ctf古典密码从0到1

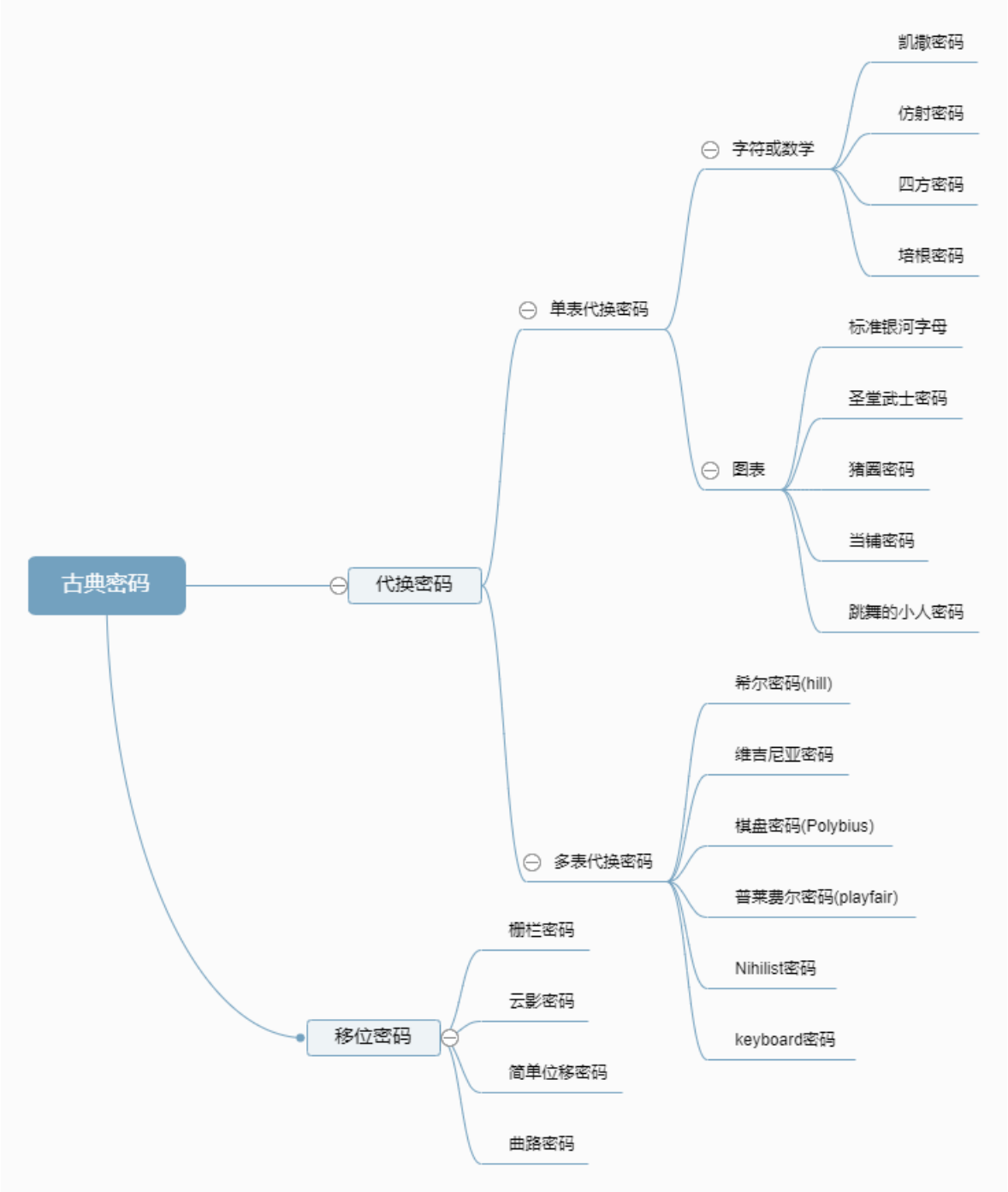
原创

合天网安实验室 于 2020-09-07 13:00:00 发布 1773 收藏 13
分类专栏： CTF 文章标签： 密码学 字符串 twitter bmp sharepoint

本文共计6357个词

阅读预计花费8分钟

```
1.古典密码和现代密码的区别：
2.代换密码
a)单表代换密码
i.字符或数学型
1.凯撒密码
2.仿射密码
3.四方密码
4.培根密码
ii.图表
1.标准银河字母
2.圣堂武士密码
3.猪圈密码
4.当铺密码
5.跳舞的小人密码
b)多表代换密码
i.希尔密码
ii.维吉尼亚密码
iii.棋盘密码（Polybius）
iv.普莱费尔密码（playfair）
v.Nihilist密码
vi.Keyboard密码
3.移位密码
a)栅栏密码
b)云影密码
c)简单位移密码
d)曲路密码
4.CTF crypto线下工具推荐
```



古典密码和现代密码的区别：

古典密码是密码学中的其中一个类型，其大部分加密方式都是利用替换式密码或移项式密码，有时则是两者的混合。其于历史中经常使用，但现代已经很少使用，大部分的已经不再使用了。一般而言，经典密码是基于一个拼音字母（像是 A-Z）、动手操作或是简单的设备。它们可能是一种简单的密码法，以致于不可信赖的地步，特别是有新技术被发展出来后。

现代的方法是用电脑或是其它数字科技，基于比特和字节上操作。许多经典密码被受尊重的人使用，像是尤利乌斯·凯撒和拿破仑，他们创造了一些常被人们使用的密码。许多密码起源于军事上，相同立场的人常使用来寄送秘密消息。经典的方法常攻击密码文，有时候甚至不知其密码系统，也可以使用工具，像是频率分析法。有些经典密码是使用先进的机器或是机电密码机器，像是恩尼格玛密码机。 ---维基

