CTF-Crypto-各种密码原理及解密方法

原创

weixin_45982862 于 2020-11-04 20:14:14 发布 3787 收藏 55

文章标签： 信息安全 加密解密 密码学

本文链接：https://blog.csdn.net/weixin_45982862/article/details/109457891

CTF-Crypto-各种密码原理及解密方法

一.常见密码格式（太懒了，待补充）

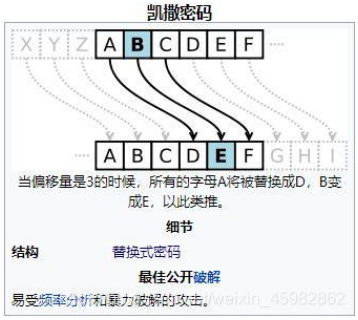
名称	密文	明文	特点
栅栏密码	fg2ivyo}{2s3_o@aw__rcl@	flag{w22_is_v3ry_cool}	1.长度一般不会太长 2.一般不会出现原来没有的字符(可能会出现用@打乱的现象)
base64	ZmxhZ3toZWxsb193b3JsZCF9IAo==	flag{hello_world!}	后面会有=

名称	密文	明文	特点
base16	666C61677B6D795F6E616D655F482121487D	flag{my_name_H!!H}	只由大写字母和数字组成
Unicode	\u0066\u006c\u0061\u0067\u007b\u0069\u005f\u0077\u0069\u006c\u006c\u005f\u006b\u0069\u006c\u006c\u005f\u0079\u006f\u0075\u0021\u007d	flag{i_will_kill_you!}	每一字符都用一个5位字符编码表示，并用\分割
urlencode	%68%61%63%6b%65%72%44%4a	hackerDJ	
词频分析	Eg qnlyjtcnzydl z umaujejmjetg qeydsn eu z bsjdtx tw sgqtxegc al kdeqd mgeju tw yrzegjsoj zns nsyrzqsx kejd qeydsnjsoj		
Ew ltm fgtk jds kzl tw sgqtxegc m kerr csj jds wrzc kdeqd eu qrzuueqzr-qeydsn_eu_gtj_usqmnejl_du		长度很长	

二.古典密码

凯撒密码

凯撒密码一般适用于26个英文字母。根据偏移量来进行加密。如图所示，当偏移量=3。即是A-D,B-E。



1.原理

密钥：K

加密解密过程：

$$e_K(x) = (x + K) \bmod 26$$
$$d_K(y) = (y - K) \bmod 26$$

2.在线加密解密网站：
https://www.qqxiuzi.cn/bianma/kaisamima.php
http://www.metools.info/code/c70.html
http://www.atoolbox.net/Tool.php?Id=778

仿射密码

1.原理

密钥：(a，b)，其中a与26互质。

加密解密过程：

$$e_K(x) = (ax + b) \bmod 26$$
$$d_K(y) = a^{11} (y - b) \bmod 26$$

2.在26上所有与26互质元素的乘法逆元

1^{-1}	3^{-1}	5^{-1}	7^{-1}	9^{-1}	11^{-1}	15^{-1}	17^{-1}	19^{-1}	21^{-1}	23^{-1}	25^{-1}
1	9	21	15	3	19	7	23	11	5	17	25

3.在线加密解密网站：
http://www.atoolbox.net/Tool.php?Id=911

4.解密脚本：

```
import primefac
def affine_decode(c,a,b,origin="abcdefghijklmnopqrstuvwxyz"):
 r=""
 n=len(origin)
 ai=primefac.modinv(a,n)%n
 for i in c:
 if origin.find(i)!=1:
 r+=origin[(ai*(origin.index(i)-b))%n]
 else:
 r+=i
 return r
print affine_decode("ihhwvcswfrcp",5,8)


def affine_guessab(m1,c1,m2,c2,origin="abcdefghijklmnopqrstuvwxyz"):
 x1=origin.index(m1)
 x2=origin.index(m2)
 y1=origin.index(c1)
 y2=origin.index(c2)
 n=len(origin)
 dxi=primefac.modinv(x1-x2,n)%n
 a=dxi*(y1-y2) % n
 b=(y1-a*x1)%n
 return a,b
print affine_guessab("a","i","f","h")
```

埃特巴什码

1.加密解密原理：使用字母表倒数第n个字母代替第n个字母

明文：A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
密文：Z Y X W V U T S R Q P O N M L K J I H G F E D C B A

例如：

明文： the quick brown fox jumps over the lazy dog
密文： gsv jfrxp yildm ulc qfnkh levi gsv ozab wlt

培根密码

1.加密解密原理：使用两种字符，每一段长度为5.

