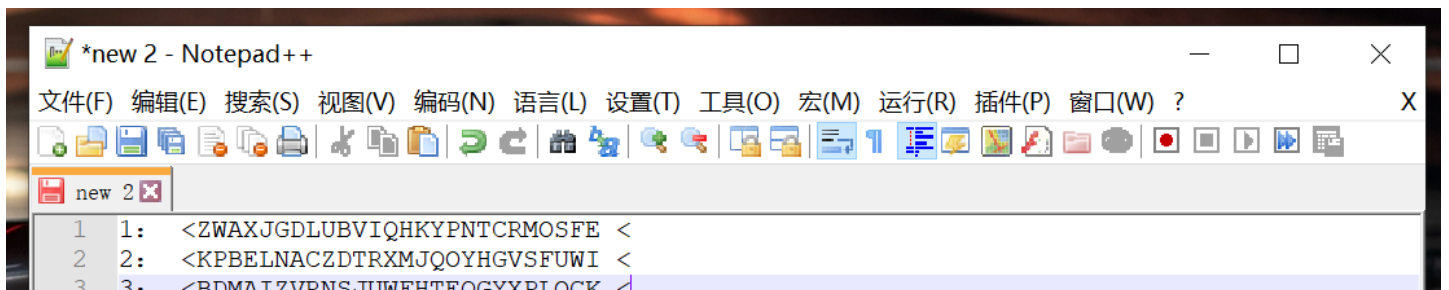
密文： HCBTSXWCRQGLES

flag格式 flag{你解密的内容}

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

解题步骤：

1, 用文本编辑器整理



```
4 4: <RPLNDVHGFCUKTEBSXQYIZMJWAO <
5 5: <IHFRLABEUOTSGJVDKCPMNZQWXY <
6 6: <AMKGHIWPNYCJBFZDRUSLOQXVET <
7 7: <GWTHSPYBXIZULVKMRAFDCEONJQ <
8 8: <NOZUTWDCVRJLXKISEFAPMYGHBQ <
9 9: <QWATDSRFHENYVUBMCOIKZGJXPL <
10 10: <WABMCXPLTDSRJQZGOIKFHENYVU <
11 11: <XPLTDAOIKFZGHENYSRUBMCQWVJ <
12 12: <TDSWAYXPLVUBOIKZGJRFHENMCQ <
13 13: <BMCSRFLHTDENQWAOXPYVUIKZGJ <
14 14: <XPHKZGJTDSENYVUBMLAOIRFCQW <
```

length : 507 lines : 14 Ln : 3 Col : 33 Sel : 0 | 0 Windows (CR LF) UTF-8 IN
<https://blog.csdn.net/MikeCoke>

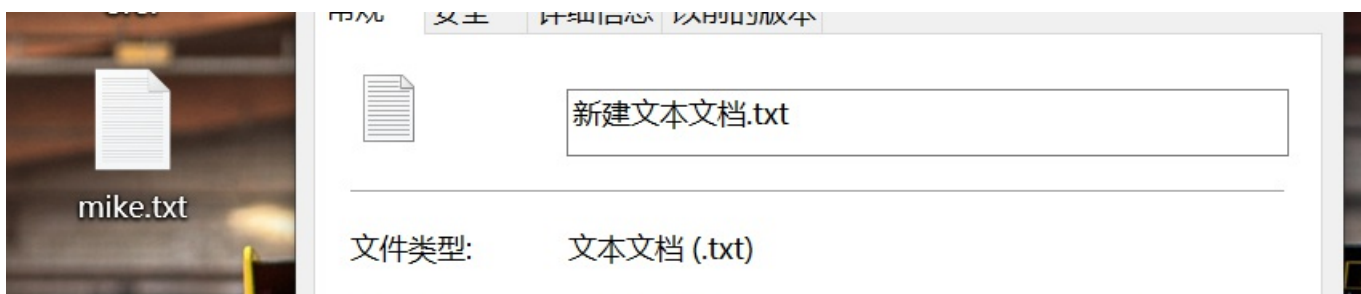
*new 2 - Notepad++

文件(F) 编辑(E) 搜索(S) 视图(V) 编码(N) 语言(L) 设置(T) 工具(O) 宏(M) 运行(R) 插件(P) 窗口(W) ? X

```
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 BMCSRFLHTDENQWAOXPYVUIKZGJ
14 XPHKZGJTDSENYVUBMLAOIRFCQW
```

length : 390 lines : 14 Ln : 8 Col : 27 Sel : 0 | 0 Windows (CR LF) UTF-8 [/blog.csdn.net/MikeCoke](https://blog.csdn.net/MikeCoke) IN

2. 建立txt文本，（可修改文件名）在代码中填入绝对文件名





打开方式:

记事本

更改(C)...