其中，古典密码学，作为一种实用性艺术存在，其编码和破译通常依赖于设计者和敌手的创造力与技巧，并没有对密码学原件进行清晰的定义。古典密码学主要包含以下几个方面：

单表替换加密（Monoalphabetic Cipher）

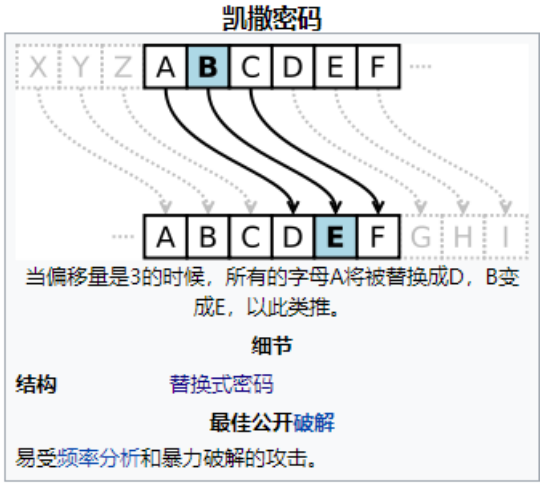
多表替换加密（Polyalphabetic Cipher）

奇奇怪怪的加密方式 --ctf wiki

凯撒密码：

凯撒曾经使用这种密码与其将军们来联系，所以用凯撒来命名这种密码。

根据图片来了解加密原理。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。



把字母转成数学，数学公式如下。

凯撒密码的加密、解密方法还能够通过同余的数学方法进行计算。首先将字母用数字代替，A=0，B=1，...，Z=25。此时偏移量为n的加密方法即为：

$$E_n(x) = (x + n) \mod 26$$

解密就是：

$$D_n(x) = (x - n) \mod 26$$

在线加解密网站：
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：

数学加密公式：

$$e(x) = ax + b \pmod{m},$$

仿射密码中解密需要用到求逆元

直接给出python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")
```

```
仿射密码在线加解密网站：
http://www.atoolbox.net/Tool.php?Id=911
```

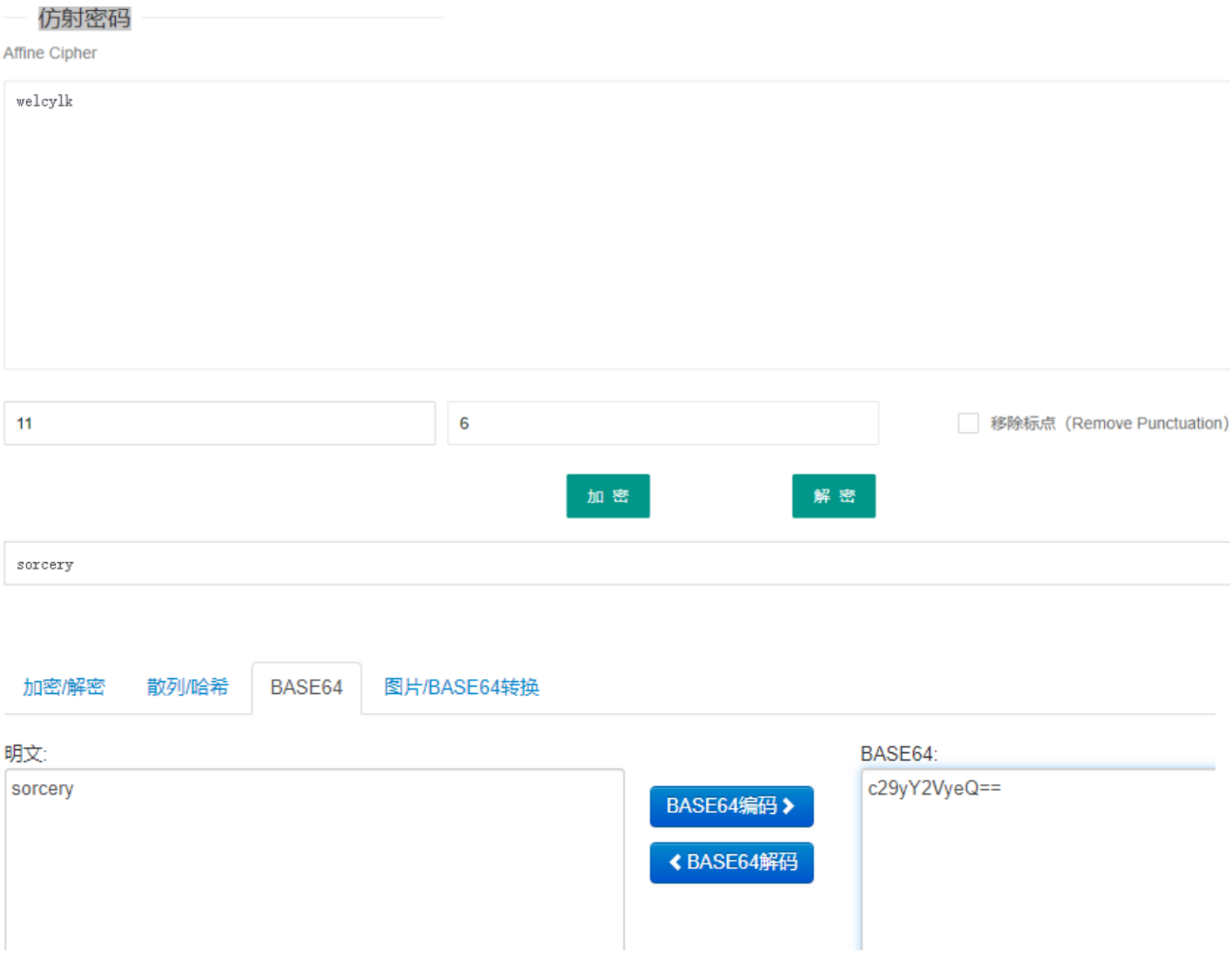
仿射密码真题-one：

Buuctf- Crypto-[GKCTF2020]小学生的密码学

e(x)=11x+6(mod26)

密文：welcylk

（flag为base64形式）



四方密码：

四方密码是一种对称式加密法，由法国人Felix Delastelle（1840年–1902年）发明。

这种方法将字母两个一组，然后采用多字母替换密码。

四方密码用4个5×5的矩阵来加密。每个矩阵都有25个字母（通常会取消Q或将I,J视作同一样，或改进为6×6的矩阵，加入10个数字）。

选两个密钥，example和keyword。去掉重复的字母。就是example变成exampl。余下的字母顺序存入矩阵即可

加密矩阵放右上和左下。

```
a b c d e   E X A M P
f g h i j   L B C D F
k l m n o   G H I J K
p r s t u   N O R S T
v w x y z   U V W Y Z

K E Y W O   a b c d e
R D A B C   f g h i j
F G H I J   k l m n o
L M N P S   p r s t u
T U V X Z   v w x y z
```

加密步骤。把字符串按两个字母一组分开

Helloworld

He ll ow or ld

找第一组第一个字母在左上角矩阵的位置：

```
a b c d e   E X A M P
f g h i j   L B C D F
k l m n o   G H I J K
p r s t u   N O R S T
v w x y z   U V W Y Z
```

```
K E Y W O   a b c d e
R D A B C   f g h i j
F G H I J   k l m n o
L M N P S   p r s t u
T U V X Z   v w x y z
```

找第一组第二个字母在右下角矩阵的位置：

```
a b c d e   E X A M P
f g h i j   L B C D F
k l m n o   G H I J K
p r s t u   N O R S T
v w x y z   U V W Y Z
```

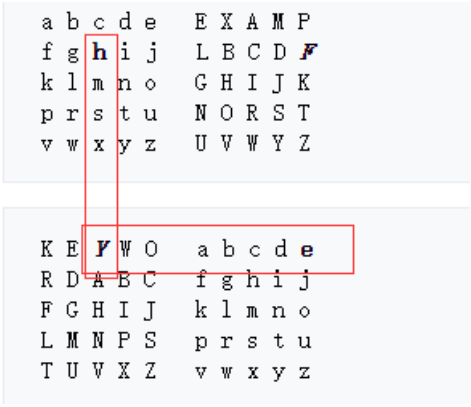
```
K E Y W O   a b c d e
R D A B C   f g h i j
F G H I J   k l m n o
L M N P S   p r s t u
T U V X Z   v w x y z
```

先找和一个字母同横的，和第二个字母同直的

```
a b c d e   E X A M P
f g h i j   L B C D F
k l m n o   G H I J K
p r s t u   N O R S T
v w x y z   U V W Y Z
```

```
K E Y W O   a b c d e
R D A B C   f g h i j
F G H I J   k l m n o
L M N P S   p r s t u
T U V X Z   v w x y z
```

第一个字母同直，第二个字母同横的



得到he加密后为FY

如此可得接下来，最后就是

he lp me ob iw an ke no bi

FY GM KY HO BX MF KK KI MD

四方密码真题-one：

Buuctf-crypo-四面八方

四方密码：

wiki上了解四方密码如何加解密的一个过程

https://zh.wikipedia.org/wiki/%E5%9B%9B%E6%96%B9%E5%AF%86%E7%A2%BC

密钥存阵

通常在题目中会给定2个密钥，我们要去掉Q或者把I和J当成一个。按照26个英文字母。秘钥中出现的不填。补充成5*5的矩阵

这题直接填充即可

securityabdfghjklmnopvwxz

securityadbfghjklmnopvwxz

abcdefghijklmnopqrstuvwxyz

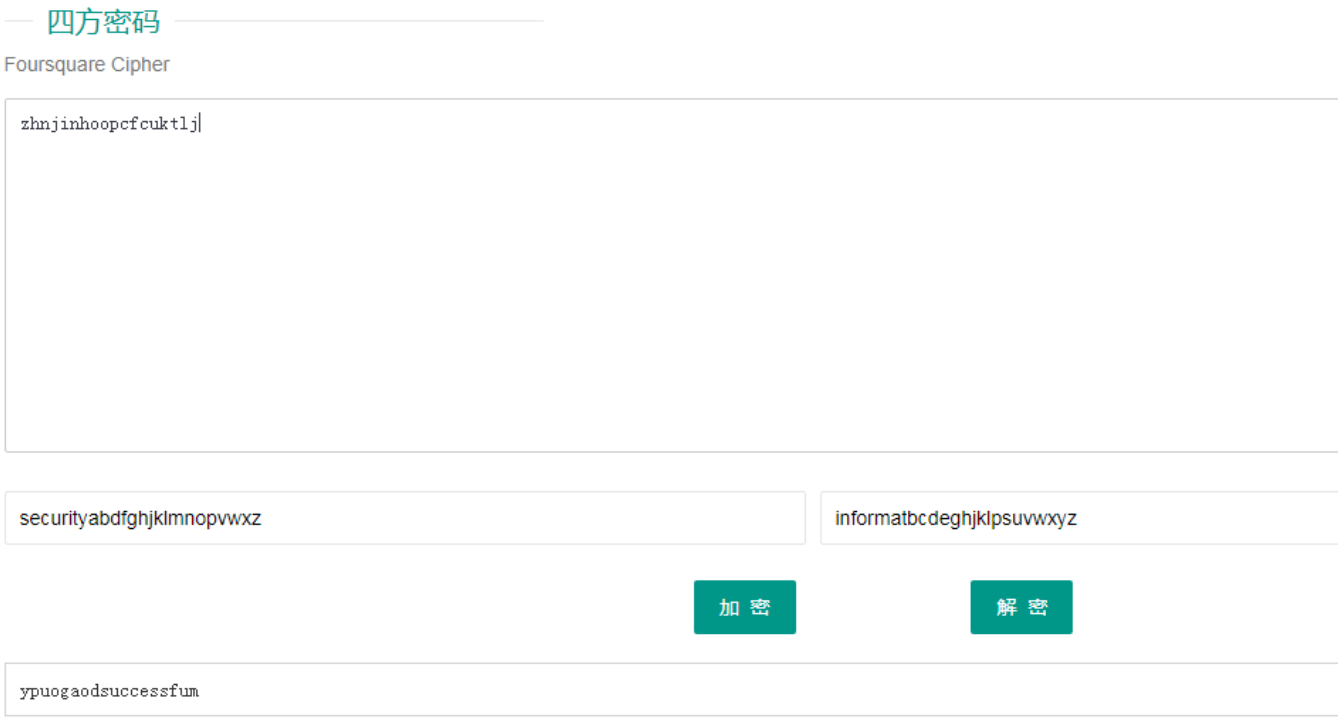
informatn

informatbcdeghjklpsuvwxyz

abcdefghijklmnopqrstuvwxyz

