CTF密码学Crypto2

转载

宁嘉 于 2020-04-13 13:22:19 发布

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

CTF密码学Crypto2

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

```
#秘钥
key="2,5,1,3,6,4,9,7,8,14,10,13,11,12"
#密文
cipher_text = "HCBTSXWCRQGLES"
f = open(r"C:\Users\MIKEWYW\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

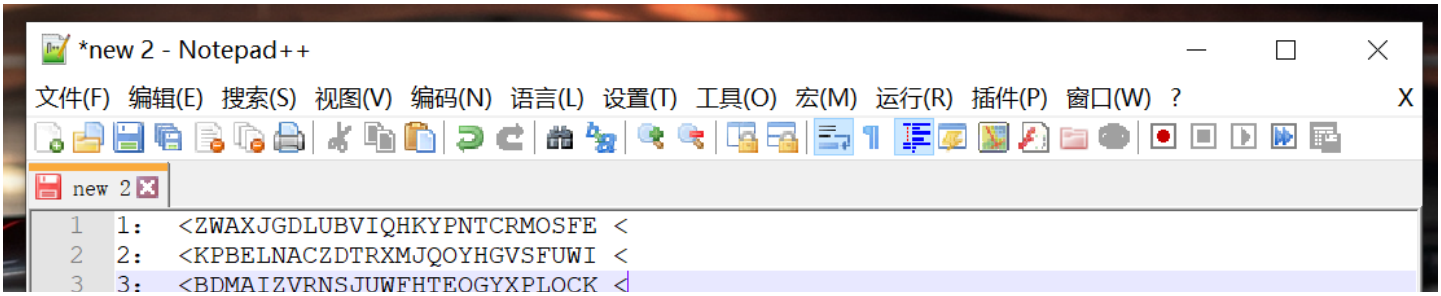
托马斯.杰斐逊

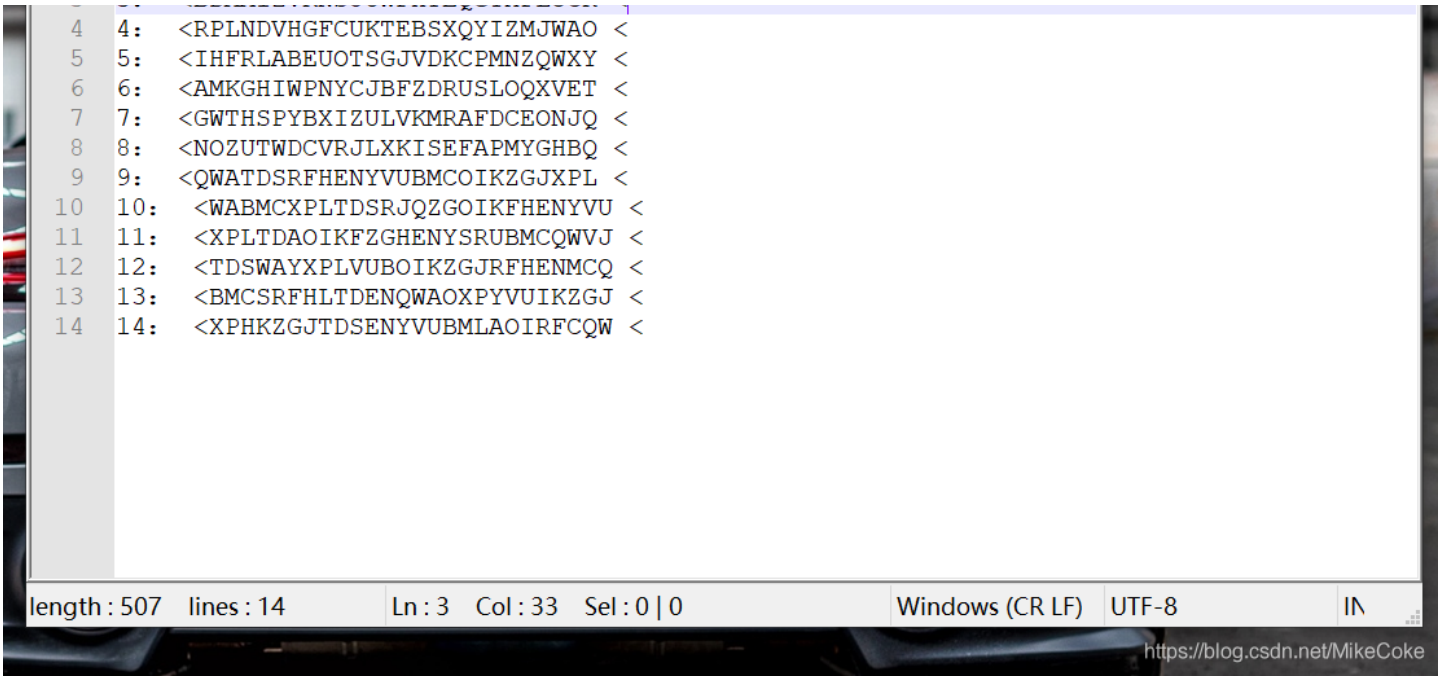
100

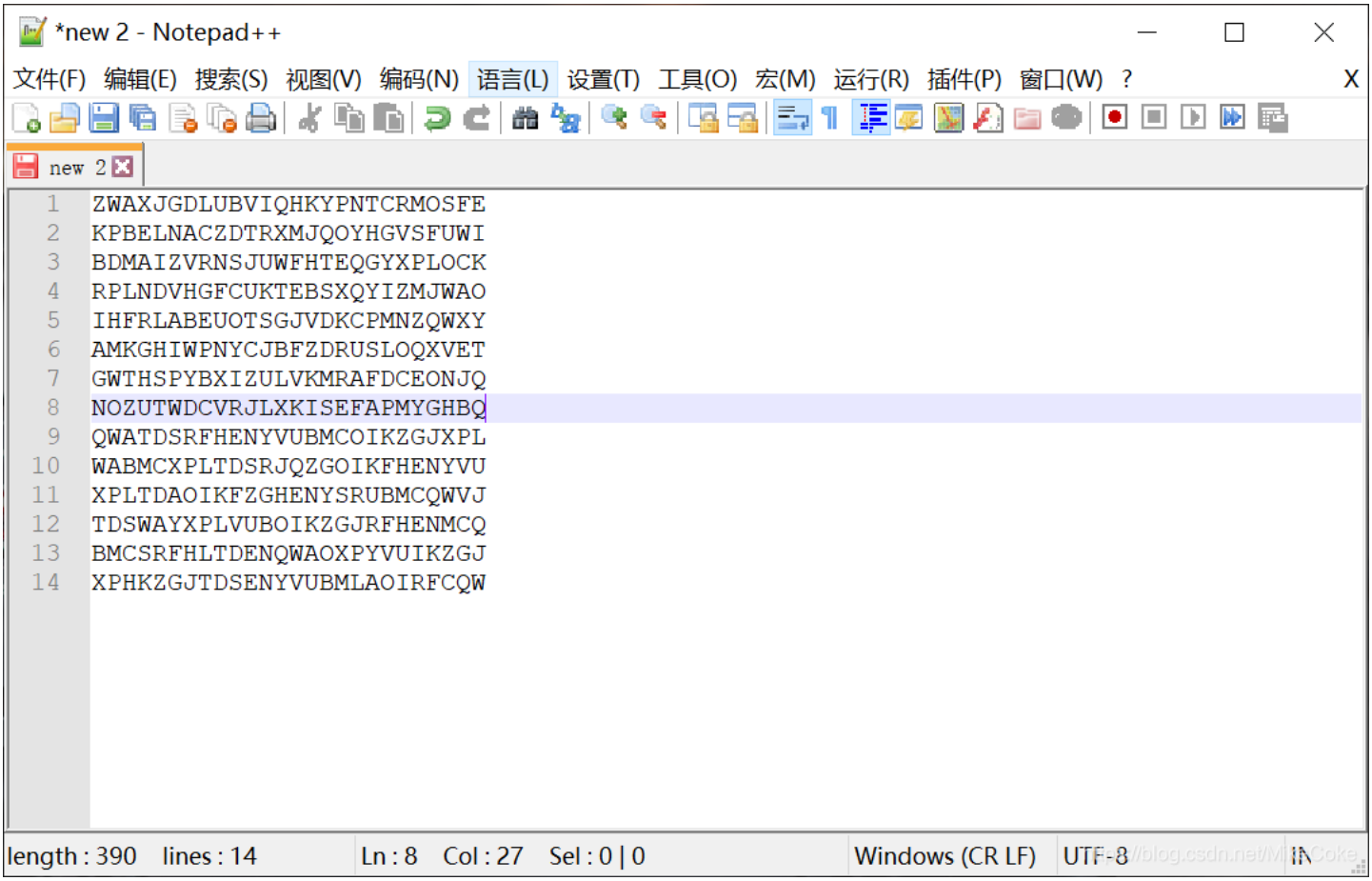
1: <ZWAXJGDLUBVIQHKYPNTCRMOSFE <2:
<KPBELNACZDTRXMJQOYHGVSFUWI <3:
<BDMAIZVRNSJUWFHTEQGYXPLOCK <4:
<RPLNDVHGFCUKTEBSXQYIZMJWAO <5:
<IHFRLABEUOTSGJVDKCPMNZQWXY <6:
<AMKGHIWPNYCJBFZDRUSLOQXVET <7:
