CTF-密码学相关

原创

AbyssssssssssS 于 2019-09-10 19:58:19 发布 3197 收藏 22
分类专栏： CTF 文章标签： ctf密码

本文链接：https://blog.csdn.net/AbyssssssssssS/article/details/100674081

参考：千千秀字、百度百科、CTF编码和加密总结 、CTF常见编码和加密特征 、CTF中Crypty（密码类）入门必看

目录

换位加密

1.栅栏密码

2.曲路密码

3.列/行置换

替换密码

1.凯撒密码

2.当铺密码

3.培根密码

4.费娜姆密码

5.猪圈密码

6.ROT5/13/18/47

7.Rabbit流密码

8.跳舞的小人

9.QWE加密

10.埃特巴什密码

11.简单替换密码

12.希尔密码

13.波利比奥斯方阵密码

14.夏多密码（曲折加密）

15.普莱菲尔密码

16.维吉尼亚密码

17.自动密钥密码

18.博福特密码

19.滚动密钥密码

20.Porta密码

21.同音替换密码

22.仿射密码

23.ADFGX和ADFGVX密码

24.双密码

25.棋盘密码/跨棋盘密码

26.分组摩尔斯替换密码

27.Bazeries密码

28.Digrafid密码

29.比尔密码

30.键盘密码

31.盲文

其他有趣的机械密码

1.恩尼格码密码

代码混淆加密:

1.asp混淆加密

2.php混淆加密

3.css/js混淆加密

4.VBScript.Encode混淆加密

5.ppencode

6.rrencode

7.jjencode/aaencode

8.JSfuck

9.jother

10.brainfuck编程语言

其他

1.SHA 1/224/256/384/512

2.MD5加密

3.Adler-32校验

4.CRC校验

5.Gost加密

6.HAVAL加密算法

7.RIPEMD算法

8.Snefru散列算法

9.Tiger散列算法

10.Whirlpool算法

11.DES加密

12.AES加密

13.TripleDES

14.RC4/5/6

15.RSA加密

一些别的网站

字符编码

1.ASCII编码

ASCII（American Standard Code for Information Interchange，美国信息互换标准代码）是基于拉丁字母的一套电脑编码系统，主要用于显示现代美式英语，并等同于国际标准ISO/IEC 646。标准ASCII编码可表示128个字符，包括大小写拉丁字母，阿拉伯数字、英语标点符号，以及在美式英语中使用的特殊控制字符。另有扩展版本的ASCII编码添加了一些西欧字符，可以表示255个字符，但是西欧国家间对扩充的字符定义不一致，并不是通用版本。

如：97（十进制）-a

ASCII在线查询

2.Unicode编码

Unicode 编码是一种力求容纳世界上所有字符的编码格式，因此也被称为万国码、统一码等等。Unicode 编码给每一个字符都指定了统一且唯一的编码，这使得不同种类的文字可以跨语言、跨平台的应用。

Unicode编码有以下四种编码方式：

源文本：`The`

- &#x [Hex]：`&#x0054;&#x0068;&#x0065;`
- &# [Decimal]：`&#00084;&#00104;&#00101;`
- \U [Hex]：`\U0054\U0068\U0065`
- \U+ [Hex]：`\U+0054\U+0068\U+0065`

转换：ASCII-Unicode-中文

Unicode编码转换

3.UTF-8编码

UTF-8 是Unicode字符集的一种转换格式，十六进制编码。UTF-8用1到4个字节编码Unicode字符，相对于Unicode固定的4字节，更省存储空间。UTF-8能表示Unicode编码中的所有字符，用在网页上可以同一页面显示多种语言文字。本页的UTF-8编码转换工具，可以将中文、日文、韩文等亚洲字符集转换成UTF-8编码格式，也可以由UTF-8编码还原为相应的文字。

如：马-%E9%A9%AC

UTF-8编码转换

4.UTF-16编码

UTF-16是Unicode字符集的一种转换格式，十六进制编码。UTF-16以 2 字节或 4 字节编码处理Unicode字符，用在网页上可以同一页面显示多种语言文字。本页的UTF-16编码转换工具，可以将中文、日文、韩文等亚洲字符集转换成UTF-16编码格式，也可以由UTF-16编码还原为相应的文字。

UTF-32 使用四个字节为每个字符编码，使得 UTF-32 占用空间通常会是其它编码的二到四倍。UTF-32 与 UTF-16 一样有大尾序和小尾序之别，编码前会放置 U+0000FEFF 或 U+FFFE0000 以区分。

如：马

Unicode编码：**00009A6C**

UTF8编码：**E9A9AC**

UTF16BE编码：**FEFF9A6C**

UTF16LE编码：**FFFE6C9A**

UTF32BE编码：**0000FEFF00009A6C**

UTF32LE编码：**FFFE00006C9A0000**

Unicode和UTF编码转换

5.进制转换

常用的有二进制、八进制、十进制和十六进制。不同进制之间转换都有一套固定的算法。

2～36进制转换

6.URL字符编码

URL 是 Uniform Resource Locator 的简称，中文译为“统一资源定位符”，也就是网络地址。URL地址（常说网址）规定了常用地数字，字母可以直接使用，另外一批作为特殊用户字符也可以直接用（/,:@等），剩下的其它所有字符必须通过%xx编码处理。

编码方法：在该字节ascii码的的16进制字符前面加%.