```
在线解密工具：
http://ctf.ssleye.com/four.html
```

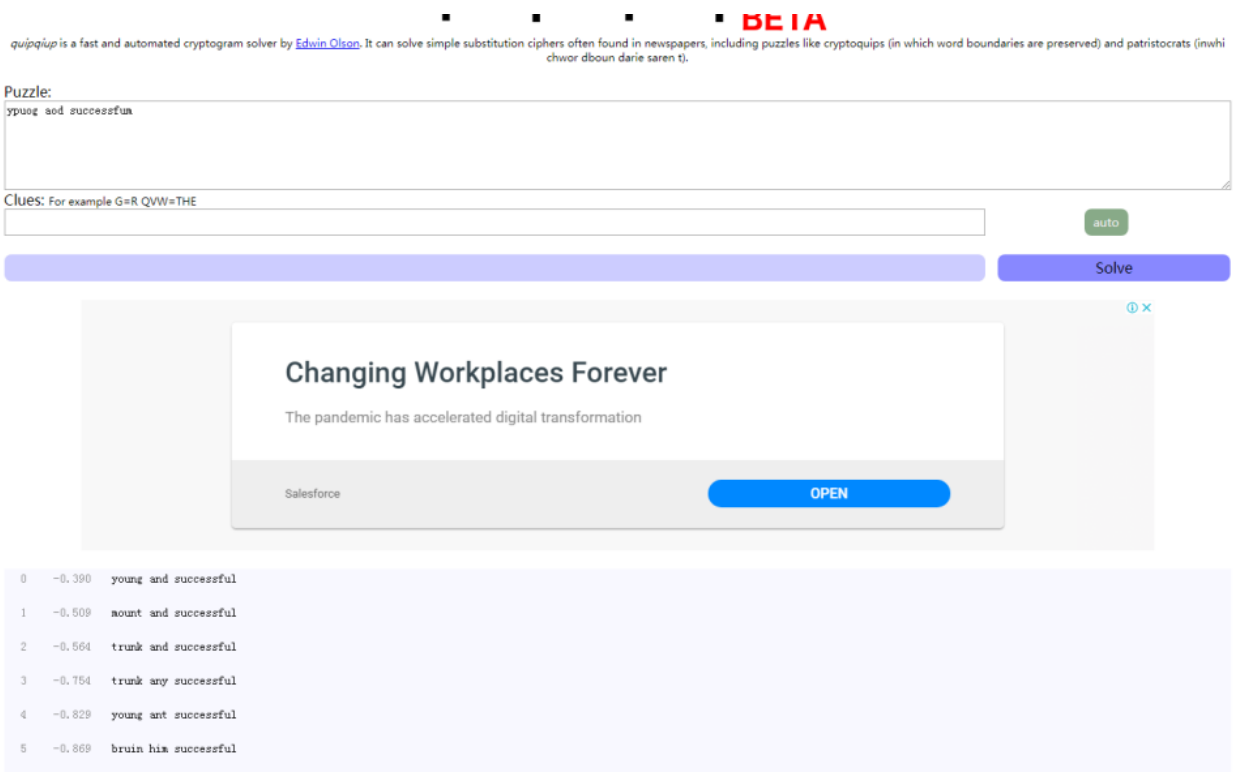
根据题目说的解出来的语句是个通顺的句子，那肯定排序就有点问题



接下来可以拿出词频分析。

这边分割可以多试试。可以看出来个success，其他位置试

https://quipqiup.com/



四方密码在线加解密网站：
http://ctf.ssleye.com/four.html

培根密码：

培根密码直接根据表中的字母进行转换。

密文一般只含有a和b字母

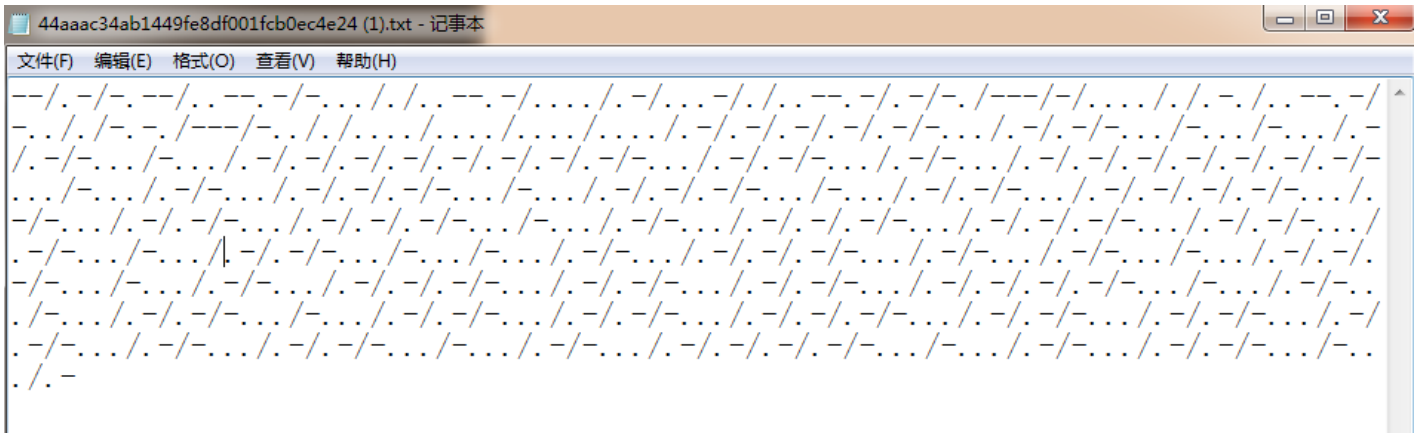
加密时，明文中的每个字母都会转换成一组五个英文字母。其转换依靠下表：

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		

培根密码在线解密：
https://tool.bugku.com/peigen/

培根密码真题-one：

攻防世界crypto新手-不仅仅是morse



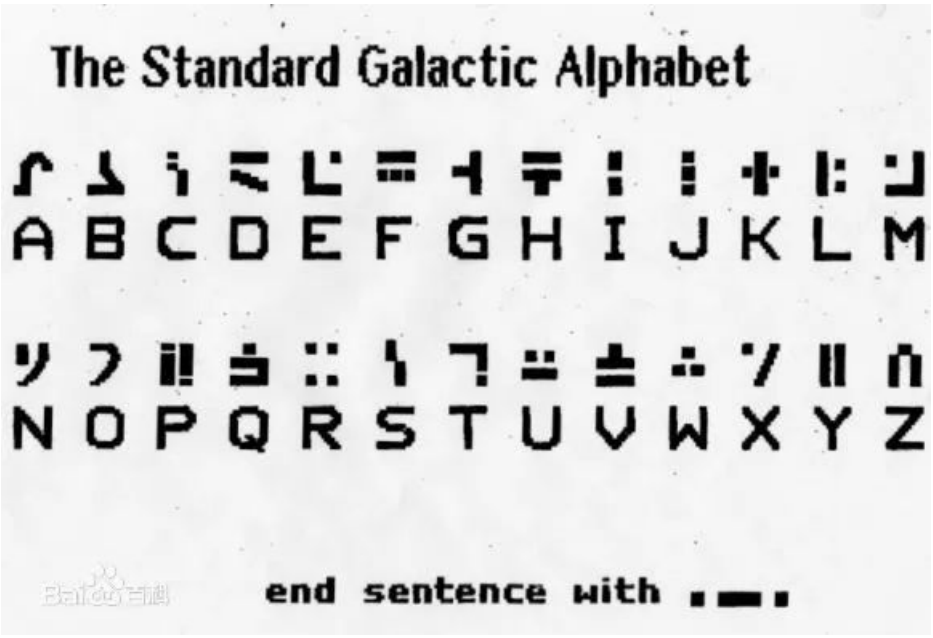
把/转换成空格。直接拿出morse解密

在看后面一段像培根密码，根据题目提示是食物加密。

标准银河字母：

标准银河字母（Standard Galactic Alphabet）出自游戏《指挥官基恩》系列。是系列中使用的书写系统。这是一个简单的替代暗号，用不同的符号取代拉丁字母。SGA可以在不同的语言中使用，比如在游戏《Minecraft》，《指挥官基恩》中。

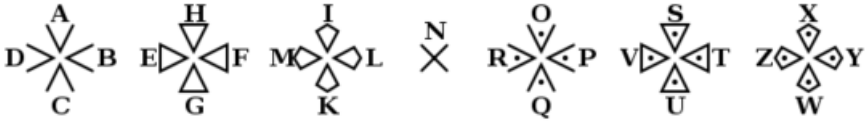
如果遇到这类题。直接根据题目来进行图翻->字母



圣堂武士密码：

圣堂武士密码(Templar Cipher)是共济会的“猪圈密码”的一个变种,一直被共济会圣殿骑士用。

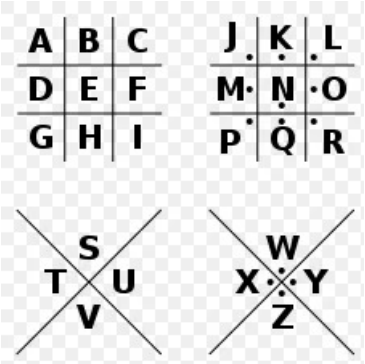
直接根据图片上的直接翻译出字母即可



猪圈密码：

猪圈密码（亦称朱高密码、共济会暗号、共济会密码或共济会员密码），是一种以格子为基础的简单替代式密码。即使使用符号，也不会影响密码分析，亦可用在其它替代式的方法。

直接图片替换字母即可




