

CTFshow-CRYPTO（持续更新）

原创

[i_kei](#) 于 2020-11-25 15:31:24 发布 7295 收藏 50

分类专栏: [CTFshow](#) 文章标签: [密码学](#) [编码学](#)

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/i_kei/article/details/110086135

版权



[CTFshow](#) 专栏收录该内容

9 篇文章 7 订阅

订阅专栏

目录

[密码学签到](#)

[crypto2](#)

[crypto3](#)

[crypto4](#)

[crypto5](#)

[crypto6](#)

[crypto7](#)

[crypto8](#)

[crypto9](#)

[crypto10](#)

[crypto11](#)

[crypto0](#)

[crypto12](#)

[crypto13](#)

[crypto14](#)

[萌新_密码5](#)

[内部赛_密码2](#)

密码学签到

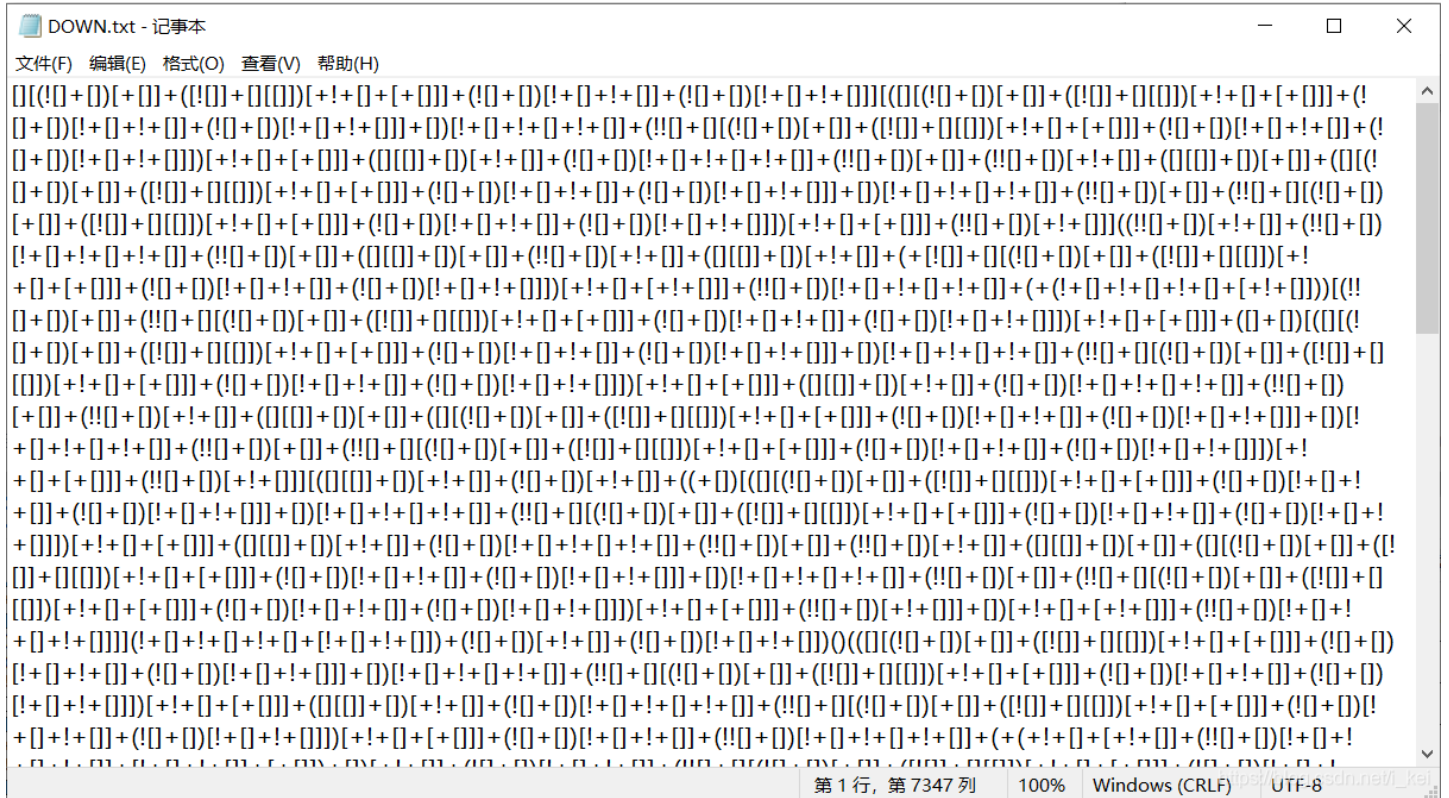
}wohs.ftc{galf

将字符串逆序即可

```
letters = '}wohs.ftc{galf'
a = list(letters)
a.reverse()

for letters in a:
    print(letters,end='')
```