位置:

C:\Users\MIKEWYW\Desktop

大小:

390 字节 (390 字节)

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

3, 用

IDLE运行python代码:

```
Python 3.8.0 Shell
File Edit Shell Debug Options Window Help
Python 3.8.0 (tags/v3.8.0:fa919fd, Oct 14 2019, 19:37:50) [MSC v.1916 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" >>>

转轮加密.py - G:\helo.py\转轮加密.py (3.8.0)
File Edit Format Run Options Window Help
#秘钥
key="2, 5, 1, 3, 6, 4, 9, 7, 8, 14, 10, 13, 11, 12"
#密文
cipher_text = "HCBTSXWCRQGLS"

f = open(r"C:\Users\MIKEWYW\Desktop\mike.txt") #待解密文件绝对地址
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]
    print(line)
    line = temp
    str_second_encry[i] = line
```

```
Python 3.8.0 Shell
File Edit Shell Debug Options Window Help
Python 3.8.0 (tags/v3.8.0:fa919fd, Oct 14 2019, 19:37:50) [MSC v.1916 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
===== RESTART: G:\helo.py\转轮加密.py =====
=====
KPBELNACZDTRXMJQOYHGVSFUWI
IHFRLABEUOTSGJVDKCPMNZQWXY
ZWAXJGDLUBVIQHKYPNTRMOSFE
BDMAIZVRNSJUWFHTEQGYXPLOCK
AMKGHIWPNYCJBFZDRUSLOQXVET
RPLNDVHGFCUKTEBSXQYIZMJWAO
QWATDSRFHENYVUBMCOIKZGJXPL
GWTHTSPYBXIZULVKMRAFDCEONJQ
NOZUTWDCVRJLXKISEFAPMYGHBQ
XPHKZGJTDSENYVUBMLAOIRFCQW
WABMCXPLTDSRJQZGOIKFHENYVU
=====
```

```
BMCSRFLTDENQWAOXPYVUIKZGJ
XPLTDAOIKFZGHENYSRUBMCQWVJ
TDSWAYXPLVUBOIKZGJRFHENMCQ

HGVSFUWIKPBELNACZDTRXMJQOY
CPMNZQWXYIHFRLABEUOTSGJVDK
BVIQHKYPNTRMOSFEZWAXJGDLU
TEQGYXPLOCKBDMAIZVRNSJUWFH
SLOQXVETAMKGHIWPNYCJBFZDRU
XQYIZMJWAORPLNDVHGFCUKTEBS
WATDSRFHENYVUBMCOIKZGJXPLQ
CEONJQGwthSPYBXIZULVKMRAFD
RjLxkiSEFAPMYGHBQNOZUTWDCV
QWXPkZGjTdsENYVUBMLAOIRFC
GOIKfHENYVUWABMCXPLTDSRjQZ
LTDENQWAOXPYVUIKZGJBMCSRfH
ENYSRUBMCQWVJXPLTDAOIKFZGH
SWAYXPLVUBOIKZGJRFHENMCQTD
>>>
```

4,转换

为小写，寻找flag,在倒数第六列:

```
*new 2 - Notepad++
文件(F) 编辑(E) 搜索(S) 视图(V) 编码(N) 语言(L) 设置(T) 工具(O) 宏(M) 运行(R) 插件(P) 窗口(W) ?
hgvsfuwikipbelnaczdtrxmjqoy
cpmnzqwxxyihfrlabeuotsgjvdk
bviqhkypntcrmosfezwaxjgdlu
teqgyxplockbdmaizvrnsjuwfh
sloqxvetamkghiwpnycjbfzdru
xqyizmjwaorplndvhgfcuktebs
watdsrfhenyvubmcoikgexplq
ceonjggwthspybxizulvkmrafd
rjlxkisefapmyghbqnozutwdcv
qwxphkzgjtdsenyvubmlaoirfc
goikfhenyvuwabmcxpltdsrjqz
ltdenqwaoxyvuiKZGjBmCsrFH
enysrubmcqWVjXpLTdaoIKfZGH
swayxplvuboiKZGjRfHnMcQTD

length: 390 lines: 14 Ln: 8 Col: 27 Sel: 0 | 0 Windows (CR LF) UTF-8
```

5. 提交答案:

密钥: 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}

flag{xsxsbugkuadmin}



Submit

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