A/a	aaaaa	H/h	aabbb	O/o	abbba	V/v	babab
B/b	aaaab	I/i	abaaa	P/p	abbbb	W/w	babba
C/c	aaaba	J/j	abaab	Q/q	baaaa	X/x	babbb
D/d	aaabb	K/k	ababa	R/r	baaab	Y/y	bbaaa
E/e	aabaa	L/l	ababb	S/s	baaba	Z/z	bbaab
F/f	aabab	M/m	abbaa	T/t	baabb		
G/g	aabba	N/n	abbab	U/u	babaa		

2.在线加密解密网址：
https://tool.bugku.com/peigen/

棋盘密码

1.加密原理：

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

另一常用表：

	A	D	F	G	X
A	b	t	a	l	p
D	d	h	o	z	k
F	q	f	v	s	n
G	g	j	c	u	x
X	m	r	e	w	y

希尔密码

1.加密解密原理：

使用每个字母在字母表中的顺序作为其对应数字。再将铭文转换为n维向量，和一个n阶方阵相乘后模26.最后将新的矩阵写成对应字母。

例子：
明文：ACT $\begin{bmatrix}0\\2\\19\end{bmatrix}$ 密钥：$\begin{bmatrix}6&24&1\\13&16&10\\20&17&15\end{bmatrix}$

加密过程：$\begin{bmatrix}6&24&1\\13&16&10\\20&17&15\end{bmatrix}\begin{bmatrix}0\\2\\19\end{bmatrix}\equiv\begin{bmatrix}67\\222\\319\end{bmatrix}\equiv\begin{bmatrix}15\\14\\7\end{bmatrix}\mod 26$

得到密文： POH

2.在线加密解密：
http://www.atoolbox.net/Tool.php?Id=914

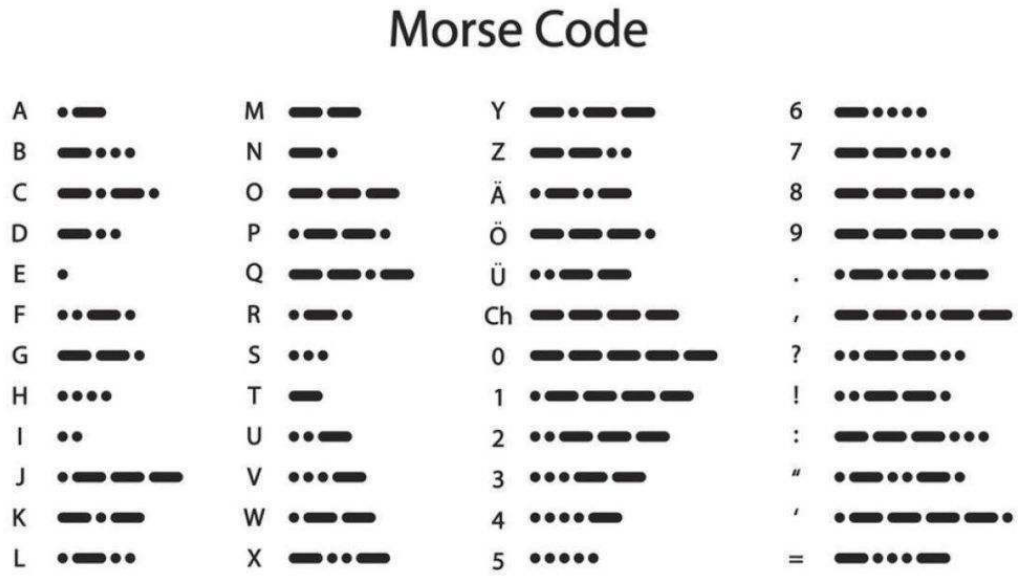
维吉尼亚密码

1.加密原理：根据密钥来决定用哪一行密表来进行替换。

2.在线加密解密网址：
https://www.qqxiuzi.cn/bianma/weijiniyamima.php

摩尔斯密码

1.加密原理：



2.在线加密解密网址：
http://www.zhongguosou.com/zonghe/moErSiCodeConverter.aspx?d=123

栅栏密码(普通型)

1.将明文分为N组，然后把每一组第一个字连起来。

明文：THERE IS A CIPHER
去掉空格后变为 THEREISACIPHER
分成两栏，两个一组得到 TH ER EI SA CI PH ER
先取出第一个字母，再取出第二个字母

- TEESCPE
- HRIAIHR

连在一起就是 TEESCPEHRIAIHR

2.在线加密解密网址：
https://www.qqxiuzi.cn/bianma/zhalanmima.php

栅栏密码(W型)

