bugku 密码学题目writeup整理（2）

原创

Void&Exists 于 2019-06-26 21:38:12 发布 925 收藏 4
分类专栏： CTF 文章标签： CTF 密码学 网络安全 bugku

> 接上一篇

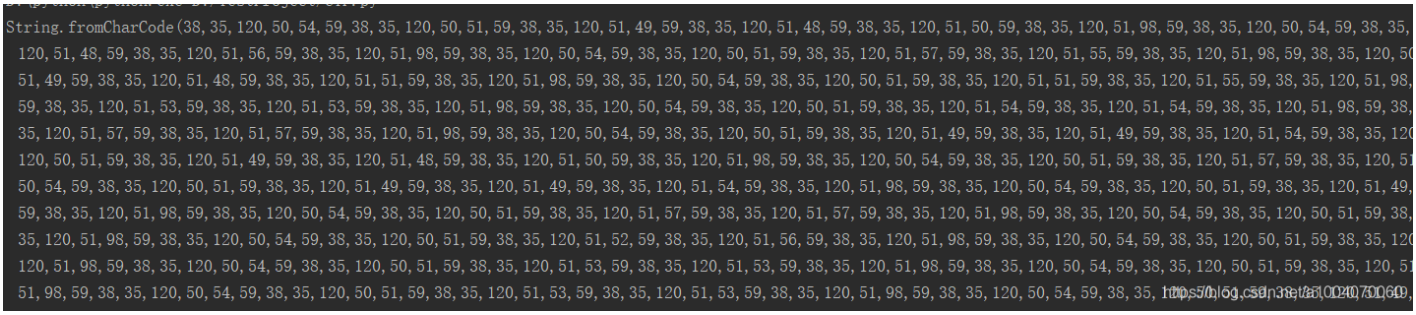
9.一段base64

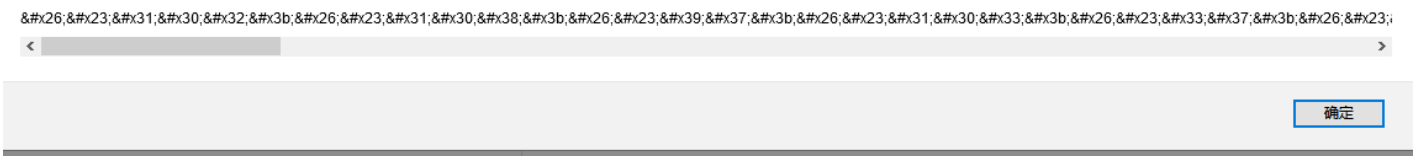
先贴代码（密文太长，只能贴图）

```
import base64
st="XDEzNFwxNzBcNjVcMTQzXDEzNFwxNzBcNjdcNjVcMTM0XDE3MFw2M1w2MFwxMzRcMTcwXDYzXDYwXDEzNFwxNzBcN
key1=str(base64.b64decode(st),'utf-8')#base64解码
key2=""
key1=key1[1:].split("\\")
# 八进制转ascii
for i in key1:
    key2+=chr(int(i,8))
key2=key2[2:].split("\\x")
#16进制解码
key3=""
for i in key2:
    key3+=str(bytes.fromhex(i),'utf-8')
key4=""
key3=key3[4:].split("\\u00")
#再次解码
for i in key3:
    key4+=str(bytes.fromhex(i),'utf-8')
key4=key4[20:-1].split(",")
key5=""
#ASCII解码
for i in key4:
    key5+=chr(int(i))
key5=key5[3:-1].split(";&#x")
key6=""
for i in key5:
    key6+=str(bytes.fromhex(i),'utf-8')
key6=key6[2:-1].split(";&#")
key7=""
for i in key6:
    key7+=chr(int(i))
print(key7)
```


本题思维含量不高但是过程很繁琐，涉及到7次编码，分别解码即可，截图都贴上来实在是太占地方了，看代码吧。。

需要注意的是第4步解出是一段js代码，可以直接放到控制台里执行，也可以写脚本转化





10..!?

依然是Ook解码，在线解码地址https://www.splitbrain.org/services/ook

11.+[]-

brainfuck解码

12.奇怪的密码

"gndk"对应"flag"分别减1、2、3、4，根据规律写脚本推出明文即可

```
astr="gndk€rlqhmtkwwp}z"
tp=1
flag=""
for i in astr:
    flag+=chr(ord(i)-tp)
    tp+=1
print(flag)
```

13.托马斯.杰斐逊

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

杰斐逊总统发明过转轮加密器，所以猜测本题应该与转轮加密有关，首先将这14行字符串按照密钥顺序排列

```
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
```

