

# CTF中的那些不为人知的古典字典

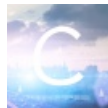
转载

网安激家 于 2021-08-17 21:11:37 发布 49 收藏 1

分类专栏: [程序员](#) 文章标签: [密码学](#) [加密解密](#) [网络安全](#) [信息安全](#) [经验分享](#)

原文链接: <https://forum.butian.net/share/360>

版权



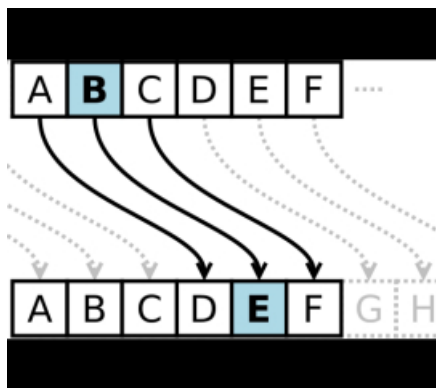
[程序员](#) 专栏收录该内容

28 篇文章 1 订阅

订阅专栏

## 一. 古典密码

### 1. 凯撒密码 (Caesar Cipher)



凯撒密码是一种非常古老的密码，其原理是通过字母的位移将原文和密文一一对应。

举个例子：明文是“Hello world”，偏移量为3。

所以A—>C，B—>D，依次类推，

所以密文就是“Khoor zruog”

根据偏移量的不同，还存在一些特定的凯撒密码名称

偏移量为10: Avocat

偏移量为13: ROT13

偏移量为-5: Cassis

偏移量为-6: Cassette

在线解密网站: <https://www.qqxiuzi.cn/bianma/kaisamima.php>

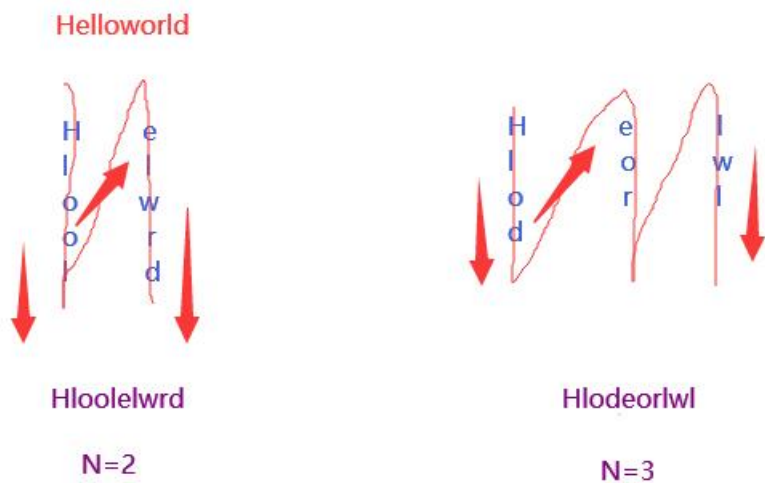
### 2. 培根密码 (Bacon's Cipher)



栅栏密码也分为两种：Z型和W型

好多文章都只讲Z型，但考试经常出W型的，所以我两种都讲一下

### Z型（常规）



就是按照N个一组分好后，按列从上到下组合成新的字符串

例如：“Helloworld”

N=2时：“Hlloolelwrđ”；N=3时：“Hlodeorlwl”

### W型（变形）

这个很恶心，我研究了半天才搞出来

W型顾名思义，就是把明文按照W型排列，按行输出

其中栏数N即为行数，如图：（只能画出来了）

abcdefghijklmnop . N=4

1	a		g		m
2	b	f	h	l	n
3	c	e	i	k	o
4	d		j		p

栅栏密码 (W型) 在线解密网站: <http://www.atoolbox.net/Tool.php?Id=777>

栅栏密码 (Z型) 在线解密网站: <https://www.qqxiuzi.cn/bianma/zhalanmima.php>

### 5. 仿射密码 (Affine Cipher)

单表加密的一种, 字母表的每个字母相应的值使用一个简单的数学函数对应一个数值, 再把对应数值转换成字母。一般仿射密码都会给你一个a一个b, 这是解密的关键

加密函数:  $E(x)=(ax+b)\text{mod } m;$

解密函数:  $D(x)=a^{-1}*(x-b)\text{mod } m;$

其中涉及到的数学知识是乘法逆元

例子: 假设a=5, b=8; 明文为AFFINECIPHER

则加密为:

明文	A	F	F	I	N	E	C	I	P	H	E	R
x	0	5	5	8	13	4	2	8	15	7	4	17
$y = 5x + 8$	8	33	33	48	73	28	18	48	83	43	28	93
$y \text{ mod } 26$	8	7	7	22	21	2	18	22	5	17	2	15
密文	I	H	H	W	V	C	S	W	F	R	C	P

解密为:

密文	I	H	H	W	V	C	S	W	F	R	C	P
$y$	8	7	7	22	21	2	18	22	5	17	2	15
$x = 21(y - 8)$	0	-21	-21	294	273	-126	210	294	-63	189	-126	147
$x \bmod 26$	0	5	5	8	13	4	2	8	15	7	4	17
明文	A	F	F	I	N	E	C	I	P	H	E	R

而有些仿射密码的题目不会给a和b，而是直接给对应的字符  
(2021MSSCTF—Crypto T1)

仿射密码没有在线的解密工具，所以以Python脚本方式展示

```
def get(a, b):
    if b == 0:
        return 1, 0
    else:
        k = a // b
        remainder = a % b
        x1, y1 = get(b, remainder)
        x, y = y1, x1 - k * y1
        return x, y
s = input("请输入解密字符: ").upper()
a = int(input("请输入a: "))
b = int(input("请输入b: "))
#求a关于26的乘法逆元
x, y = get(a, 26)
a1 = x % 26
l = len(s)
for i in range(1):
    cipher = a1 * (ord(s[i]) - 65 - b) % 26
    res = chr(cipher + 65)
    print(res, end='')
```

此处鸣谢：CSDN博主“向那风”

## 6. 猪圈密码 (Pigpen Cipher)

(2020第四届强网杯青少年专项赛线上—Crypto—easy\_Crypto)

猪圈密码是一种以格子为基础的简单替代密码，一一对应的  
这个玩意儿长这样：

└	┐	┌	┘	◻	◻	└	┐
└	┐	┌	┘	◻	◻	└	┐
∨	∩	∪	∧	∨	∩	∪	∧
⋮	⋮	⋮	⋮	:	=	[	\
.	-	'	<	>		~	∕

遇到之后直接用在线解密平台解密即可

猪圈密码在线解密平台：<http://ctf.ssleye.com/pigpen.html>

## 7. 维吉尼亚密码 (Vigenère Cipher)

是使用一系列凯撒密码组成密码字母表的加密算法

意思是什么呢？

维吉尼亚密码通常会有两个元素：明文和密钥

密钥的长度不一定要和明文长度一样

加密时，密钥先循环称为密钥流，使其与明文长度相同，然后以偏移量加密

ps: 偏移量是指当前字母相对于A的偏移量

举个例子：明文时ATTACKDAWN；密钥为LEMON

首先循环密钥形成密钥流：LEMONLEMONLE

然后根据偏移量进行逐个字符的加密

如第1位明文是A，密钥是L，L的偏移量为12-1=11，则加密后应该为(A+11)mod 26，即为L。

同理，第二位明文是T，密文是E，E的偏移量为5-1=4，则加密后应该为(A+4)mod 26，即为X。

依次类推，可以得到密文LXFOPVEFRNHR。

当然，还可以利用图表进行加密（我觉得眼都花了）

	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

维吉尼亚密码在线解密网站：<http://www.atoolbox.net/Tool.php?id=856>

## 结尾

以上就是CTF中经常出现的古典密码

其实有些特征都很明显，一看都能看出来是哪种密码（培根，猪圈等）

像凯撒密码这类一般都会给题目提示或者要尝试

密码学只能多练...没别的方法，多见见就知道是谁了

如果进线下赛了就要去网上找解密脚本了（因为线下赛不让联网哈哈）