1.加密解密原理：分组时呈W型排列。

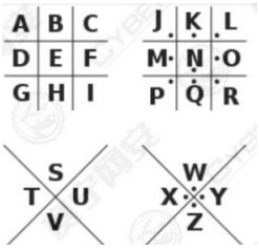
```
cf{pacenelerr_eapbc}ioghyeoige_gorc
c-------e--------p--------y--------o----
-f-----n-l-----a-b-----h-e-----g-r---
--{---e---e---e---c---g---o---_---c--
---p-c-----r-_-----}-o-----i-e-------
----a-------r-------i-------g--------
```

2.在线加密解密网址：

http://www.atoolbox.net/Tool.php?Id=777.com

猪圈密码

1.加密原理：



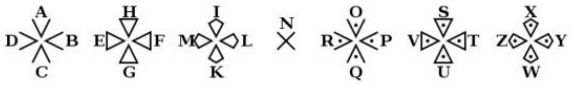
2.在线加密解密网址：

http://www.metools.info/code/c90.html

圣堂武士密码

猪圈密码的一种变形

1.加密解密原理：



Ook!密码

1.加密原理：

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

2.在线加密解密网址：

https://www.splitbrain.org/services/ook

BrainFuck密码

1.加密解密原理：

```
+++++ ++++[ ->+++ +++++ +<]>+ +++++ +++++ +++++ ++.<+ +++[-
>++++ <]>+.
<+++[ ->--- <]>-- ---.< +++++ +++[- >---- ----< ]>--- ---.<
+++++ +++[-
>++++ ++++< ]>+++ .++++ ++.++ +++++ .---- ----. ---.< +++[- >+++
< ]>+++
+.<++ +++++ ++[-> ----- ----< ]>-.< +++++ +++[- >++++ ++++<
]>+++ +++++
+.<++ +[->+ ++<]> +.<++ +++++ ++[-> ----- ----< ]>--. <++++ ++++
[ ->+++
```


2.在线加密解密网址：

https://www.splitbrain.org/services/ook

JS加密

1.加密解密方法：

```
ﾟωﾟﾉ= /｀ｍ´）ﾉ ~┻━┻   //*´∇｀*/ ['_']; o=(ﾟｰﾟ)  =_=3; c=(ﾟΘﾟ) =(ﾟｰﾟ)-(ﾟｰﾟ); (ﾟДﾟ) =(ﾟΘﾟ)= (o^_^o)/
(o^_^o);(ﾟДﾟ)={ﾟΘﾟ: '_' ,ﾟωﾟﾉ : ((ﾟωﾟﾉ==3) +'_') [ﾟΘﾟ] ,ｰ~ﾟ/ :(ﾟωﾟﾉ+ '_')[o^_^o -(ﾟΘﾟ)] ,ﾟДﾟﾉ:((ﾟｰﾟ==3)
+'_')[ﾟｰﾟ] }; (ﾟДﾟ) [ﾟΘﾟ] =((ﾟωﾟﾉ==3) +'_') [c^_^o];(ﾟДﾟ) ['c'] = ((ﾟДﾟ)+'_') [ (ﾟｰﾟ)+(ﾟｰﾟ)-(ﾟΘﾟ) ];(ﾟДﾟ)
['o'] = ((ﾟДﾟ)+'_') [ﾟΘﾟ];(ﾟoﾟ)=(ﾟДﾟ) ['c']+(ﾟДﾟ) ['o']+(ﾟωﾟﾉ +'_')[ﾟΘﾟ]+ ((ﾟωﾟﾉ==3) +'_') [ﾟｰﾟ] + ((ﾟДﾟ)
+'_') [(ﾟｰﾟ)+(ﾟｰﾟ)]+ ((ﾟｰﾟ==3) +'_') [ﾟΘﾟ]+((ﾟｰﾟ==3) +'_') [(ﾟｰﾟ) - (ﾟΘﾟ)]+(ﾟДﾟ) ['c']+((ﾟДﾟ)+'_') [(ﾟｰﾟ)+(ﾟ
ｰﾟ)]+ (ﾟДﾟ) ['o']+((ﾟｰﾟ==3) +'_') [ﾟΘﾟ];(ﾟДﾟ) ['_'] =(o^_^o) [ﾟoﾟ] [ﾟoﾟ];(ﾟεﾟ)=((ﾟｰﾟ==3) +'_') [ﾟΘﾟ]+ (ﾟДﾟ)
.ﾟДﾟﾉ+((ﾟДﾟ)+'_') [(ﾟｰﾟ) + (ﾟｰﾟ)]+((ﾟｰﾟ==3) +'_') [o^_^o -ﾟΘﾟ]+((ﾟｰﾟ==3) +'_') [ﾟΘﾟ]+ (ﾟωﾟﾉ +'_') [ﾟΘﾟ]; (ﾟ
ｰﾟ)+=(ﾟΘﾟ); (ﾟДﾟ)[ﾟεﾟ]='¥¥'; (ﾟДﾟ).ﾟΘﾟﾉ=(ﾟДﾟ+ ﾟｰﾟ)[o^_^o -(ﾟΘﾟ)];(oﾟｰﾟo)=(ﾟωﾟﾉ +'_')[c^_^o];(ﾟДﾟ) [ﾟ
oﾟ]='¥"';(ﾟДﾟ) ['_'] ( (ﾟДﾟ) ['_'] (ﾟεﾟ+(ﾟДﾟ)[ﾟoﾟ]+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ (ﾟΘﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+
((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((o^_^o) +(o^_^o))+
((o^_^o) - (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((o^_^o) +(o^_^o))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+((ﾟｰﾟ) + (ﾟΘﾟ))+ (c^_^o)+ (ﾟДﾟ)
[ﾟεﾟ]+(ﾟｰﾟ)+ ((o^_^o) - (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟΘﾟ)+ (c^_^o)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ ((ﾟｰﾟ) + (ﾟ
Θﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟ
Θﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ ((ﾟｰﾟ) + (o^_^o))+ (ﾟДﾟ)[ﾟεﾟ]+((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟｰﾟ)+ (c^_^o)+ (ﾟ
Дﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟΘﾟ)+ ((o^_^o) - (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ (ﾟΘﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+((o^_^o) +
(o^ ^o))+ ((o^ ^o) +(o^ ^o))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ (ﾟΘﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((o^ ^o) - (ﾟΘﾟ))+
```