如：马-%E9%A9%AC

URL字符编码解码

7.摩斯电码

摩尔斯电码（又译为摩斯电码，Morse code）是一种时通时断的信号代码，这种信号代码通过不同的排列顺序来表达不同的英文字母、数字和标点符号等。

如：-ma--- .-

摩尔斯电码

8.Base64/32/16编码

base32的编码表是由（A-Z、2-7）32个可见字符构成，“=”符号用作后缀填充。
base64的编码表是由（A-Z、a-z、0-9、+、/）64个可见字符构成，“=”符号用作后缀填充。
base58的编码表相比base64少了数字0，大写字母I，O，小写字母 l (这个是L），以及符号‘+’和‘/’

Base16编码使用16个ASCII可打印字符（数字0-9和字母A-F）对任意字节数据进行编码。base16不可能用到填充符号“=”

编码原理：Base64将输入字符串按字节切分，取得每个字节对应的二进制值（若不足8比特则高位补0），然后将这些二进制数值串联起来，再按照6比特一组进行切分（因为2^6=64），最后一组若不足6比特则末尾补0。将每组二进制值转换成十进制，然后在上述表格中找到对应的符号并串联起来就是Base64编码结果。（详情见Base64编码转换）

如:

base32（1234567）= GEZDGNBVGY3Q====
特征：大写字母和数字，不满5的倍数，用‘=’补齐。
base64（1234567）= MTIzNDU2Nw==
特征：大小写字母和数字，不满3的倍数，用‘=’补齐。
base58（1234567）= 2s8YYFs4Vc

Base64编码转换

9.shellcode编码

Shellcode实际是一段代码（也可以是填充数据），是用来发送到服务器利用特定漏洞的代码，一般可以获取权限。另外，Shellcode一般是作为数据发送给受攻击服务的。

如：The quick brown fox jumps over the lazy dog　→

```
\x54\x68\x65\x7f\x71\x75\x69\x63\x6b\x7f\x62\x72\x6f\x77\x6e\x7f\x66\x6f\x78\x7f\x6a\x75\x6d\x70\x73\x7f\x6f\x7
```

ShellCode变形编码大法

10.Quoted-printable编码

Quoted-Printable编码可译为“可打印字符引用编码”，或者“使用可打印字符的编码”。通常我们接收电子邮件，查看电子邮件原始信息，经常会看到这种类型的编码，电子邮件信头显示：Content-Transfer-Encoding: quoted-printable。它是多用途互联网邮件扩展（MIME) 一种实现方式。Quoted-Printable编码是字符对应的编码，每个末编码的二进制字符被编码成三个字符，即一个等号和一个十六进制的数字。

Quoted-Printable编码（QP编码）详解

如：马了戈壁-=E9=A9=AC=E4=BA=86=E6=88=88=E5=A3=81

Quoted-Printable编码解码

11.XX encode编码

XXencode是一种二进制到文字的编码！它跟UUencode以及Base64编码方法很类似。它也是定义了用可打印字符表示二进制文字一种方法，不是一种新的编码集合。

XXencode将输入文本以每三个字节为单位进行编码，如果最后剩下的资料少于三个字节，不够的部份用零补齐。三个字节共有24个Bit，以6-bit为单位分为4个组，每个组以十进制来表示所出现的字节的数值。这个数值只会落在0到63之间。它64可打印字符固定字符范围及顺序！包括大小写字母、数字以及+-字符。

它较UUencode编码优点在于它64字符是常见字符，没有任何特殊字符！跟base64打印字符相比，就是uuencode多一个‘-’字符，少一个‘/’字符。但是，它里面字符顺序与base64完全不一样。

如：马勒戈壁-6kir+pPXegRc+

在线XXencode编码解码

12.UU encode编码

UUencode是一种二进制到文字的编码，它不是MIME编码中一员。最早在unix 邮件系统中使用，全称：Unix-to-Unix encoding。它也是定义了用可打印字符表示二进制文字一种方法，并不是一种新的编码集合。

Uuencode将输入文本以每三个字节为单位进行编码，如果最后剩下的资料少于三个字节，不够的部份用零补齐。三个字节共有24个Bit，以6-bit为单位分为4个组，每个组以十进制来表示所出现的字节的数值。这个数值只会落在0到63之间。**然后将每个数加上32**，所产生的结果刚好落在ASCII字符集中可打印字符（32-空白…95-底线）的范围之中。跟Base64具有非常多的类似，也做了一些特殊转码说明！因为对所有文本都会编码一次可读性不是很好！

如：马勒戈壁-(PNW`U;CJL=H`

在线UUencode编码解码

13.Escape/Unescape编码

Escape/Unescape加密解码/编码解码,又叫%u编码，采用UTF-16BE模式， Escape编码/加密,就是字符对应UTF-16 16进制表示方式前面加%u。Unescape解码/解密，就是去掉"%u"后，将16进制字符还原后，由utf-16转码到自己目标字符。如：字符“中”，UTF-16BE是：“6d93”，因此Escape是“%u6d93”。

如：马勒戈壁-%u9a6c%u52d2%u6208%u58c1

在线Escape编码/加密

14.HTML字符实体编码

字符实体是用一个编号写入HTML代码中来代替一个字符，在使用浏览器访问网页时会将这个编号解析还原为字符以供阅读。

字符实体分10进制和16进制。HTML ISO-8859-1 参考手册

如：马-马（10）或者马（16）

HTML字符实体转换

15.敲击码

敲击码(Tap code)是一种以非常简单的方式对文本信息进行编码的方法。因该编码对信息通过使用一系列的点击声音来编码而命名，敲击码是基于5×5方格波利比奥斯方阵来实现的，不同点是是用K字母被整合到C中。