crypto2



打开浏览器的控制台，复制粘贴回车即可得到flag



crypto3



这一题同上



crypto4

crypto4

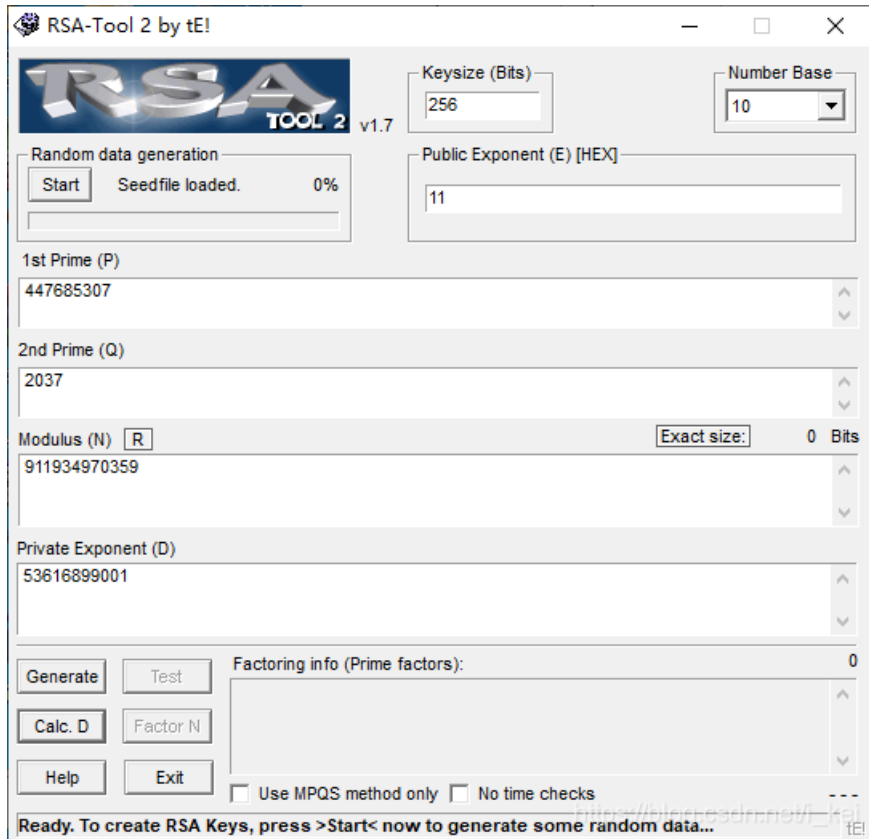
1

p=447685307 q=2037 e=17

提交flag{d}即可

https://blog.csdn.net/j_kei

如图填写即可，一开始e填写的是17，一直回答错误，后来经过群内大佬提醒软件的e是十六进制的，17转十六进制就是0x11



crypto5

crypto5

1

$p=447685307$ $q=2037$ $e=17$ $c=704796792$

提交flag{m}

$m = c \cdot d \pmod n$

$m = 704796792^{53616899001} \pmod{911934970359}$

求出 $m=904332399012$

The image shows two software windows side-by-side. The left window is 'RSA-Tool 2 by tE!' v1.7. It displays RSA key generation parameters: Key size (Bits) is 256, Number Base is 10, Public Exponent (E) [HEX] is 11. The 1st Prime (P) is 447685307, the 2nd Prime (Q) is 2037, the Modulus (N) is 911934970359, and the Private Exponent (D) is 53616899001. The right window is 'Big Integer Calculator v1.13'. It shows a calculation with X=704796792, Y=53616899001, and Z=911934970359. The result of the calculation is shown as 'Ans' = 904332399012. The calculator also shows various mathematical operations like X-Y, X+Y, X*Y, X/Y, A^X+B^Y, X^A+Y^B+Z, X^Y MOD Z, X!, Prime(X), X^n, X^(1/n), GCD(X, Y), X^Y*Z^A^B, and X^A*Y^B MOD Z. The base is set to 10, and the bit lengths are x=30, y=36, z=40, a=0, b=30, ans=40.

crypto6

密文:

U2FsdGVkX19mGsGlfI3nciNVpWZZRqZO2PYjJ1ZQuRqoiknyHSWeQv8ol0uRZP94
MqeD2xz+

密钥:

加密方式名称

Rabbit加密 (get\新加密方式)

