

CTF_Crypto

原创

[ybzzz](#) 于 2020-02-26 16:21:31 发布 539 收藏 1

分类专栏: [CTF 密码学](#)

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/ybzzz/article/details/104517578>

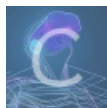
版权



[CTF](#) 同时被 2 个专栏收录

4 篇文章 0 订阅

订阅专栏



[密码学](#)

3 篇文章 1 订阅

订阅专栏

Base64

[Base64在线互译](#)

线索: 结尾 =

应用范围

- base64是一种以64个可见字符集对二进制数据进行编码的编码算法
- 常用于网络数据传输过程的编解码环节, HTTP环境下传递较长的标识信息

编码表

十进制数值	编码字符	十进制数值	编码字符	十进制数值	编码字符	十进制数值	编码字符
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	,

编码过程

base64编码，每3个8位明文数据为一组，取这3个字数据的ASCII码，然后以6位为一组组成4个新的数据。对于不足3字节的处理：

1. 不足三字节后面填充0；
2. 对于编码前的数据产生的6位，如果为0，则索引到的字符为'A'；因不足6位而填充的0，用 '=' 来替代，有点结束符的意思

原字符	A	B	C	D		
hex	0x41	0x42	0x43	0x44		
bin	0 1 0 0 0 0 0 0	0 1 0 0 0 0 1 0 0 0	1 0 0 0 0 0 1 1 0 1	0 1 0 0 0 1 0 0	0 0 0 0 0 0	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
base64值	16	20	9	3	17	0 0 0
base64字符	Q	U	J	D	R	A = =

凯撒密码

凯撒密码在线互译

线索：和解密后的密文格式很像

- 一种替换加密的技术，明文中的所有字母都在字母表上向后（或向前）按照一个固定数目进行偏移后被替换成密文

摩尔斯电码

摩尔斯电码在线互译

- 可用空格或单斜杠/来分隔摩斯电码，但只可用一种，不可混用
- 用 - 替换1表示长音，. 替换0表示短音

编码表

字母

字符	电码符号	字符	电码符号	字符	电码符号	字符	电码符号
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	- - . . .				

数字长码

字符	电码符号	字符	电码符号	字符	电码符号	字符	电码符号
0	- - - - -	1	. - - - -	2	. . - - -	3	. . . - -
4 -	5	6	-	7	- - . . .
8	- - - . .	9	- - - - .				

标点符号

字符	电码符号	字符	电码符号	字符	电码符号	字符	电码符号
.	. - . - . -	:	- - - . . .	,	- - . . - -	;	- . - . - .
?	. . - - . .	=	- . . . -	'	. - - - - .	/	-
!	- . - . - -	-	- -	_	. . - - - .	"	. -
(- . - - . .)	- . - - - -	\$. . . - . . -	&
@	. - - . - .	+	. - . - .				

ASCII

[ASCII在线互译](#)

培根密码

[培根密码在线互译](#)

培根密码本质上是將二进制信息通过样式的区别，加在了正常书写之上，实际上就是一种替换密码

编码表

第一种方式

A	aaaaa	H	aabbb	O	abbba	V	babab
B	aaaab	I	abaaa	P	abbbb	W	babba
C	aaaba	J	abaab	Q	baaaa	X	babbb
D	aaabb	K	ababa	R	baaab	Y	bbaaa
E	aabaa	L	ababb	S	baaba	Z	bbaab
F	aabab	M	abbaa	T	baabb		
G	aabba	N	abbab	U	babaa		

第二种方式

a	AAAAA	g	AABBA	n	ABBAA	t	BAABA
b	AAAAB	h	AABBB	o	ABBAB	u-v	BAABB
c	AAABA	i-j	ABAAA	p	ABBBA	w	BABAA
d	AAABB	k	ABAAB	q	ABBBB	x	BABAB
e	AABAA	l	ABABA	r	BAAAA	y	BABBA
f	AABAB	m	ABABB	s	BAAAB	z	BABBB

幂数加密

任意的十进制数都可以用 **2的幂次和** 的形式表示出来

云影密码 (01248)

编码过程

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，例如 **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

维吉尼亚密码

加密方法

加密公式： $C = (P + K) \% 26$

C: 密文

P: 原文

K: 第几套加密方式

一个密钥字母代表一套加密方式，比如：**a**代表第**1**套加密方式，**b**代表第**2**套加密方式，一共**25**套

这样密钥和原文每个字符一一对应，如果密钥长度不足，那么循环替代