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

16.hex编码

Hex编码就是把一个8位的字节数据用两个十六进制数展示出来，编码时，将8位二进制码重新分组成两个4位的字节，其中一个字节的低4位是原字节的高四位，另一个字节的低4位是原数据的低4位，高4位都补0，然后输出这两个字节对应十六进制数字作为编码。Hex编码后的长度是源数据的2倍。

如：ma-6D61

Hex编码/解码

文本加密为汉字

这个文本加密和解密工具可以将正常文本内容打乱为不可连读的文字或符号，换行等格式信息也会被清除，达到加密的作用。在进行文本加密时可以设定一个密码，这样只有知道密码的人才能解密文本。密码可以是数字、字母和下划线，最多九位。

如：dsfjksdnvjkds-启嚼圯豳懒嚼启喵纾豳懒启嚼=

文本加密为汉字

换位加密

1.栅栏密码

栅栏密码是一种简单的移动字符位置的加密方法，规则简单，容易破解。栅栏密码的加密方式：把文本按照一定的字数分成多个组，取每组第一个字连起来得到密文1，再取每组第二个字连起来得到密文2……最后把密文1、密文2……连成整段密文。例如：

明文：栅栏密码加密规则示例
每组字数：5

按照字数先把明文分成：
栅栏密码加
密规则示例

先取每组第一个字：栅密
再取每组第二个字：栏规
……

最后得到“栅密栏规密则码示加例”。

解密则反推：
密文被分成2个字一组：
栅密
栏规
密则
码示
加例

先取每组第一个字：栅栏密码加
再取每组第二个字：密规则示例

最后得到“栅栏密码加密规则示例”。

提示：当前的栅栏密码程序不删除空格和换行符。

- 明文或密文中如果出现连续空格将原样保留，复制到其它地方时连续空格可能会变成一个空格，注意保持原样。
- 在进行多行文本（段落）加密时，每行独立进行加密。

栅栏密码加密解密

2.曲路密码

曲路密码(Curve Cipher)是一种换位密码，需要事先双方约定密钥(也就是曲路路径)。

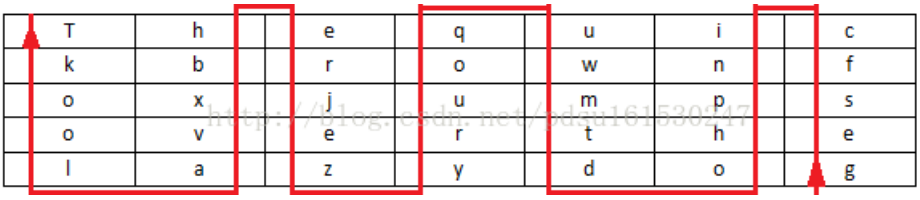
详细见链接

明文：The quick brown fox jumps over the lazy dog

填入5行7列表（事先约定填充的行列数）

T	h	e	q	u	i	c
k	b	r	o	w	n	f
o	x	j	u	m	p	s
o	v	e	r	t	h	e
l	a	z	y	d	o	g

加密的回路线(事先约定填充的行列数)



密文：gesfc inpho dtmwu qoury zejre hbxva lookT

3.列/行置换

（参考）利用这种加密方法，明文按行填写在一个矩阵中，而密文则是以预定的顺序按列读取生成的。例如如果矩阵是4列5行，那么明文“encryption algorithm”（省去空格后）可以如下写入该矩阵：

2	3	1	4
e	n	c	r
y	p	t	i
o	n	a	l
g	o	r	i
t	h	m	s

按一定的顺序读取列以生成密文。

对于这个示例，如果读取顺序为递增顺序，则明文就是：“ctarm eyogt npnoh rilis”(添加空格只是为了便于观察)。

替换密码

1.凯撒密码

凯撒密码最早由古罗马军事统帅盖乌斯·尤利乌斯·凯撒在军队中用来传递加密信息，故称凯撒密码。这是一种位移加密方式，只对26个字母进行位移替换加密，规则简单，容易破解。

凯撒密码加密解密

2.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：

王夫 井工 夫口 由中人 井中 夫夫 由中大：67 84 70 123 82 77 125

3.培根密码

培根密码中的ab,代表的是数学二进制中的0和1.通过下列的密码表进行加密和解密：
A aaaaa B aaaab C aaaba D aaabb E aabaa F aabab G aabba H aabbb I abaaa J abaab
K ababa L ababb M abbaa N abbab O abbba P abbbb Q baaaa R baaab S baaba T baabb
U babaa V babab W babba X babbb Y bbaaa Z bbaab
培根密码（看不懂）

还可以通过正体斜体表示a、b 如题

培根密码在线加解密

4.费娜姆密码

（密码：00110110010001001100100010000010110；密钥：study）

二战时德军使用过的一种密码，其实是利用了二进制的表示法来替代字母，有如下的表格作为基础：

A 1000001 B 1000010 C 1000011 D 1000100 E 1000101 F 1000110 G 1000111 H 1001000 I 1001001 J 1001010 K 1001011 L 1001100 M 1001101 N 1001110 O 1001111 P 1010000 Q 1010001 R 1010010 S 1010011 T 1010100 U 1010101 V 1010110 W 1010111 X 1011000 Y 1011001 Z 1011010