在线Rabbit算法加密解密工具

U2FsdGVkX19mGsGlfI3nciNVpWZZRqZO2PYjJ1ZQuRqoiknyHSWeQv8ol0uRZP94
MqeD2xz+

Rabbit

Rabbit加密

Rabbit解密

清空输入框

复制结果文本

flag{a8d.

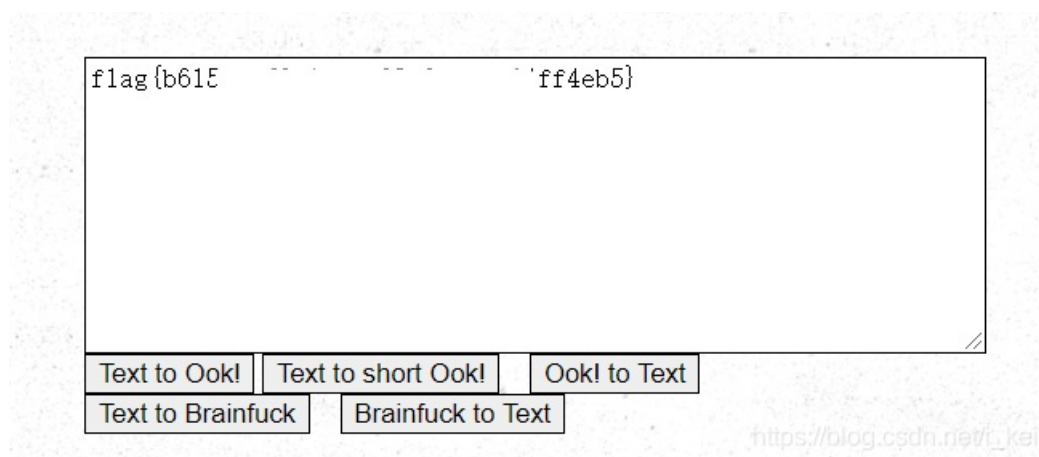
554fc9}

https://blog.csdn.net/j_kei

Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook? Ook. Ook? Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook! Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook. Ook? Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook! Ook! Ook! Ook!
Ook! Ook! Ook? Ook. Ook? Ook! Ook. Ook? Ook! Ook! Ook! Ook! Ook! Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook. Ook? Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook? Ook. Ook? Ook! Ook. Ook? Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook! Ook! Ook! Ook!
Ook! Ook! Ook! Ook! Ook! Ook! Ook? Ook. Ook? Ook! Ook. Ook? Ook! Ook. Ook?
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook?
Ook! Ook! Ook. Ook? Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook!
Ook! Ook? Ook. Ook? Ook! Ook. Ook? Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook!
Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook. Ook! Ook! Ook! Ook! Ook!
Ook! Ook! Ook! Ook! Ook! Ook! Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook? Ook. Ook? Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook.
Ook Ook Ook Ook Ook Ook Ook Ook Ook Ook Ook Ook Ook Ook Ook Ook