```
猪圈密码在线解密网站：
http://www.metools.info/code/c90.html
```

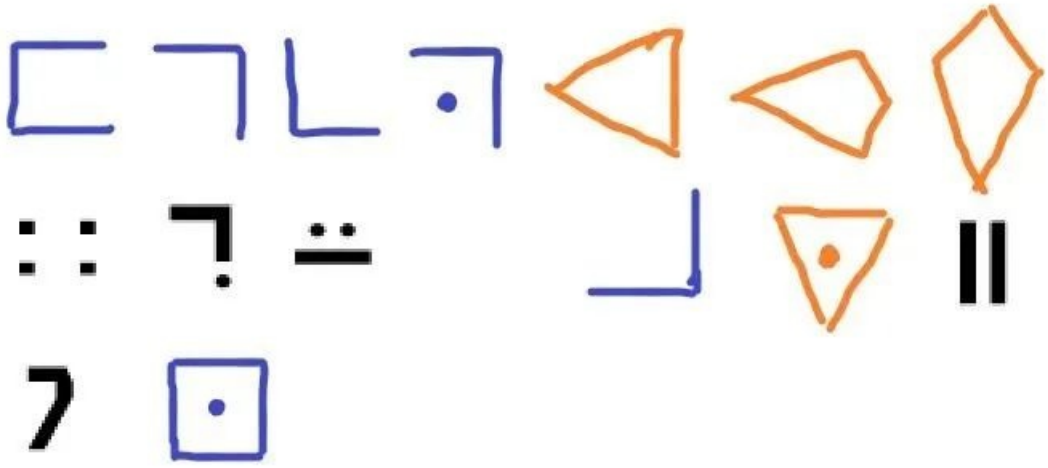
猪圈密码真题：

Buuctf-crypto-萌萌哒的八戒

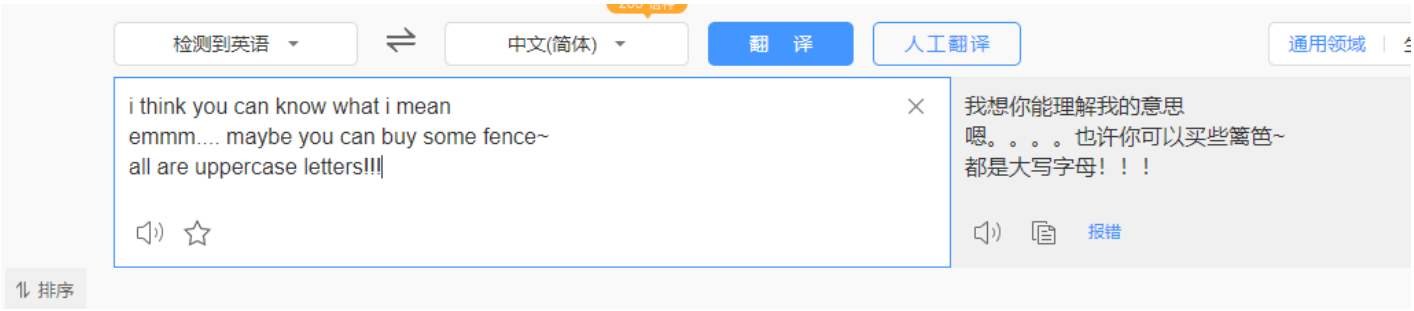
直接解密

猪圈密码-圣堂武士密码-标准银河字母-栅栏密码真题：

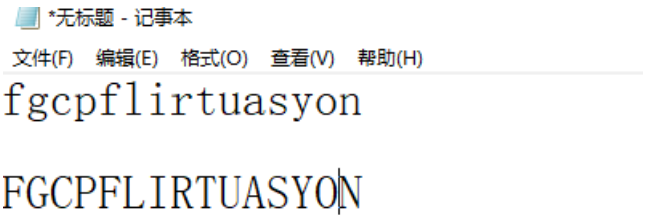
Buuctf-Crypto- [MRCTF2020]古典密码知多少

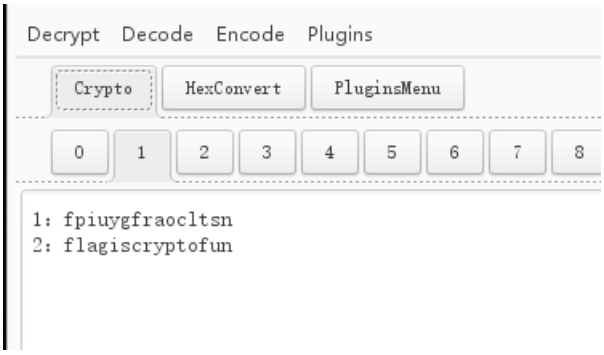


i think you can know what i mean.
emmm.... maybe you can buy some fence~
all are uppercase letters！！！



图上的蓝色就是猪圈密码，橙色的是圣堂武士密码，黑色的是银河字母。





当铺密码：

当铺密码就是一种将中文和数字进行转化的密码，算法相当简单: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

具体映射可查看：
https://www.cnblogs.com/cc11001100/p/9357263.html

当铺密码真题：

Buuctf-crypto-GKCTF2020汉字的秘密

王壮 夫工 王中 王夫 由由井 井人 夫中 夫夫 井王 土土 夫由
土夫 井中 士夫 王工 王人 土由 由口夫

王壮夫工中由井人土士口
6 9 7 4 2 1 8 3 5 5 0

直接解码发现不对。

翻看ascii码。改进一下脚本：

自己猜一下flag开头为flag。可以看到ascii嘛每一位都是递增的。

差为1,2,3,4

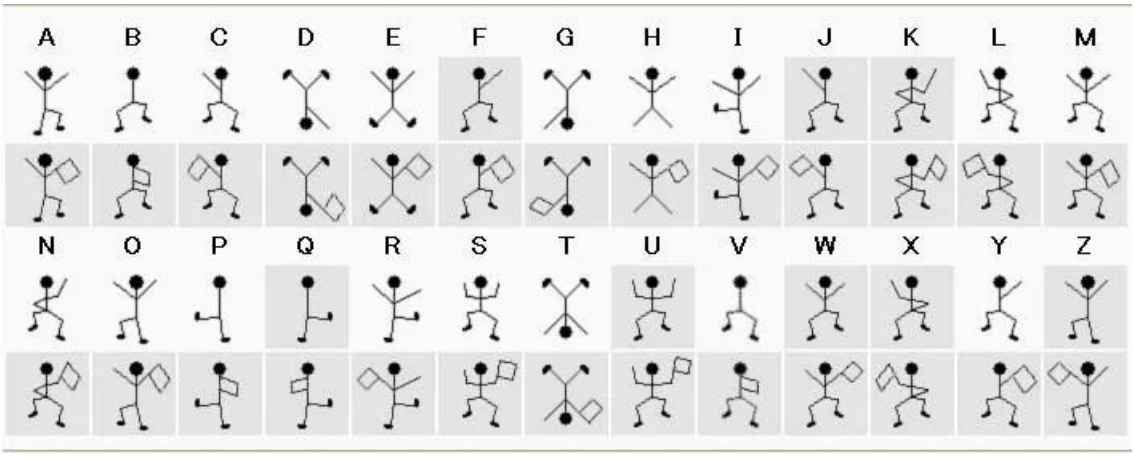
```python
s = [69, 74, 62, 67, 118, 83, 72, 77, 86, 55, 71, 57, 82, 57, 64, 63, 51, 107]
ans = ''
for i in range(len(s)):
    ans += chr(s[i]+1+i)
    print(i, chr(s[i]+1+i))

print(ans)
print(ans.lower())

```

```
问题  输出  调试控制台  终端                                  1: Python Debug Consc

13 G
14 O
15 O
16 D
17 }
FLAG{YOU_ARE_GOOD}
flag{you_are_good}

C:\Users\Administrator\Desktop>
```

跳舞的小人密码：

跳舞的人，讲的是一个黑帮发明的一种密码，其密码就是用一个一个的跳舞的小人组成的，一个小人是一个字母。有人用这种密码进行通信，来威胁某人，福尔摩斯后来破解了这个密码，抓住了坏人。

这题直接根据表来进行转换即可。加解密同



这题感觉是做过的。但没翻到例题。就不放了。

希尔密码（hill）：

希尔密码（Hill Cipher）是运用基本矩阵论原理的替换密码，由Lester S. Hill在1929年发明。每个字母当作26进制数字：A=0, B=1, C=2... 一串字母当成n维向量，跟一个n×n的矩阵相乘，再将得出的结果MOD26。

直接给出网上的脚本可以参考：

```
import numpy as np




m = 'YOURPINNOISFOURONETWOSIX'  #明文
a = np.matrix([[11,2,19],[5,23,25],[20,7,17]])  #密钥LCTFXZUHR
num_m = []
temp = []
count = 1
for i in m:  #将明文分为三个一组
    temp.append(ord(i)-ord('A'))
    if count % 3 == 0:
        num_m.append(temp)
        temp = []
    count += 1
mat_m = [np.matrix(i).T for i in num_m]  #将明文分组转换为向量形式
mat_c = [a * i % 26 for i in mat_m]  #得到密文分组的向量形式
num_c = []
temp = []
for i in mat_c:  #将密文向量转换为列表形式，且合并到一个列表
    temp = i.tolist()
    for j in range(3):
        num_c.append(temp[j][0])
c = [chr(i+ord('A')) for i in num_c]
print(''.join(c))  #连接成字符串,输出密文
```

```
希尔密码在线加解密：
http://www.atoolbox.net/Tool.php?Id=914
```

维吉尼亚密码：

维吉尼亚密码（又译维热纳尔密码）是使用一系列凯撒密码组成密码字母表的加密算法，属于多表密码的一种简单形式。

维吉尼亚加解密表格：

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

当明文为

ATTACKATDAWN

选择某一关键词并重复而得到密钥，如关键词为LEMON时，密钥为：

LEMONLEMONLE

对于明文的第一个字母A，对应密钥的第一个字母L，于是使用表格中L行字母表进行加密，得到密文第一个字母L。类似地，明文第二个字母为T，在表格中使用对应的E行进行加密，得到密文第二个字母X。以此类推，可以得到：

明文：ATTACKATDAWN

密钥：LEMONLEMONLE

密文：LXFOPVEFRNHR