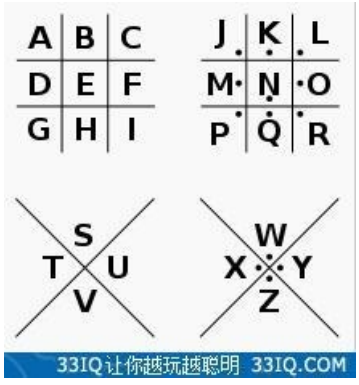
那么，比如我们要加密“Hello”，密钥用“study”，则以如下方式进行加密：

H E L L O = 1001000 1000101 1001100 1001100 1001111
S T U D Y = 1010011 1010100 1010101 1000100 1011001

加密原则：1+1=0，0+0=0，1+0=1
于是得密文：00110110010001001100100010000010110

5.猪圈密码

猪圈密码 (亦称朱高密码,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。右边的例子，是把字母填进格子的模样。　密码表：



变种：圣堂武士密码

商会加密

6.ROT5/13/18/47

ROT5：只对数字进行编码，用当前数字往前数的第5个数字替换当前数字，
ROT13：只对字母进行编码，用当前字母往前数的第13个字母替换当前字母，
ROT18：这是一个异类，本来没有，它是将ROT5和ROT13组合在一起，将其命名为ROT18。
ROT47：对数字、字母、常用符号进行编码，按照它们的ASCII值进行位置替换，用当前字符ASCII值往前数的第47位对应字符替换当前字符，用于ROT47编码的字符其ASCII值范围是33－126。

ROT5/13/18/47编码转换

7.Rabbit流密码

```
从技术上讲，Rabbit由伪随机比特流生成器组成    它采用128位密钥和64位初始化向量（IV）    输入并生成128位块流。加密是通过将此
```

详细资料：

1.http://www.cryptico.com/Files/filer/rabbit_fse.pdf

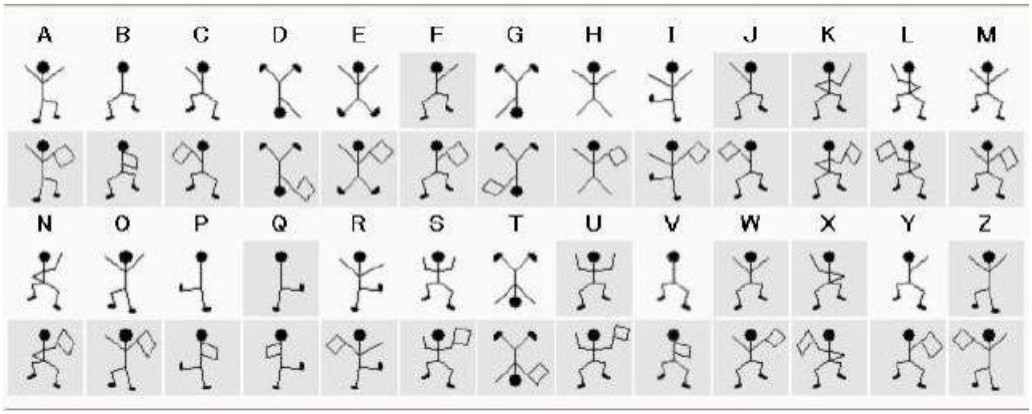
2.http://www.ietf.org/rfc/rfc4503.txt

如：马可打野（无密钥加密）- U2FsdGVkX19WEKH5FU2qI1GDp8+wkyQCxmJm9g==

Rabbit加密解密

8.跳舞的小人

来自夏洛克福尔摩斯在《归来记》中侦探案件使用的一种加密方式。



9.QWE加密

从电脑键盘上的字母从Q开始数，顺序是Q W E R T Y U I。。。对应的字母顺序依次是A B C D E F G H 也就是说Q=A,W=B,E=C，依次类推。

QWE加密解密

10.埃特巴什密码

埃特巴什码(Atbash Cipher)是一种以字母倒序排列作为特殊密钥的替换加密，也称也就是下面的对应关系：

ABCDEFGHIJKLMNOPQRSTUVWXYZ
ZYXWVUTSRQPONMLKJIHGFEDCBA

明文：the quick brown fox jumps over the lazy dog

密文：gsv jfrxp yildm ulc qfnkh levi gsv ozab wlt

Atbash加密解密

11.简单替换密码

简单换位密码(Simple Substitution Cipher)加密方式是以每个明文字母被与之唯一对应且不同的字母替换的方式实现的，它不同于恺撒密码，因为密码字母表的字母不是简单的移位，而是完全是混乱的。 比如：
明文字母 : abcdefghijklmnopqrstuvwxyz
明文字母 : phqgiumeaylnofdxjkrcvstzwb
明文：the quick brown fox jumps over the lazy dog
密文：cei jvaql hkdtf udz yvoxr dsik cei npbw gdm
当密文数据足够多时这种密码我们可以通过字频分析方法破解或其他方法破解

12.希尔密码

希尔密码(Hill Cipher)是基于线性代数多重代换密码，由Lester S. Hill在1929年发明。每个字母转换成26进制数字：A=0, B=1, C=2…Z=25一串字母当成n维向量，跟一个n×n的矩阵相乘，再将得出的结果MOD26。

希尔密码解码

如：the（key = 5 17 4 15）- gzvx

13.波利比奥斯方阵密码

波利比奥斯方阵密码（Polybius Square Cipher或称波利比奥斯棋盘）是棋盘密码的一种，是利用波利比奥斯方阵进行加密的密码方式，简单的来说就是把字母排列好，用坐标(行列)的形式表现出来。字母是密文，明文便是字母的坐标。