ook加密

ook解密网站



crypto8

m(2).txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```

+++++ ++++++ [->+ ++++++ +++++<] >+.,+ ++++++ .<++++ [->-- <]>- .,+++ +++++.<
+++++ [->+ +++++ +<]>+ +++++.< ++++++ +++++[- >----- < ]>-. .-.-.-.-.-.-.-.-.-.-.
+++++ +.,- -.-.<+ ++++++ +[->+ ++++++ +<]>+ +.,<+ ++++++ [->----- <] >-----
----- .----- .<+ ++++++ [->+ +++++ +<] >+ ++++++ ++++++ +++++.< ++++++ + +[-> -----
--<]> .,+.,- ----- .<+ ++++++ +++++[- >+ +++++ +++++<] >+ +++++. --.<+ ++++++ [->----- <
]>----- ----- .+ .<+ +++++ +++++[- >+ +++++ +++++<]> ++++++ ++++++ +++++.<+ ++++++ [->--
----- < ]>----- ----- .- .+ +++++ .<+ +++++ +++++[- >+ +++++ +++++<]> ++++++ +++++.< ++++++
+[->- ----- <]>- ----- .- ----- .+ +++++ ++++++ .----- .<+ +++++ + +[->
+++++ +<]>+ ++++++ ++++++ +.,<+ ++++++ [- >+ +++++ +<]>+ + + +.<

```

https://blog.csdn.net/i_kei

[brainfuck加密](#)

[brainfuck解密网址](#)

Brainfuck

Encode
Decode

```

+++++ ++++++ [->+ ++++++ +++++<] >+.,+ ++++++ .<++++ [->-- <]>-
.,+++ +++++.<
+++++ [->+ +++++ +<]>+ +++++.< ++++++ +++++[- >----- < ]>-. .-.-.-.-.-.-.-.-.-.-.
+++++ +.,- -.-.<+ ++++++ +[->+ ++++++ +<]>+ +.,<+ ++++++ [->-----
<] >-----
----- .----- .<+ ++++++ [->+ +++++ +<] >+ ++++++ ++++++ +++++.< ++++++ + +
[-> -----
--<]> .,+.,- ----- .<+ ++++++ +++++[- >+ +++++ +++++<] >+ +++++. --.<+ ++++++ [->--
----- <
]>----- ----- .+ .<+ +++++ +++++[- >+ +++++ +++++<]> ++++++ ++++++ +++++.<+
+++++ + ++++++ [->--
----- < ]>----- ----- .- .+ +++++ .<+ +++++ +++++[- >+ +++++ +++++<]> ++++++ +++++.<
+++++
+[->- ----- <]>- ----- .- ----- .+ +++++ ++++++ .----- .<+ +++++ + +[->
+++++ +<]>+ ++++++ ++++++ +.,<+ ++++++ [- >+ +++++ +<]>+ + + +.<

```

```

flag{99^          16091a}

```

https://blog.csdn.net/i_kei

crypto9

暴力破解压缩包，口令为4132

口令已成功恢复! ✕

Advanced Archive Password Recovery 统计信息:

总计口令	4,131
总计时间	9ms
平均速度(口令/秒)	459,000
这个文件的口令	4132
十六进制口令	34 31 33 32

💾 保存...
✔ 确定

卡了半天后来偷看了羽大佬博客，才知道压缩包名就是加密方式。。。 (又一次get√新加密方式)

a8db1d82db78ed452ba0882fb9554fc

乍这么一瞅，MD5，结果解密失败，后来用word打开发现只有31个字符，通过群主大大的提示，在最后一位补足32位，获得flag

解密网站

<https://www.somd5.com/>

crypto0

凯撒

crypto12

Atbash Cipher (埃特巴什码) Encode Decode

uozt{Zgyzhv_xlww_uiln_xguhsld} flag{a .how}

https://blog.csdn.net/i_kei

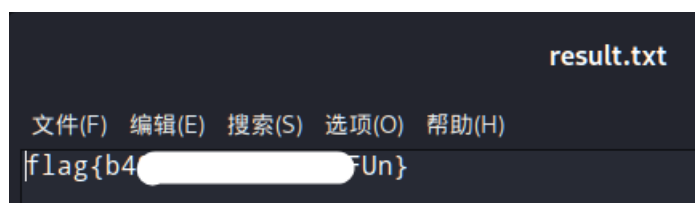
亏我凯撒和栅栏试了半天，结果是埃特巴什码，好家伙

crypto13