```
维吉尼亚密码在线加解密：
https://www.qqxiuzi.cn/bianma/weijiniyamima.php
```

维吉尼亚密码真题-one：

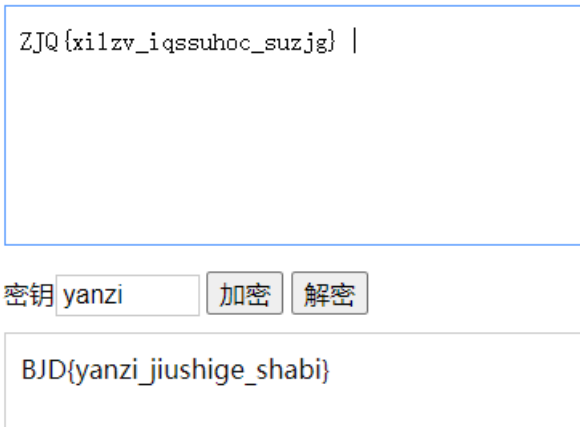
BUUCTF-Crypto-[BJDCTF 2nd]燕言燕语-y1ng

小燕子，穿花衣，年年春天来这里，我问燕子你为啥来，燕子说:

79616E7A69205A4A517B78696C7A765F6971737375686F635F73757A6A677D20

16进制转字符串

维吉尼亚在线直接解



棋盘密码（Polybius）：

波利比奥斯棋盘（Polybius Checkerboard）是棋盘密码的一种，是利用波利比奥斯方阵(Polybius Square)进行加密的密码方式，产生于公元前两世纪的希腊，相传是世界上最早的一种密码。简单的来说就是把字母排列好，用坐标的形式表现出来。字母是密文，明文便是字母的坐标。

借鉴知乎上的图

	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

先看纵向，在看横向。得到密文

明文HELLO 密文：23 15 31 31 34

普莱费尔密码（playfair）：

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）。

取playfair example为密钥。即可得到表

P L A Y F

I R E X M

B C D G H

K N O Q S

T U V W Z

需要加密的为Hide the gold

HI DE TH EG OL

加密后为

BM OD ZB XD

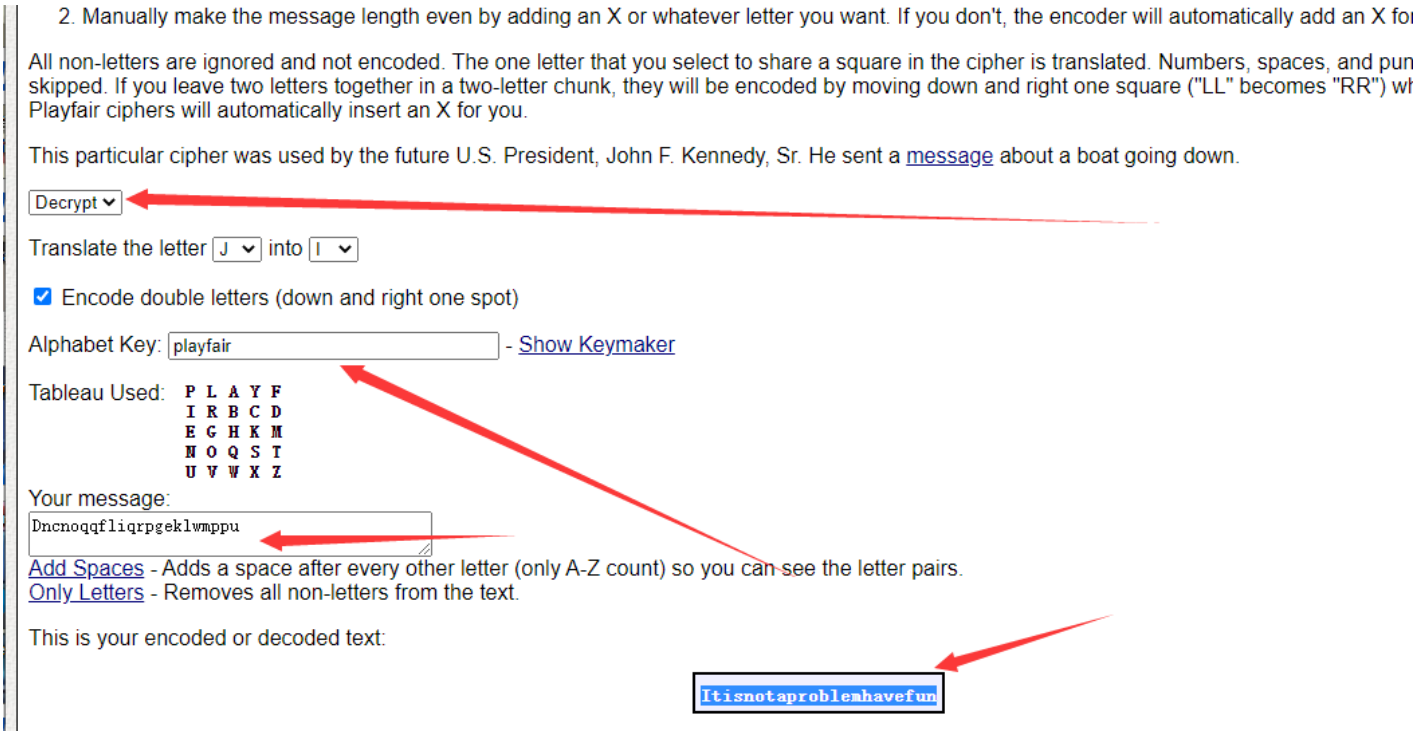
```
在线普莱费尔加解密：
http://www.atoolbox.net/Tool.php?Id=912
http://rumkin.com/tools/cipher/playfair.php
```

普莱费尔真题-one：

Buuctf-crypto-cipher

还能提示什么呢？公平的玩吧（密钥自己找） Dncnoqqfliqrpgeklwmppu 注意：得到的 flag 请包上 flag{} 提交，flag{小写字母}

http://rumkin.com/tools/cipher/playfair.php



Nihilist密码：

Nihilist跟polybius密码差不多

相同的先看纵向，在看横向。

例如a=[2,3]=23

	1	2	3	4	5
1	h	e	l	o	w
2	r	d	a	b	c
3	f	g	i/j	k	m
4	n	p	q	s	t
5	u	v	x	y	z

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键包含

9键表就是通过九键上多次字母来进行字母提取

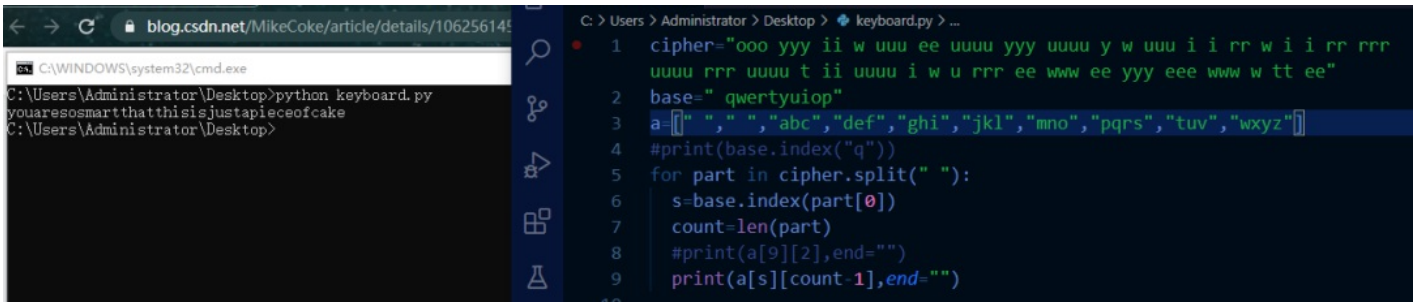
26键包含通过明文多个字符对应一个密文

9键表真题：

直接放两道题来理解

Buuctf- Crypto-[NCTF2019]Keyboard

分析第一个字符串，ooo，o在键盘上对应的是9，有3个o，表示第9个格子的第三个字母，就是y。那yyy就是指字母o