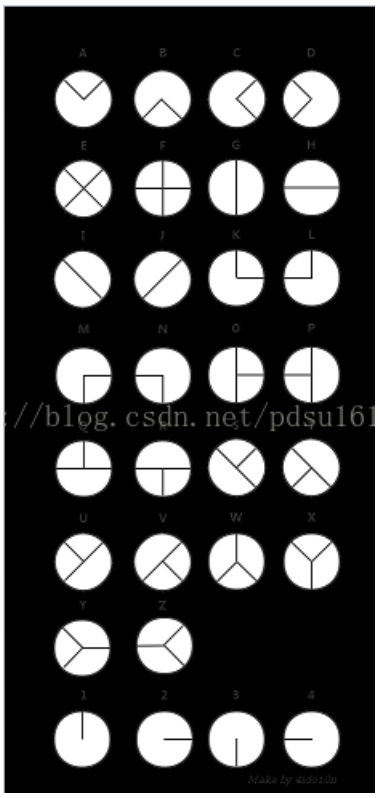
常见的排布方式：

	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

加密实例：
明文：THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG
密文：442315 4145241325 1242345233 213453 2445323543 442315 31115554 143422

14.夏多密码（曲折加密）

夏多密码是作者麦克斯韦·格兰特在中篇小说《死亡之链》塑造夏多这一英雄人物中所自创的密码，如下图所示：



15.普莱菲尔密码

普莱菲尔密码(Playfair Cipher)是第一种用于实际的双字替换密码，用双字加密取代了简单代换密码的单字加密

可以分为三个步骤，即编制密码表、整理明文、编写译文

一个示例加密:

```
明文：wearediscoveredsaveyourselfx
密文：ugrmkcsxhmufmkbtoxgcmvatluiv
```

上例子详情&在线加密解密

16.维吉尼亚密码

维吉尼亚密码(Vigenère Cipher)是在单一恺撒密码的基础上扩展出多表代换密码，根据密钥(当密钥长度小于明文长度时可以循环使用)来决定用哪一行的密表来进行替换，以此来对抗字频统计。

在线加密解密

变种：格罗斯费尔德密码（用数字代替字母）

17.自动密钥密码

自动密钥密码(Autokey Cipher)是多表替换密码，与维吉尼亚密码密切相关，但使用不同的方法生成密钥，通常来说要比维吉尼亚密码更安全。自动密钥密码主要有两种，关键词自动密钥密码和原文自动密钥密码.下面我们以关键词自动密钥为例：
明文：THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG
关键词：CULTURE
自动生成密钥：CULTURE THE QUICK BROWN FOX JUMPS OVER THE
接下来的加密过程和维吉尼亚密码类似，从密表可得：
密文：VBP JOZGD IVEQV HYY AIICX CSNL FWW ZVDP WVK
自动密钥密码在线加密

18.博福特密码

博福特密码(Beaufort Cipher)，是一种类似于维吉尼亚密码的代换密码，由弗朗西斯·蒲福(Francis Beaufort)发明。它最知名的应用是Hagelin M-209密码机。博福特密码属于对等加密，即加密演算法与解密演算法相同。
明文：THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG
密钥(循环使用，密钥越长相对破解难度越大)：CULTURE
加密过程：如果第一行为明文字母，第一列为密文字母，那么沿明文字母'T'列出现密钥字母'C'的行号就是密文字母'J'，以此类推。
密文：JNH DAJCS TUFYE ZOX CZICM OZHC BKA RUMV RDY
Beaufort Cipher在线加密解密

19.滚动密钥密码

滚动密钥密码(Running Key Cipher)和维吉尼亚密码有着相同的加密机制，区别是密钥的选取，维吉尼亚使用的密钥简短，而且重复循环使用，与之相反，滚动密钥密码使用很长的密钥，比如引用一本书作为密钥。这样做的目的是不重复循环使用密钥，使密文更难破译，尽管如此，滚动密钥密码还是可以被攻破，因为有关于密钥和明文的统计分析模式可供利用，如果滚动密钥密码使用统计上的随机密钥来源，那么理论上是不可破译的，因为任何可能都可以成为密钥，并且所有的可能性都是相等的。
明文：THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG
密钥：选取C语言编程(1978版)第63页第1行"errors can occur in several places. A label has…"，去掉非字母部分作为密钥(实际选取的密钥很长，长度至少不小于明文长度)。
加密过程：加密过程和维吉尼亚密码加密过程相同
密文:XYV ELAEK OFQYH WWK BYHTJ OGTC TJI DAK YESR
已知密钥在线加解密

20.Porta密码

Porta密码(Porta Cipher)是一个由意大利那不勒斯的医生Giovanni Battista della Porta发明的多表代换密码，Porta密码具有加密解密过程的是相同的特点。
密表：

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

明文：THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG
密钥(循环使用，密钥越长相对破解难度越大)：CULTURE
加密过程：明文字母'T'列与密钥字母'C'行交点就是密文字母'F',以此类推。
密文：FRW HKQRY YMFMF UAA OLWHD ALWI JPT ZXHC NGV
Porta Cipher在线加密解密

21.同音替换密码

同音替换密码(Homophonic Substitution Cipher)是单字母可以被其他几种密文字母同时替换的密码，通常要比标准替换密码破解更加困难，破解标准替换密码最简单的方法就是分析字母出现频率，通常在英语中字母'E'(或'T')出现的频率是最高的，如果我们允许字母'E'可以同时被3种不同字符代替，那么就不能还是以普通字母的频率来分析破解，如果允许可代替字符越多，那么密文就会更难破译。