2.在线加密解密网址：

https://utf-8.jp/public/aaencode.html
https://www.sojson.com/jsjiemi.html

JSFuck加密

1.加密解密原理：

```
[][(![]+[])[+[]]+(![]+[])[!+[]+!+[]]+(![]+[])[+!+[]]+(!![]+[])[+[]]][([][(![]+[])
[+[]]+(![]+[])[!+[]+!+[]]+(![]+[])[+!+[]]+(!![]+[])[+[]]]+[])[!+[]+!+[]+!+[]]+(!!
[]+[][(![]+[])[+[]]+(![]+[])[!+[]+!+[]]+(![]+[])[+!+[]]+(!![]+[])[+[]]])[+!+[]+[+
[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+
([][[]]+[])[+[]]+([][(![]+[])[+[]]+(![]+[])[!+[]+!+[]]+(![]+[])[+!+[]]+(!![]+[])[+
[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+(![]+[])[!+[]+!+
[]]+(![]+[])[+!+[]]+(!![]+[])[+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]]((!![]+[])[+!+
[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+([][[]]+[])[+[]]+(!![]+[])[+!+[]]+([]
[[]]+[])[+!+[]]+(+[![]]+[][(![]+[])[+[]]+(![]+[])[!+[]+!+[]]+(![]+[])[+!+[]]+(!!
[]+[])[+[]]])[+!+[]+[+!+[]]]+(!![]+[])[!+[]+!+[]+!+[]]+(+(!+[]+!+[]+!+[]+[+!+[]]))
```