```
cipher="ooo yyy ii w uuu ee uuuu yyy uuuu y w uuu i i rr w i i rr rrr uuuu rrr uuuu t ii uuuu i w u rrr ee
base=" qwertyuiop"
a=[" "," ","abc","def","ghi","jkl","mno","pqrs","tuv","wxyz"]
#print(base.index("q"))
for part in cipher.split(" "):
  s=base.index(part[0])
  count=len(part)
  #print(a[9][2],end="")
  print(a[s][count-1],end="")
```

第一步：

构造3个需要的值，变量和列表

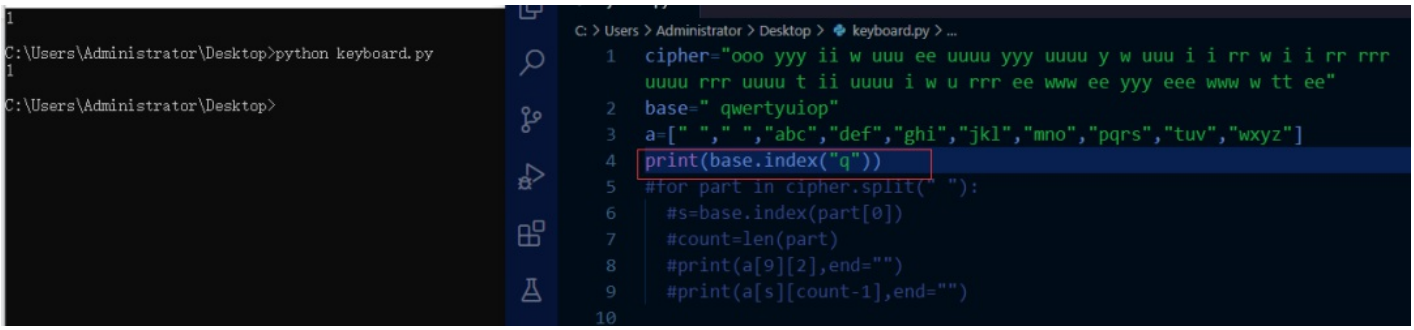
cipher就是题目附件的字符串

base就是键盘上一行对应的数字，第一个为空。因为索引的时候，第一个为0。使得q正好为1

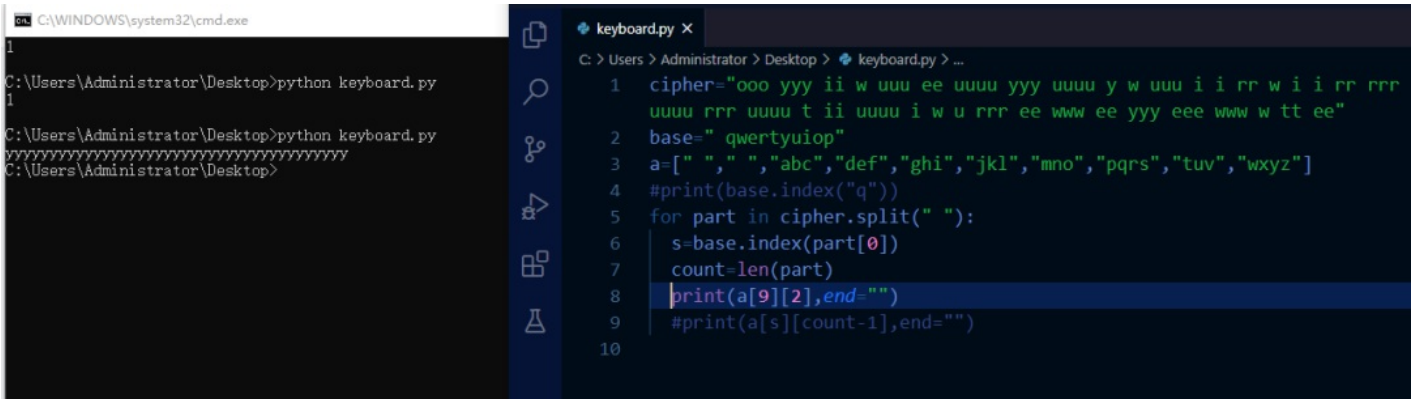
a列表第一个的空格字符串同理。也是0。如下走下来空格对应九格键盘上的1，abc就对应九格键盘上的数字2，def对应3。

第二步：

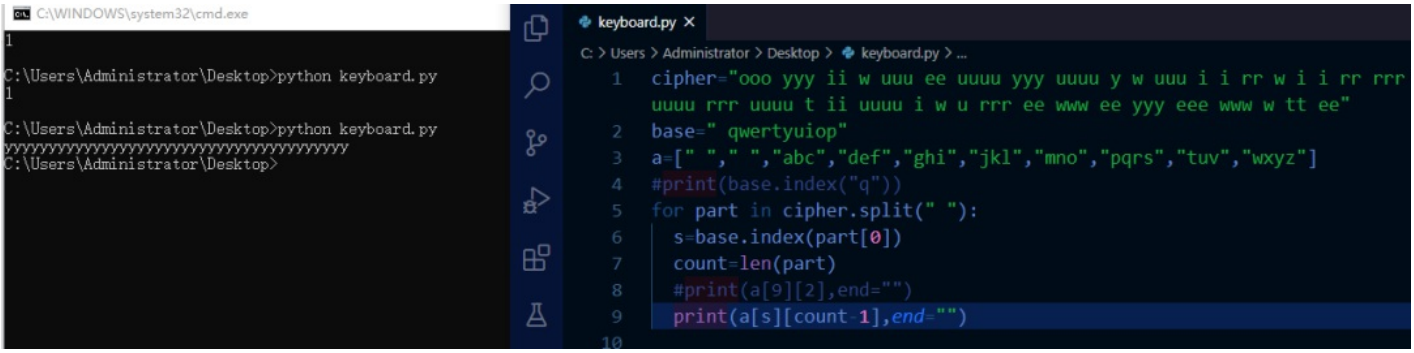
index就是索引的值，就是取键盘上的数字



a[][]。列表的两次，就直接取对应的字母了。end是为了不换行。



count的减1，还是因为第一个是0



Buuctf- Crypo-[MRCTF2020]keyboard

得到的flag用

MRCTF{xxxxxx}形式上叫

都为小写字母

6

666

22

444

555

33

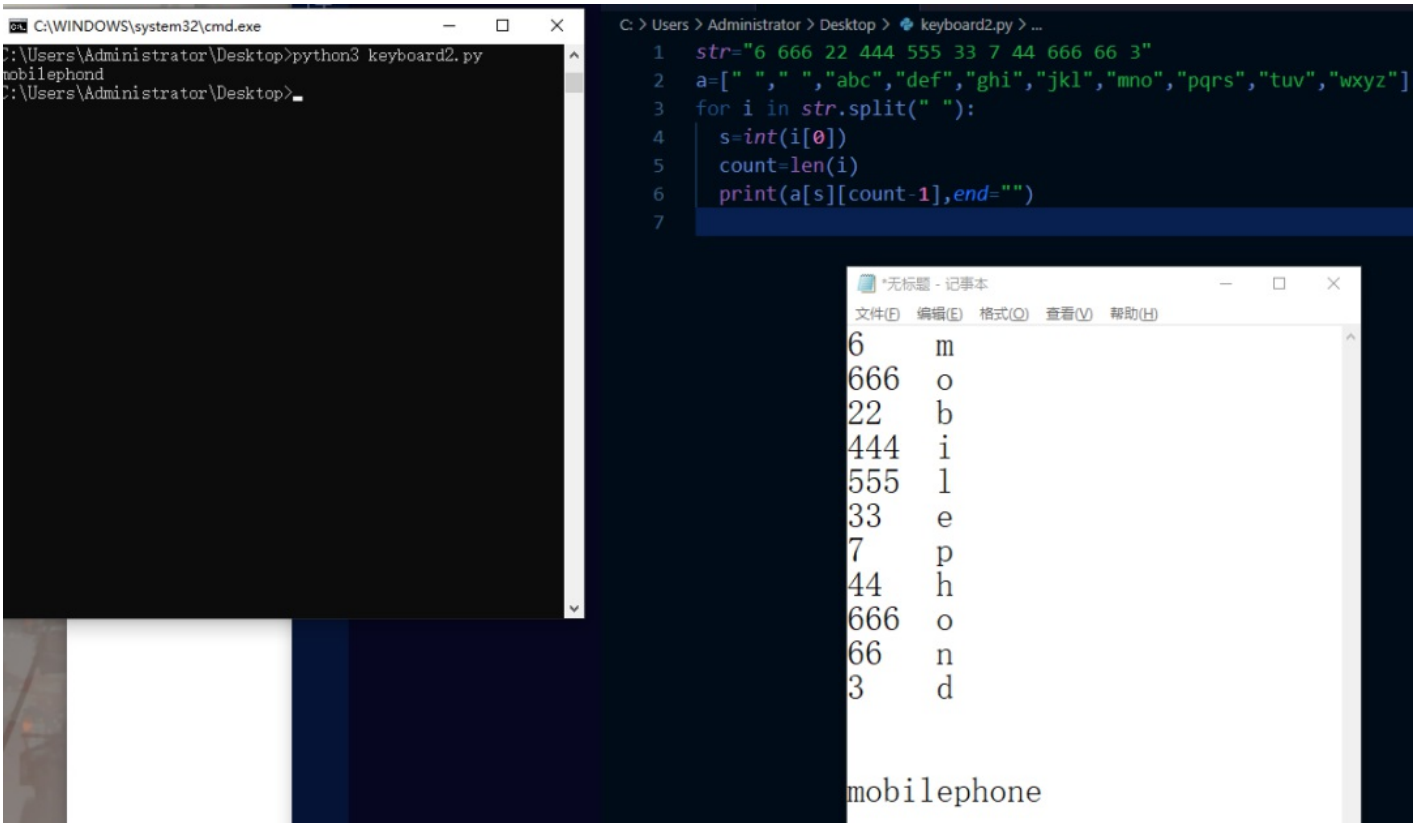
7

44

666

66

3