常见代换规则表：

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
D	X	S	F	Z	E	H	C	V	I	T	P	G	A	Q	L	K	J	R	U	O	W	M	Y	B	N
9			7				3					5	0				4	6							
			2																						
			1																						

明文:THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG
密文(其中一种)：6CZ KOVST XJ0MA EQY IOGL4 0W1J UC7 P9NB F0H

22.仿射密码

仿射密码(Affine Cipher)是一种单表代换密码，字母表中的每个字母相应的值使用一个简单的数学函数映射到对应的数值，再把对应数值转换成字母。这个公式意味着每个字母加密都会返回一个相同的字母，意义着这种加密方式本质上是一种标准替代密码。

仿射密码在线加密解密

23.ADFGX和ADFGVX密码

ADFGX密码(ADFGX Cipher)是结合了改良过的Polybius方格替代密码与单行换位密码的矩阵加密密码，使用了5个合理的密文字母：A，D，F，G，X，这些字母之所以这样选择是因为当转译成摩尔斯电码(ADFGX密码是德国军队在一战发明使用的密码)不易混淆，目的是尽可能减少转译过程的操作错误。

ADFGVX密码实际上就是ADFGX密码的扩充升级版，一样具有ADFGX密码相同的特点，加密过程也类似，不同的是密文字母增加了V，使得可以再使用10数字来替换明文。

如：attack（keysquare=phqgmeaynofdxkrcvszwbutil）（keyword=german）- XFDDDDFAFGXG

ADFGX Cipher在线加解密

24.双密码

双密码(Bifid Cipher)结合了波利比奥斯方阵换位密码，并采用分级实现扩散，这里的"双"是指用2个密钥进行加密。双密码是由法国Felix Delastelle发明，除此之外Felix Delastelle还发明了三**分密码**(Trifid Cipher)，四方密码(Four-Square Cipher)。还有一个**两方密码**(Two-Square)与四方密码类似，**共轭矩阵双密码**(Conjugated Matrix Bifid Cipher)也是双密码的变种。

25.棋盘密码/跨棋盘密码

棋盘密码（Checkerboard Cipher)是使用一个波利比奥斯方阵和两个密钥作为密阵的替换密码，通常在波利比奥斯方阵中J字母往往被包含在I字母中。

跨棋盘密码(Straddle Checkerboard Cipher)是一种替换密码，当这种密码在结合其他加密方式，加密效果会更好。在线加密解密

26.分组摩尔斯替换密码

分组摩尔斯替换密码(Fractionated Morse Cipher)首先把明文转换为莫尔斯电码，不过每个字母之间用x分开，每个单词用xx分开。然后使用密钥生成一个替换密表，这个密表包含所有. - x组合的情况(因为不会出现xxx的情况，所以一共26种组合)。

27.Bazeries密码

Bazeries密码(Bazeries Cipher)是换位密码和替换密码的组合，使用两个波利比奥斯方阵，一个明文字母方阵，使用一个随机的数字(一般小于1000000)的生成一个密钥矩阵同时作为第一轮明文划分分组，比如2333这个数字翻译为英文便是TWO THOUSAND THREE HUNDRED THIRTY THREE,从第一个字母T开始选取不重复的字母，之后再从字母表中按序选取没有出现的字母组成密钥矩阵。

28.Digrafid密码

Digrafid密码(Digrafid Cipher)使用两个密钥生成分别生成类似波利比奥斯方阵的3×9方格的密表。

29.比尔密码

比尔密码起源于1885年出版的一本23页小册子《The Beale Papers》，作者真实身份不详，通过代理人J·B·沃德（J.B.Ward）出版了小册子。小册子包含了三份密码及关于密码的故事。详情见链接。

30.键盘密码

一般用到的键盘密码就是手机键盘和电脑键盘两种，2014 0ctf比赛里Crypto类型中Classic一题就是电脑键盘密码，详细可以参考，另外给出另外一些参考情况。

31.盲文

其他有趣的机械密码

1.恩尼格码密码

恩尼格玛密码机（德语：Enigma，又译哑谜机，或“谜”式密码机）是一种用于加密与解密文件的密码机。确切地说，恩尼格玛是对二战时期纳粹德国使用的一系列相似的转子机械加解密机器的统称，它包括了许多不同的型号，为密码学对称加密算法的流加密。

在线模拟传送门

代码混淆加密：

1.asp混淆加密

ASP代码修复工具

2.php混淆加密

PHP混淆类在线破解

3.css/js混淆加密

CSS, JavaScript 压缩, 美化, 加密, 解密

4.VBScript.Encode混淆加密

ASP/VBScript/JScript.Encode 在线解密

5.ppencode

ppencode-Perl把Perl代码转换成只有英文字母的字符串。

如：print"the"加密后为：

#!/usr/bin/perl -w
length q bless glob and print chr ord q open do and print chr ord q qr eq and print chr ord q sin s and print chr ord qw q ne q and print chr ord q gt log and print chr hex length q q not eval getsockname q and print chr ord q lt eval and print chr ord q chr lc and print chr ord q ge log and print chr length q q ge getc getpriority printf split q

ppencode - JavaScript demo

6.rrencode

rrencode可以把ruby代码全部转换成符号。

```
hello,world!

($,|$$&&@@_=$@);$><<($,&$,||(%!%!<<(?!+?!+?!))%(?|-?<+(?]-?=+?/-?')))+($,|$$&&(%!%!<<(?!+?!+?!))%(?}-?=+(?_
```