```
import base64

s=''
with open('base.txt', 'r', encoding='UTF-8') as f:
    s=''.join(f.readlines()).encode('utf-8')
src=s
while True:
    try:
        src=s
        s=base64.b16decode(s)
        str(s,'utf-8')
        continue
    except:
        pass
    try:
        src=s
        s=base64.b32decode(s)
        str(s,'utf-8')
        continue
    except:
        pass
    try:
        src=s
        s=base64.b64decode(s)
        str(s,'utf-8')
        continue
    except:
        pass
    break
with open('result.txt','w', encoding='utf-8') as file:
    file.write(str(src,'utf-8'))
print("Decryption complete!")
```

把脚本和base.txt放在同一目录下，运行后，result.txt中即为flag



crypto14

crypto14

5

感谢@星河皆灿烂提供的题目 00110011 00110011
00100000 00110100 00110101 00100000 00110101
00110000 00100000 00110010 01100110 00100000
00110011 00110011 00100000 00110101 00110110
00100000 00110100 01100101 00100000 00110100
00110110 00100000 00110100 00110110 00100000
00110110 01100100 00100000 00110100 01100101
00100000 00110100 00110101 00100000 00110100
00110001 00100000 00110110 01100101 00100000
00110110 01100011 00100000 00110100 00111000
00100000 00110100 00110100 00100000 00110011
00110101 00100000 00110110 00110100 00100000
00110100 00110011 00100000 00110100 01100100
00100000 00110110 01100100 00100000 00110101
00110110 00100000 00110100 00111000 00100000
00110100 00110100 00100000 00110011 00110101
00100000 00110110 00110001 00100000 00110110
00110100 00100000 00110011 00111001 00100000
00110111 00110101 00100000 00110100 00110111
00100000 00110000 01100001

https://blog.csdn.net/i_kei

把空格去掉，然后二进制转16进制，16进制转字符，得到字符串3EP/3VNFFmNEAnlHD5dCMmVHD5ad9uG
没思路，又一次偷看羽大佬博客，运行脚本得出正确的base64

```
#author 羽
s= '3EP/3VNFFmNEAnlHD5dCMmVHD5ad9uG'
t = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
l=""
for i in s:
    l += t[(t.index(i)-30)%64]

if len(l)%4!=0:
    l=l+"*"*(4-(len(l)%4))
print(l)
```

附上羽大佬博客链接

crypto0-13

<https://blog.csdn.net/miuzzx/article/details/104321319>

crypto14

<https://blog.csdn.net/miuzzx/article/details/104495832>

萌新_密码5

当铺密码，下载羽大佬的脚本运行得flag（没错又是羽大佬，tql）

```
s = '田由中人工大王夫井羊'
code=input("请输入当铺密码：")
code = code.split(" ")
w = ''
for i in code:
    k=""
    for j in i:
        k+=str(s.index(j))
    w+=chr(int(k))
print(w)
```

```
1 s = '田由中人工大王夫井羊'
2 code=input("请输入当铺密码：")
3 code = code.split(" ")
4 w = ''
5 for i in code:
6     k=""
7     for j in i:
8         k+=str(s.index(j))
9     w+=chr(int(k))
10 print(w)
11
```

Run: 当铺密码 () x