<GWTHSPYBXIZULVKMRAFDCEONJQ <8:
<NOZUTWDCVRJLXKISEFAPMYGHBQ <9:
<QWATDSRFHENYVUBMCOIKZGJXPL <10:
<WABMCXPLTDSRJQZGOIKFHENYVU <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
flag格式 flag{你解密的内容}

解题步骤：

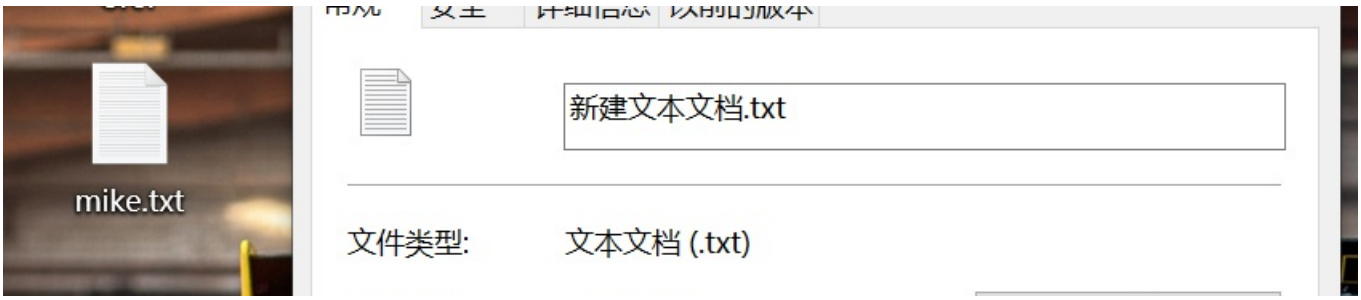
1，用文本编辑器整理





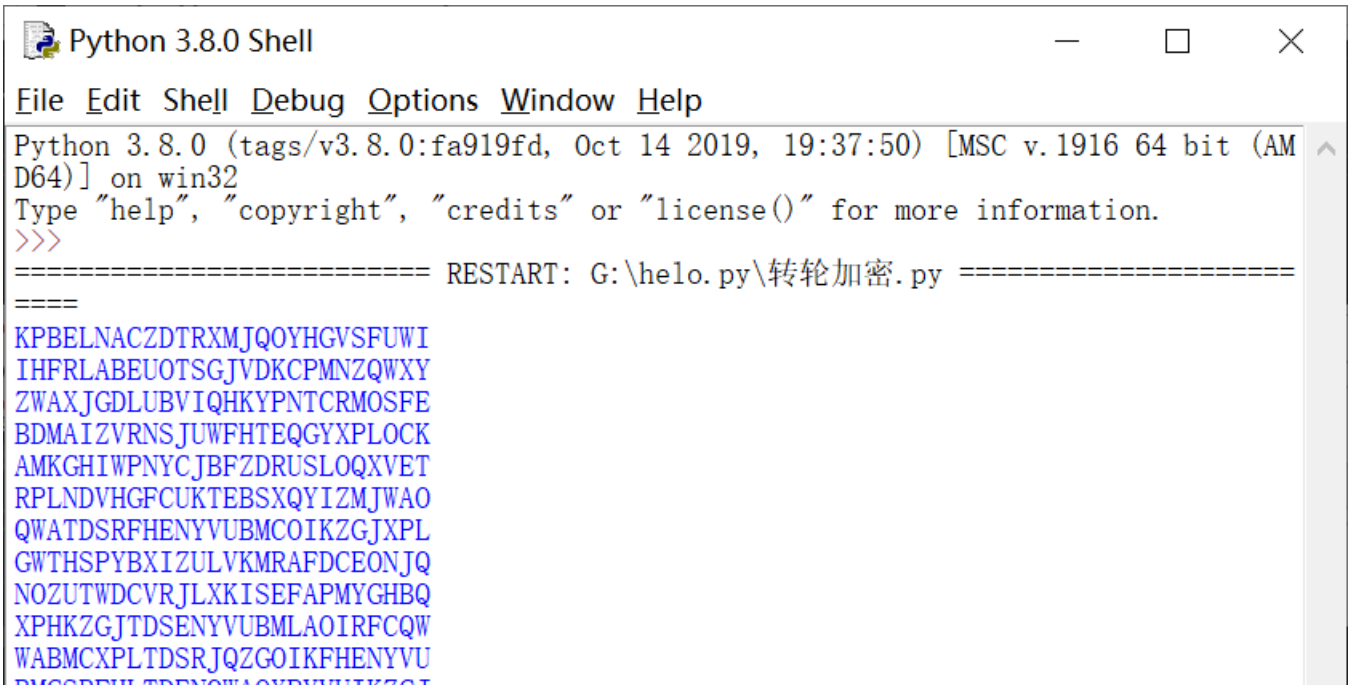


2，建立txt文本，（可修改文件名）在代码中填入**绝对文件名**