7.jjencode/aaencode

jjencode和aaencode都是Yosuke HASEGAWA的作品，前者将JS代码转换成只有符号的字符串，类似于rrencode，介绍的PPT见http://utf-8.jp/public/20090710/jjencode.pps。

后者更好玩，可以将JS代码转换成常用的网络表情，例如“(ﾟΘﾟ)”。

aaencode demo

8.JSfuck

JSFuck 可以让你只用 6 个字符[ ]( ) ! +来编写 JavaScript 程序。

JSFuck加密

9.jother

jother是一种运用于javascript语言中利用少量字符构造精简的匿名函数方法对于字符串进行的编码方式。其中8个少量字符包括：！ + （ ） [ ] { }。只用这些字符就能完成对任意字符串的编码。

Ｊother编码工具

10.brainfuck编程语言

Brainfuck是一种极小化的计算机语言，按照"Turing complete（完整图灵机）"思想设计的语言，它的主要设计思路是：用最小的概念实现一种“简单”的语言，BrainF**k 语言只有八种符号，所有的操作都由这八种符号(> < + - . , [ ])的组合来完成。

如：hello!

密文为：

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

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

----- --<]> ----- ----- .<
```

其他

分类：可逆/不可逆加密、对称性、非对称性

↑上图链接

1.SHA 1/224/256/384/512

安全散列算法（英语：Secure Hash Algorithm）是一种能计算出一个数字消息所对应到的，长度固定的字符串（又称消息摘要）的算法。且若输入的消息不同，它们对应到不同字符串的机率很高；而SHA是FIPS所认证的五种安全散列算法。这些算法之所以称作“安全”是基于以下两点（根据官方标准的描述）：

1. 由消息摘要反推原输入消息，从计算理论上来说是很困难的。
2. 想要找到两组不同的消息对应到相同的消息摘要，从计算理论上来说也是很困难的。任何对输入消息的变动，都有很高的机率导致其产生的消息摘要迥异。

SHA家族的五个算法，分别是SHA-1、SHA-224、SHA-256、SHA-384，和SHA-512

如：the（SHA-1加密）- bbccdf2efb33b52e6c9d0a14dd70b2d415fbea6e

2.MD5加密

MD5是英文 Message-Digest Algorithm 5 的缩写，中文意思就是“消息摘要算法第五版”。MD5能够生成数据或文件的“数字指纹”，就像每个人都有自己独一无二的指纹一样，MD5生成的这个“数字指纹”也是独一无二的，可以用来验证数据或文件的一致性。

如：the（32位MD5加密）- 8fc42c6ddf9966db3b09e84365034357

3.Adler-32校验

Adler-32是Mark Adler在1995年提出的一种校验算法，该算法通过求解两个16位的数值A、B实现，并将结果连结成一个32位整数。Adler-32算法和32位CRC算法相比具有更快的执行效率，但这两者的安全性都不高。Adler-32的可靠性介于fletcher-16和fletcher-32之间，在输入较短的消息时Adler-32变得很不可靠。

如：the - 02940142

4.CRC校验

循环冗余校验（英语：Cyclic redundancy check，通称“CRC”）算法由W. Wesley Peterson于1961年发表。CRC是一种根据网络数据包或电脑文件等数据产生简短固定位数校验码的一种散列算法，主要用来检测或校验数据传输或者保存后可能出现的错误。生成的数字在传输或者存储之前计算出来并且附加到数据后面，然后接收方进行检验确定数据是否发生变化。一般来说，循环冗余校验的值都是32位的整数。由于CRC算法易于用二进制的电脑硬件使用、容易进行数学分析并且尤其善于检测传输通道干扰引起的错误，因此获得广泛应用。

如：the（CRC-32-b加密）- 3c456de6

5.Gost加密

Gost（Gosudarstvennyi Standard）算法是由前苏联设计的类似DES算法的分组密码算法。它是一个64位分组及256位密钥的采用32轮简单迭代型加密算法。DES算法中采用的是56位长密钥，在密码科学中，一个对称密码系统安全性是由算法的强度和密钥长度决定的，在确保算法足够强（攻击密码系统的唯一方法就是采用穷举法试探所有可能的密钥）的前提下，密钥的长度直接决定着穷举攻击的复杂度。

如：the - d65b89fae511120220ee04da94b4447fbeaef4e23ec17ed43b0e6018ae1f8abe

6.HAVAL加密算法

HAVAL加密算法是由Yuliang Zheng、Josef Pieprzyk和Jennifer Seberry在1992提出。

HAVAL加密算法可以产生不同长度的散列值，包括128位、160位、192位、224位、256位。并且可以指定生成散列计算的轮数（3、4或5）。128位3轮计算的HAVAL密钥已被证实是不安全的。

如：the（HAVAL-160-3加密）- eddf481174b32be373754bc96af3964c136f7ba3

7.RIPEMD算法

RIPEMD（RACE Integrity Primitives Evaluation Message Digest），中文译为“RACE原始完整性校验消息摘要”，是比利时鲁汶大学COSIC研究小组开发的散列函数算法。RIPEMD使用MD4的设计原理，并针对MD4的算法缺陷进行改进，1996年首次发布RIPEMD-128版本，在性能上与较受欢迎的SHA-1相似。