再按照密文转动转轮得到新的排列

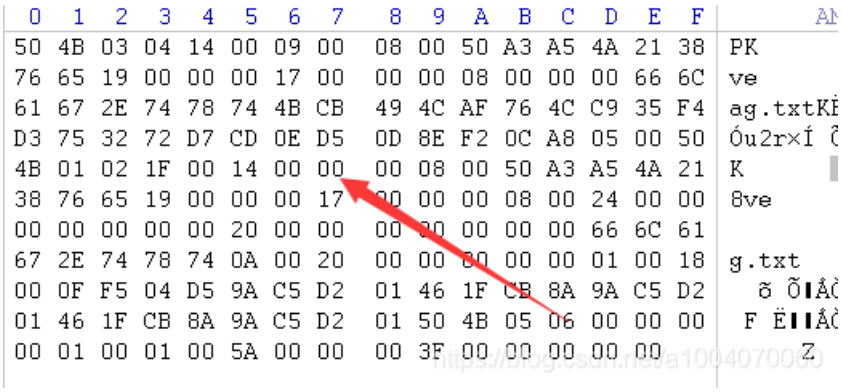
```
HGVSFUWIKPBELNACZDTRXMJQOY
CPMNZQWXYIHFRLABEUOTSGJVDK
BVIQHKYPNTCRMOSFEZWAXJGDLU
TEQGYXPLOCKBDMAIZVRNSJUWFH
SLOQXVETAMKGHIWPNYCJBFZDRU
XQYIZMJWAORPLNDVHGFCUKTEBS
WATDSRFHENYVUBMCOIKZGJXPLQ
CEONJQGWTHSPYBXIZULVKMRAFD
RJLXKISEFAPMYGHBQNOZUTWDCV
QWXPHKZGJTDSENYVUBMLAOIRFC
GOIKFHENYVUWABMCXPLTDSRJQZ
LTDENQWAOXPYVUIKZGJBMCSRFH
ENYSRUBMCQWVJXPLTDAOIKFZGH
SWAYXPLVUBOIKZGJRFHENMCQTD
```

排列完成后顺序读出每一列，找出有实际意义的字符串。说实话挺难找的，仔仔细细找了好几遍才看到有bugku和admin两个单词的一条，最后别忘了转成小写

```
key=open("KEY.txt",'r')
a=[]
for i in key:
    a.append(i)
for j in range(26):
    str=""
    for k in range(len(a)):
        str+=a[k][j]
    print(str)
```

14.ZIP伪加密

利用ZIP伪加密原理，把压缩包拖到16进制编辑器里，找到第二组“504B”，将其后7位的“09”改为“00”即可。



```
 0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
50 4B 03 04 14 00 09 00  08 00 50 A3 A5 4A 21 38  PK
76 65 19 00 00 00 17 00  00 00 08 00 00 00 66 6C  ve
61 67 2E 74 78 74 4B CB  49 4C AF 76 4C C9 35 F4  ag.txtKÌ
D3 75 32 72 D7 CD 0E D5  0D 8E F2 0C A8 05 00 50  Óu2r×Í Õ
4B 01 02 1F 00 14 00 00  00 08 00 50 A3 A5 4A 21  K
38 76 65 19 00 00 00 17  00 00 00 08 00 24 00 00  8ve
00 00 00 00 00 20 00 00  00 00 00 00 00 66 6C 61
67 2E 74 78 74 0A 00 20  00 00 00 00 00 01 00 18  g.txt
00 0F F5 04 D5 9A C5 D2  01 46 1F CB 8A 9A C5 D2    õ ÕÅÒ
01 46 1F CB 8A 9A C5 D2  01 50 4B 05 06 00 00 00   F ËÅÒ
00 01 00 01 00 5A 00 00  00 3F 00 00 00 00 00       Z
```

15.告诉你一个秘密

很有意思的一道题目，拿到16进制密文先转字符串得到一串base64

```
cjV5RyBscDlJIEJqTSB0RmhCVDZ1aCB5N2lKIFFzWiBiaE0g
```

解码后得到一组空格间隔的字符串

```
r5yG lp9I BjM tFhBT6uh y7iJ QsZ bhM
```

刚看到这堆东西我是崩溃的，尝试了很多方式都没结果，一筹莫展之际低头看看键盘发现每一组字符正好对应键盘上一圈按键，中间都包围着另一个键，于是尝试将结果读出，提交，100pt到手！(提交的时候不要加任何其他格式，以大写形式提交)

16.这不是MD5

飞花，当然不是MD5，有经验的话看到666c就知道flag差不多已经出来了，直接hex解码即可，100pt水的过分了。。

17.贝斯家族

base91编码，之前没见过，真心做吐了。国内能找到的在线解码网站大部分都开始收费了，找到一个github上的项目，运行代码解码即可。https://github.com/aberaud/base91-python

18.富强民主

Challenge 1599 Solves

富强民主

100

公正公正公正诚信文明公正民主公正法治法治友善平等和谐敬业和谐富强和谐富强和谐文明和谐平等公正公正和谐法治公正公正公正文明和谐民主和谐敬业和谐平等和谐敬业和谐敬业和谐和谐和谐公正法治友善法治

Flag

Submit

核心价值观编码，线上解码工具解码即可