```
str="6 666 22 444 555 33 7 44 666 66 3"
a=[" "," ","abc","def","ghi","jkl","mno","pqrs","tuv","wxyz"]
for i in str.split(" "):
  s=int(i[0])
  count=len(i)
  print(a[s][count-1],end="")
```

这边解出来最后一个字母是d。但提交不上。搜一下这个单词就知道最后一个应该打错了。是e

26键包含真题：

密码学-keyword

根据题目hint：应该。是键盘包围，或者画图

BHUK,LP TGBNHGYT BHUK,LP UYGBN TGBNHGYT BHUK,LP BHUK,LP TGBNHGYT BHUK,LP TGBNHGYT UYGBN

空格划组 逗号也算一个里面

直接画出来

NBNCBNNBNBC

栅栏密码：

栅栏密码是典型的置换密码。把明文分成n个1组。在进行连接。根据如何连接，又分为普通栅栏密码（|||栅栏密码）和W型栅栏密码。

普通栅栏密码（|||栅栏密码）

值和n：

fslda1g2{3a}

n=2

按2个分组

fs ld a1 g2 {3 a}

取第一个

flag{a

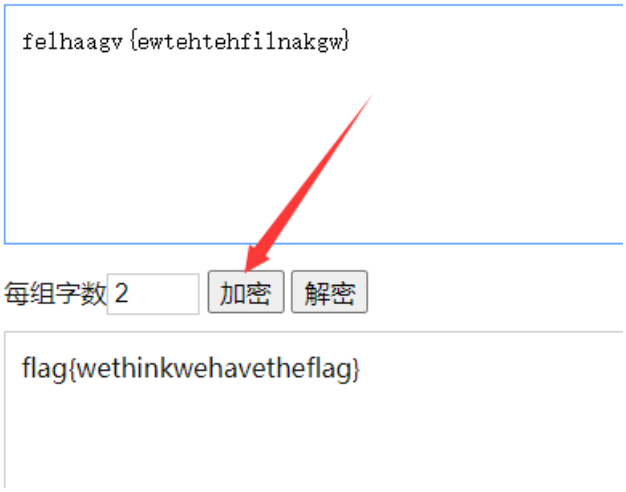
在取全部

flag{asd123}

普通栅栏密码（|||栅栏密码）真题-one：

Buuctf-Crypto-篱笆墙的影子

直接两栏获得flag



w型栅栏密码

写成W型的栅栏密码。但读取还是按行从左往右读取。

值和n：

flag{asd123}

n=2

照样是2个分组

f.a.{.s.1.3

.l.g.a.d.2.}

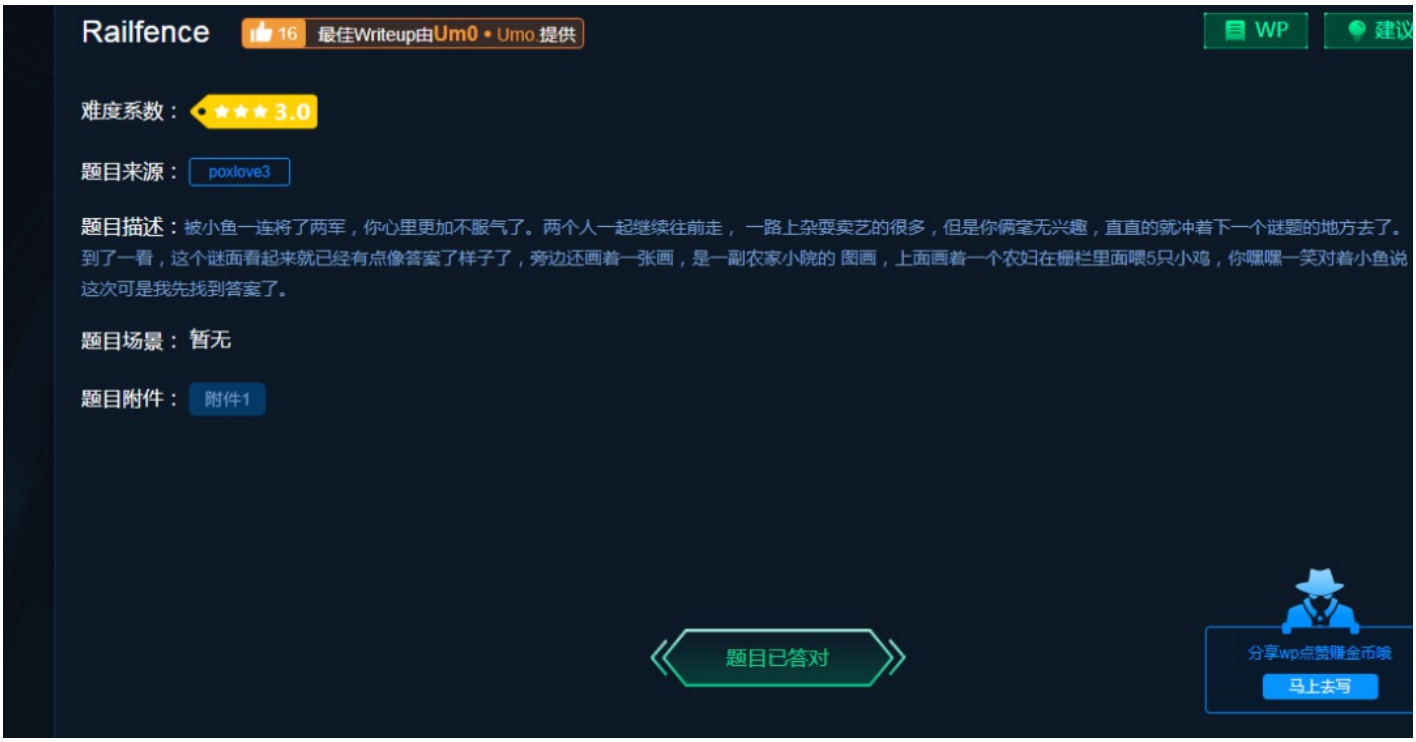
直接从左往右读取

fa{s13lgad2}

W型栅栏密码真题-one：

攻防世界Crypto新手-Railfence

根据题目名和题目描述可知是栅栏密码。



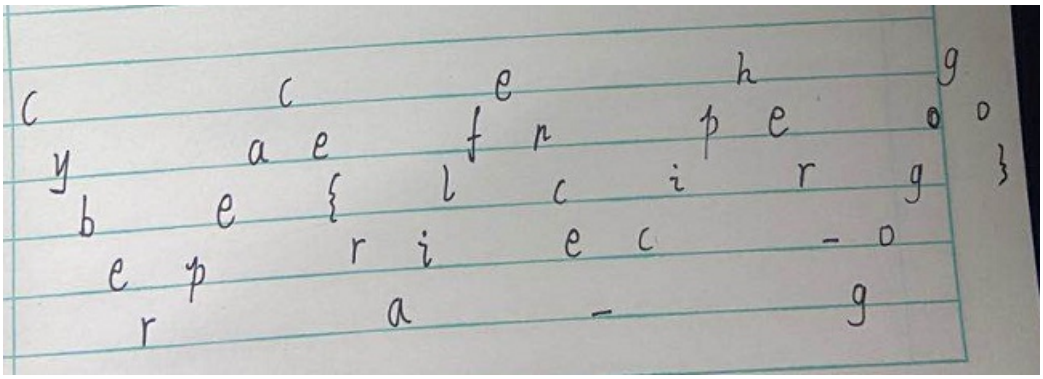
但不是普通的|||型栅栏密码

是变种的W型栅栏密码

```
在线解密：
http://www.atoolbox.net/Tool.php?Id=777
```

手解：

把值按照W型进行横排排列，把明文的第一个填充到密文的第一行第1个位置，把明文的第二个填充到密文的第一行第9个位置。在把明文的第三个填充到密文的第17个位置。在把明文的第四个填充到密文的第25个位置。在把明文的第五个填充到密文的第33个位置。



当len=35，key=5时（这个就自己画一画吧）然后你就会发现：首行和尾行的间隔依旧不变，假设行数为i，当当前数为第2行的奇数的时候，下一个数字为2+6=8也就是（key-i）*2,若当前数为第二行偶数的时候，下一个数字为8+2=10也就是(i-1)*2。

```
                    11  13  15  17  19  21  23  25  27  29  31  33  35
c c e h g y a e f n p e o b b e { l c i r g } e p r i e c _ o r a _ g
1 2 3 4 5 6 7 8 9 10  12  14  16  18  20  22  24  26  28  30  32  34
c-------f-------{-------p-------a--------
-c-----e-n-----e-l-----e-r-----r-_-------
--e---a---p---b---c---}---i---o---g------
---h-y-----e-o-----i-g-----e-_------------
----g-------o-------r-------c------------


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--------
key=5
len=35
1   9   17    25   33                        (key-1)*2=8
2   8   10    16   18   32   34               (key-i)*2=6    (i-1)*2=2
3   7   11    15   19   23   27   31   35     (key-i)*2=4    (i-1)*2=4
4   6   12    14   20   22   28   30          (key-i)*2=2    (i-1)*2=6
5   13  21    29                             (key-1)*2
```

普通栅栏密码加解密：
https://www.qqxiuzi.cn/bianma/zhalanmima.php

W型栅栏密码在线加解密：
http://www.atoolbox.net/Tool.php?Id=777

云影密码：

有1，2，4，8这四个数字，可以通过加法来用这四个数字表示0-9中的任何一个数字，列如0=28， 也就是0=2+8，同理7=124， 9=18。这样之后再用1-26来表示26个英文字母，就有了密文与明文之间的对应关系。引入0来作为间隔，以免出现混乱。所以云影密码又叫“01248密码”。

也给出一个python脚本地址：
https://www.jianshu.com/p/b5aa5cf60f83