如：the（RIOEMD-160加密）- 8a2092e3124e0eea32578ce04fcca4e6aab32562

8.Snefru散列算法

Snefru算法，由Ralph Merkle设计，将任意长度的消息散列成128或256位的值。已经证明128位是不安全的，几分钟之内就能找到M'，使H(M')=H(M)。

如：the - 0eadb88909a50c748b1453ad0809caead8c53e6d41c7ab2e4c60dbdf2ba7bc95

9.Tiger散列算法

Tiger是一种散列算法，用于生成数据的密钥。Tiger算法最早在1995年提出，运行在64位平台的192位版本，另外还有截短的128位和160位版本，它们与192位版本的初始化值没有区别，只是作了截短处理，就像是192位版本散列值的前缀。

如：the（Tiger-192-3加密）- ea8e57a5f89fd8dc0d2602c02d0c4e5141f63611cbb19e53

10.Whirlpool算法

Whirlpool是基于分组密码的散列算法，与AES的Rijndael算法非常相似。不过因为Whirlpool的分组长度和密钥均为512比特，所以效率是AES-128算法的一半。

Whirlpool算法具有强大的安全性，被国际标准组织ISO和国际电子技术协会IEC采用作为ISO/IEC 10118-3国际标准。

如：the - d199dc243669863cd2958bd3b013aa3532bef205f200e06b6dff88c692a9ba69948024081057786f29d729c726e

11.DES加密

DES是对称性加密里面常见一种，全称为Data Encryption Standard，即数据加密标准，是一种使用密钥加密的块算法。密钥长度是64位(bit)，超过位数密钥被忽略。所谓对称性加密，加密和解密密钥相 同。对称性加密一般会按照固定长度，把待加密字符串分成块。不足一整块或者刚好最后有特殊填充字符。往往跨语言做DES加密解密，经常会出现问题。往往是 填充方式不对、或者编码不一致、或者选择加密解密模式(ECB,CBC,CTR,OFB,CFB,NCFB,NOFB)没有对应上造成。常见的填充模式 有：'pkcs5','pkcs7','iso10126','ansix923','zero' 类型，包括DES-ECB,DES-CBC,DES-CTR,DES-OFB,DES-CFB。

如：the（密码123）- LQGp0SW0g94=

在线DES加密解密

12.AES加密

密码学中的高级加密标准（Advanced Encryption Standard，AES），又称 高级加密标准Rijndael加密法，是美国联邦政府采用的一种区块加密标准。这个标准用来替代原先的DES，已经被多方分析且广为全世界所使用。经过五 年的甄选流程，高级加密标准由美国国家标准与技术研究院 （NIST）于2001年11月26日发布于FIPS PUB 197，并在2002年5月26日成为有效的标准。2006年，高级加密标准已然成为对称密钥加密中最流行的算法之一。

如：the（密码123）- PBwuqDh+j0yPGvA8+dS8AQ==

在线AES加密解密

13.TripleDES

3DES（又叫Triple DES）是三重数据加密算法（TDEA，Triple Data Encryption Algorithm）块密码的通称。它相当于是对每个数据块应用三次DES加密算法。密钥长度是128位，192位(bit)，如果密码位数少于等于64 位，加密结果与DES相同。原版DES容易被破解，新的3DES出现，增加了加密安全性,避免被暴力破解。它同样是对称性加密，同样涉及到加密编码方式， 及填充方式。包括3DES-ECB,3DES-CBC,3DES-CTR,3DES-OFB,3DES-CFB

如：the（密码123）-LQGp0SW0g94=

在线3DES加密解密

14.RC4/5/6

RC4加密算法是RSA三人组中的头号人物Ron Rivest在1987年设计的密钥长度可变的流加密算法簇。该算法的速度可以达到DES加密的10倍左右，且具有很高级别的非线性。1994年9月，它 的算法被发布在互联网上。由于RC4算法加密是采用的xor，所以，一旦子密钥序列出现了重复，密文就有可能被破解。RC4作为一种老旧的验证和加密算法 易于受到黑客攻击，现在逐渐不推荐使用了。

如：the（密码123）- J5ja

在线RC4加密解密

15.RSA加密

RSA公钥加密算法是1977年由Ron Rivest、Adi Shamirh和LenAdleman在（美国麻省理工学院）开发的。RSA取名来自开发他们三者的名字。RSA是目前最有影响力的公钥加密算法，它能够抵抗到目前为止已知的所有密码攻击，已被ISO推荐为公钥数据加密标准。

RSA算法基于一个十分简单的数论事实：将两个大素数相乘十分容易，但那时想要对其乘积进行因式分解却极其困难，因此可以将乘积公开作为加密密钥。RSA算法是第一个能同时用于加密和数字签名的算法，也易于理解和操作。

RSA算法是一种非对称密码算法，所谓非对称，就是指该算法需要一对密钥，使用其中一个加密，则需要用另一个才能解密。

RSA的算法涉及三个参数，n、e1、e2。

其中，n是两个大质数p、**q的积，n的二进制表示时所占用的位数，就是所谓的密钥长度。**

e1和e2是一对相关的值，e1可以任意取，但要求e1与(p-1)*(q-1)互质；再选择e2，要求(e2*e1)mod((p-1)*(q-1))=1。

(n及e1),(n及e2)就是密钥对。

RSA加解密的算法完全相同,设A为明文，B为密文，则：A=B^e1 mod n；B=A^e2 mod n；

e1和e2可以互换使用，即：

A=B^e2 mod n；B=A^e1 mod n;

在线RSA加密解密,RSA2加密解密

一些别的网站

13种最为荒谬的编程语言

33iq上一个牛逼博主