```
"D:\Keep Learning\PyCharm\venv\Scripts\python.exe" "D:/Keep Learning/PyCharm/当铺密码 ().py"
请输入当铺密码： 由田中 由田井 羊夫 由田人 由中人 羊羊 由由王 由田中 由由大 由田工 由由由 由由羊 由中大
flag{c[REDACTED]}

Process finished with exit code 0
```

https://blog.csdn.net/i_kei

内部赛 密码2

```
ctfctfshowctf
ctfshowctfctf
ctfshow
showshowctf
showshowshowshow showshowshowshow showshowctfctfctf showctfctfctf
showshowctfctfctf ctfctfctfshowshow showctfshowctf showctfctf
showctfctfctfctf showshowshowshow showctfctf showctfshowctf
showshowctfctfctf showshowctfctfctf ctfctfctfshowshow showctfshowctf
ctfctfctfctfctf ctfctfshowshowshow ctfctfctfctfshow showctfctf
ctfctfctfctfshow ctf showctfctfctf ctfshow
showshowshowshow showshowshowshow showshowctfctfctf showctfctf
```

将ctf替换成., show替换成-, 得到摩斯密码



用CTFcrack解出一段字符



FLAG后面是每4位的16进制

附上代码

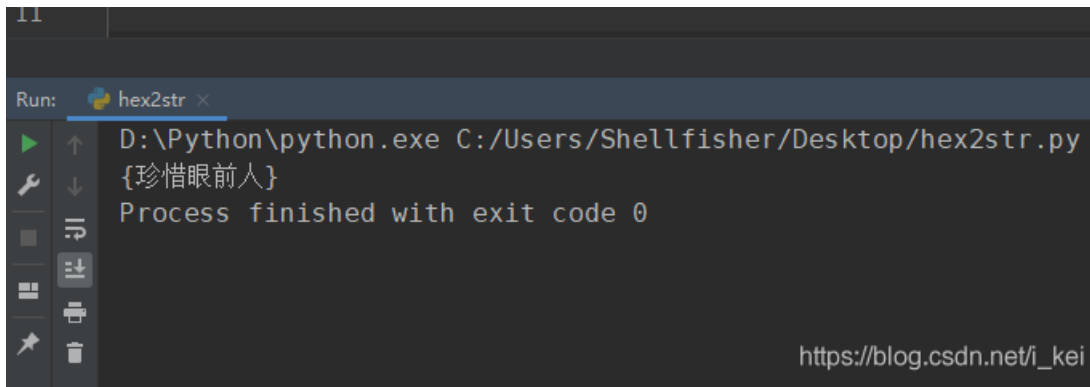
```
# -*- coding: utf-8 -*-
# @Author : i_kei
# @Time : 2021/1/22 11:43

import re

s = '007B73CD60DC773C524D4EBA007D'

for i in re.findall(r".{4}",s):
    print(chr(int(i,16)),end="")
```

```
1 # -*- coding: utf-8 -*-
2 # @Author : i_kei
3 # @Time : 2021/1/22 11:43
4
5 import re
6
7 s = '007B73CD60DC773C524D4EBA007D'
8
9 for i in re.findall(r".{4}",s):
10     print(chr(int(i,16)),end="")
```



小插曲：刚刚摩斯密码用网页工具和CaptfEncoder都只能解出一部分，卡了好长时间，无意中用了CTFcrack才都解出来，如果想用其他工具也解，可以把回车替换成空格



这样其他工具也可以完全解出来摩斯了，让这个换行符坑的好惨，主要是太菜了_(:_」∠)_

摩斯密码在线翻译

英文摩斯密码翻译工具 可以对英文和数字进行摩斯电码加密解密。如果用到汉字，请使用：[中文摩斯密码翻译](#)
公告：[可以在微信中使用本摩斯密码工具啦！查看>>](#)

输入摩尔斯电码，点击“解密”，即可将摩尔斯电码翻译成可识别的字符。

.....
.....
.....

解密

flag007b73cd60dc773c524d4eba007d

推荐：[中文摩斯密码翻译>>](#)

输入英文或数字，如：I love you，可将字符翻译成摩斯密码。