```
#!/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)
```

简单位移密码：

这个密码是我在《ctf特训营》这本书上看到的。自己并没有在题目中做到过

实例借鉴书中

m=flag{easy_easy_crypto}

k=”3124”

len(k)=4，切分m。

flay {eas y_ea sy_c rypt o}

按照3124直接排列

Lafg ea{s _eya y_sc yprt }o

密文：

Lafgea{s_eyay_scyprt}o

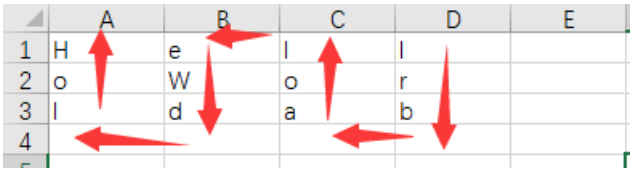
解密代码：

```
def shift_decrypt(c,k):
    l=len(k)
    m=""
    for i in range(0,len(c),l):
        tmp_m=[""]*l
        if i+l>=len(c):
            tmp_c=c[i:]
            use=[]
            for kindex in range(len(tmp_c)):
                use.append(int(k[kindex])-1)
            use.sort()
            for kindex in range(len(tmp_c)):
                tmp_m[kindex]=tmp_c[use.index(int(k[kindex])-1)]
        else:
            tmp_c=c[i:i+l]
            for kindex in range(len(tmp_c)):
                tmp_m[kindex]=tmp_c[int(k[kindex])-1]
        m+="".join(tmp_m)
    return m
c="lafgea{s_eyay_scyprt}o"
k="3124"
print shift_decrypt(c,k)
```

曲路密码：

按照事先约定的原则把明文填入表中

例如：明文为HelloWorldab



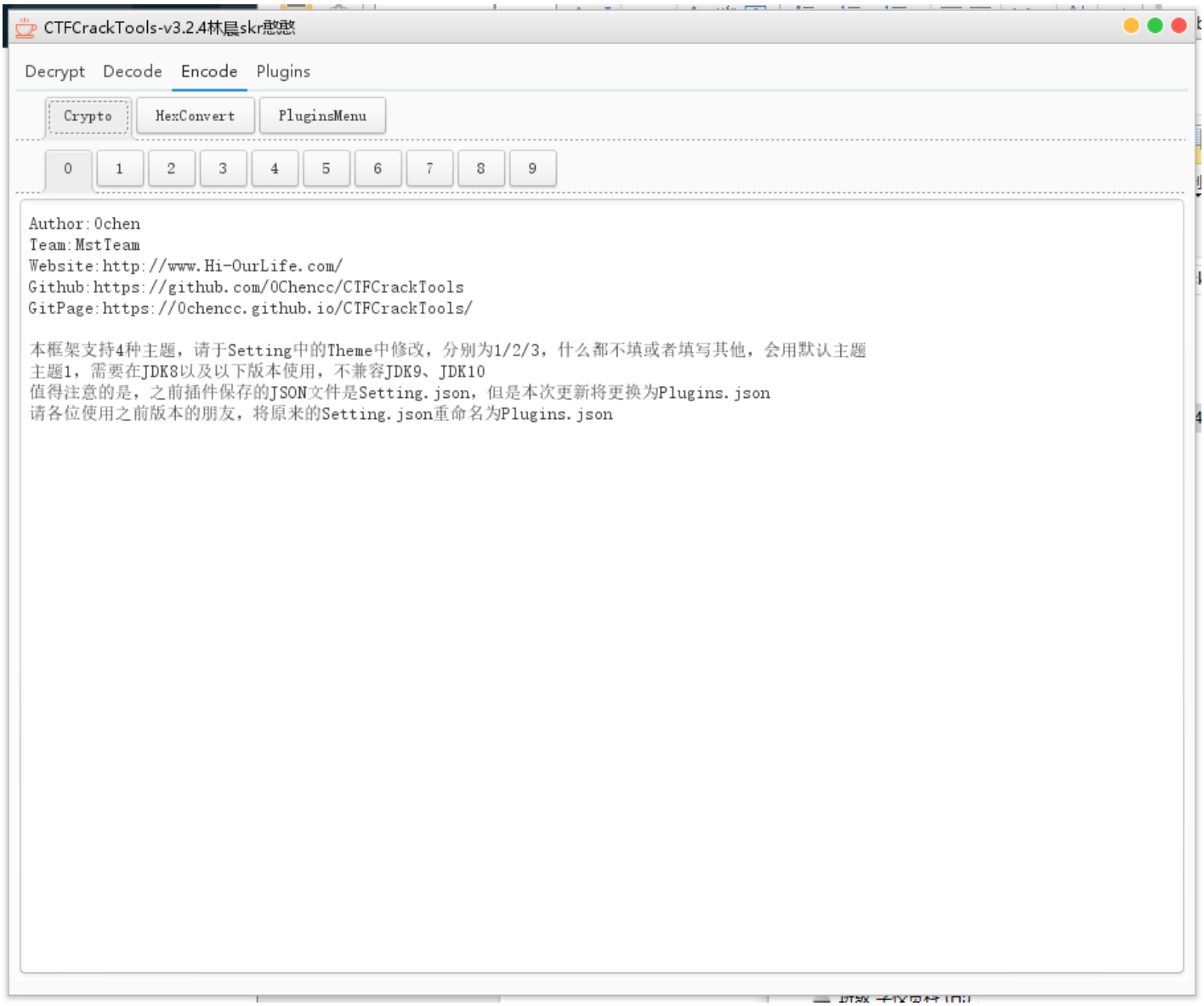
按照一定的顺序进行遍历

密文就是lrbaoleWdloH

CTF crypto线下工具推荐：

CTFCrackTools

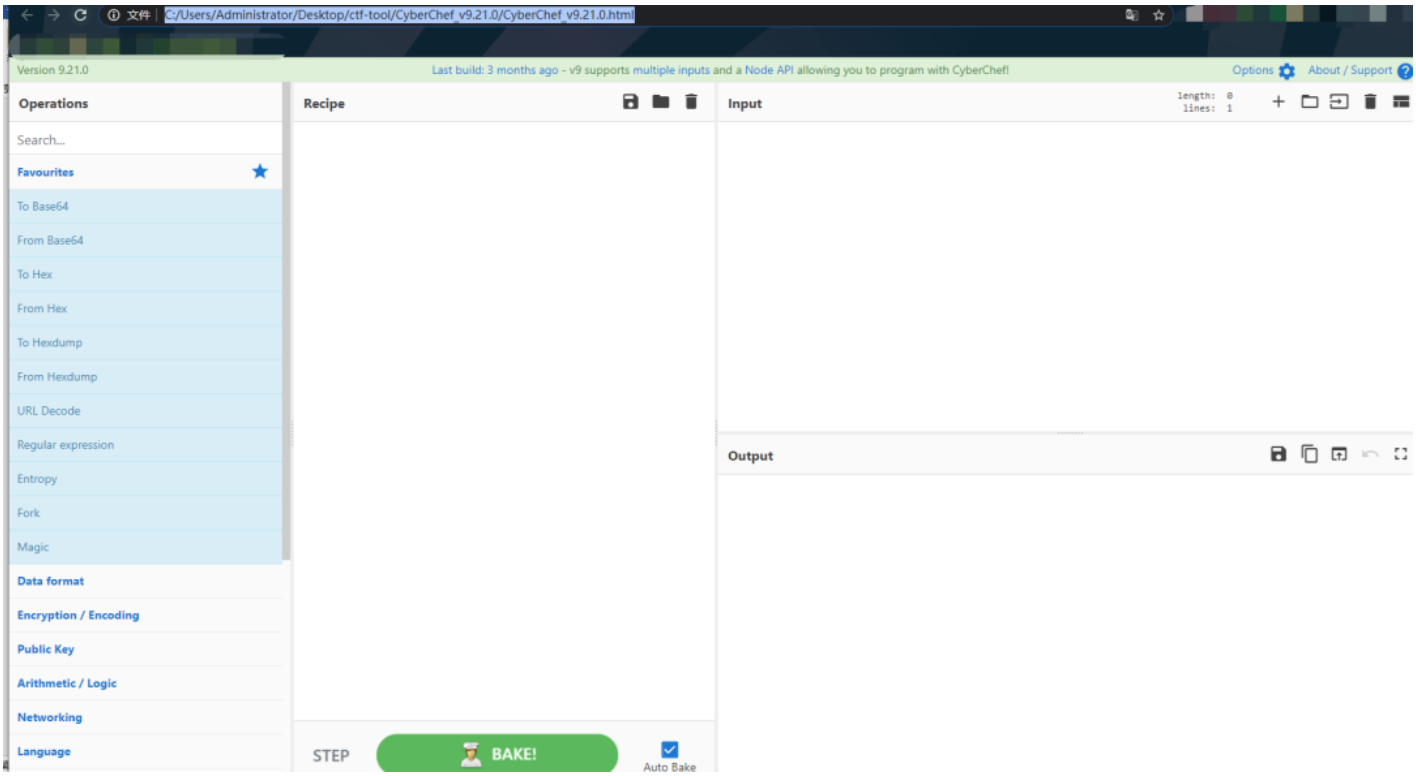
https://github.com/Acmesec/CTFCrackTools



CyberChef

https://www.chinabaiker.com/cyberchef.htm

直接可以下载到本地



参考：

```
https://ctf-wiki.github.io/ctf-wiki/crypto
https://zh.wikipedia.org/wiki
https://baike.baidu.com
《ctf特训营》
https://buuoj.cn/
```

相关实验：

相关实验：密码学原理

https://www.hetianlab.com/cour.do?w=1&c=c990c65e-108f-4d10-9efa-4aad77fc852b

（密码学是研究如何隐密地传递信息的学科。通过本课程实验掌握密码学的相关知识。）