2.在线加密解密网址：

http://www.jsfuck.com/
https://www.sojson.com/jsjiemi.html

盲文

1.加密解密原理：

[illegible]==

2.在线加密解密网址：
https://www.qqxiuzi.cn/bianma/wenbenjiami.php?s=mangwen

四方密码

1.加密解密原理：

密钥：K1，K2

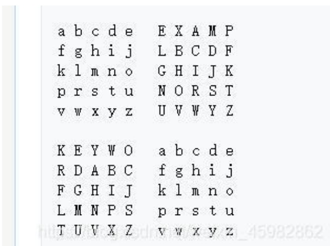
加密解密过程：

将密钥去掉重复字母，写进一个5*5的矩阵中，剩余字母按字母表中的顺序填充(将Q去除，或将I和J视作同一字)，与密钥重复的字母就不要写进去了。

将两个矩阵放在右上和左下，右下和左上的矩阵按字母表的顺序组成。这样就组成了一个22*的*55的密钥存阵。

加密时两个字母一组。第一个字母加密后就是和一个字母同横的，和第二个字母同直的密钥存阵中的字母；第二个字母加密后就是和第一个字母同直，第二个字母同横的字母。

例如：
密钥为example和keyword
明文为he
加密矩阵为



故密文为FY。

2.在线加密解密网址：

http://ctf.ssleye.com/four.html

标准银河字母

1.加密解密原理：

当铺密码

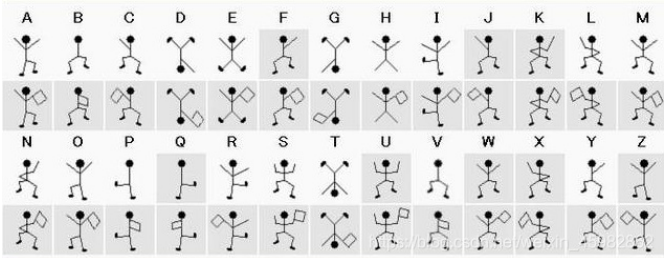
将中文和数字进行转化的密码

1.加密解密原理：

当前汉字有多少笔画**出头**，就是转化成数字几
例如：口 0 田 0 由 1 中 2 人 3 工 4 大 5 王 6 夫 7 井 8 羊 9

跳舞的小人密码

1.加密解密原理：



普莱费尔密码

1.加密解密原理：

密钥：K

加密解密过程：

选取一个英文字作密钥。除去重复出现的字母。将密钥的字母逐个逐个加入5×5的矩阵内，剩下的空间将未加入的英文字母依a-z的顺序加入。（将Q去除，或将I和J视作同一字。）

将要加密的讯息分成两个一组。若组内的字母相同，将X（或Q）插入两字母之间，重新分组（例如 HELLO 将分成 HE LX LO）。若剩下一个字，也加入X字。

在每组中，找出两个字母在矩阵中的地方。

若两个字母不在同一直行或同一横列，在矩阵中找出另外两个字母，使这四个字母成为一个长方形的四个角。

若两个字母在同一横列，取这两个字母右方的字母（若字母在最右方则取最左方的字母）。

若两个字母在同一直行，取这两个字母下方的字母（若字母在最下方则取最上方的字母）。

2.在线加密解密网址：
http://www.atoolbox.net/Tool.php?Id=912
http://rumkin.com/tools/cipher/playfair.php

Keyboard密码

Keyboard密码在ctf中应该是分多种类型的。这里提两种。即9键表和26键。

1.加密解密原理：

9键表就是通过九键上多次字母来进行字母提取，26键包含通过明文多个字符对应一个密文。

例如：ooo在键盘上对应9，3个o即代表第九个格子第三个字母即y

云影密码(01248密码)

1.加密解密原理：

将一个数字各位数字加起来之和得到的数字对应的字母就是密文

例如：123=6，即f。

2.解密脚本：

```
#!/usr/bin/python
# -*- coding=utf8 -*-
"""
# @Author : pig
# @CreatedTime:2019-11-2423:54:02
# @Description :
"""

def de_code(c):
 dic = [chr(i) for i in range(ord("A"), ord("Z") + 1)]
 flag = []
 c2 = [i for i in c.split("0")]
 for i in c2:
 c3 = 0
 for j in i:
 c3 += int(j)
 flag.append(dic[c3 - 1])
 return flag

def encode(plaintext):
 dic = [chr(i) for i in range(ord("A"), ord("Z") + 1)]
 m = [i for i in plaintext]
 tmp = [];flag = []
 for i in range(len(m)):
 for j in range(len(dic)):
 if m[i] == dic[j]:
 tmp.append(j + 1)
 for i in tmp:
 res = ""
 if i >= 8:
 res += int(i/8)*"8"
 if i%8 >=4:
 res += int(i%8/4)*"4"
 if i%4 >=2:
 res += int(i%4/2)*"2"
 if i%2 >= 1:
 res += int(i%2/1)*"1"
 flag.append(res + "0")
 print ("".join(flag)[:-1])

c = input("输入要解密的数字串:")
print (de_code(c))
m_code = input("请输入要加密的数字串:")
encode(m_code)
```

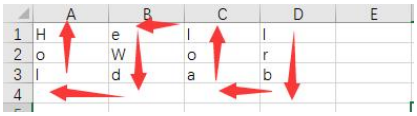
曲路密码

1.加密解密原理：

按照事先约定的原则把明文填入表中，再按照一定的顺序进行遍历

例如：

明文为HelloWorldab



密文就是lrbaoleWdloH

三.现代密码（太懒了，待补充）

参考网址：https://www.cnblogs.com/hetianlab/p/13628249.html
https://blog.csdn.net/vhkjhwbs/article/details/99692399