3，用

IDLE运行python代码：

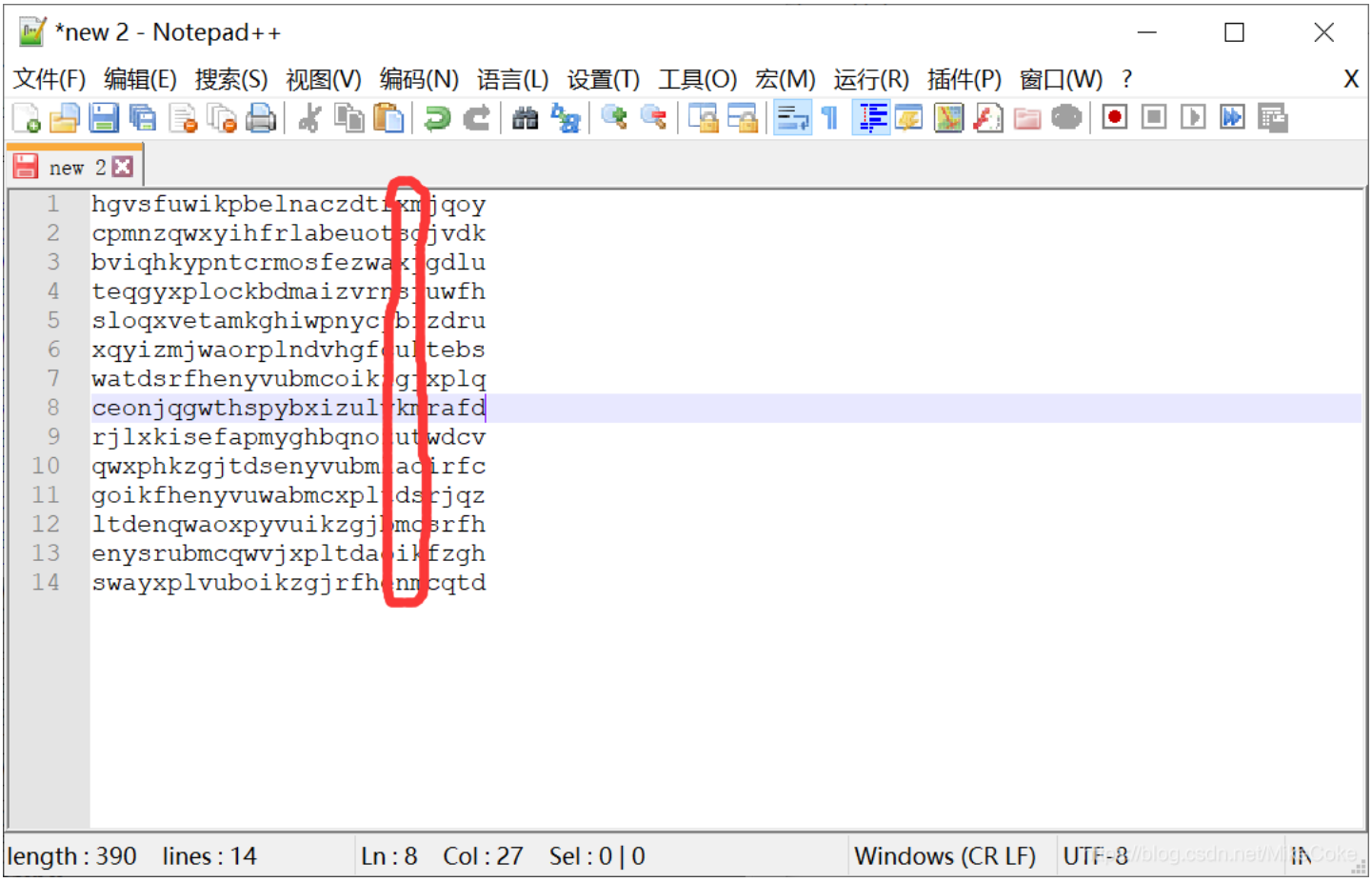


```
BMCSRFHLTDENQWAOXPYVUIKZGJ
XPLTDAOIKFZGHENYSRUBMCQWVJ
TDSWAYXPLVUBOIKZGJRFHENMCQ
------------------------------------
HGVSFUWIKPBELNACZDTRXMJQOY
CPMNZQWXYIHFRLABEUOTSGJVDK
BVIQHKYPNTCRMOSFEZWAXJGDLU
TEQGYXPLOCKBDMAIZVRNSJUWFH
SLOQXVETAMKGHIWPNYCJBFZDRU
XQYIZMJWAORPLNDVHGFCUKTEBS
WATDSRFHENYVUBMCOIKZGJXPLQ
CEONJQGWTHSPYBXIZULVKMRAFD
RJLXKISEFAPMYGHBQNOZUTWDCV
QWXPHKZGJTDSENYVUBMLAOIRFC
GOIKFHENYVUWABMCXPLTDSRJQZ
LTDENQWAOXPYVUIKZGJBMCSRFH
ENYSRUBMCQWVJXPLTDAOIKFZGH
SWAYXPLVUBOIKZGJRFHENMCQTD
>>>
```

Ln: 34 Col: 4

4,转换

为小写，寻找flag,在倒数第六列：



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