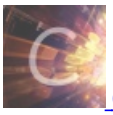
Crypto-移位编码

原创

Qwzf 于 2019-07-16 17:56:46 发布 719 收藏

分类专栏： CTF 文章标签： CTF

本文链接：https://blog.csdn.net/qq_43625917/article/details/96160862


Crypto 同时被 3 个专栏收录

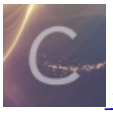
5 篇文章 0 订阅

订阅专栏


CTF

30 篇文章 6 订阅

订阅专栏


移位编码

1 篇文章 0 订阅

订阅专栏

Crypto-移位编码

前言

学习了解了一下简单的**移位编码**，于是做题总结了一下

Crypto1：困在栅栏里的凯撒

看到题目，应该和凯撒密码和栅栏密码有关。所以做题之前先了解一下**栅栏密码和凯撒密码**

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”。

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。下面是位移1次的对比：

明文字母表	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
密文字母表	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

将明文字母表向后移动1位，A变成了B，B变成了C……，Z变成了A。同理，若将明文字母表向后移动3位：

明文字母表	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
密文字母表	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

则A变成了D，B变成了E……，Z变成了C。

字母表最多可以移动25位。凯撒密码的明文字母表向后或向前移动都是可以的，通常表述为向后移动，如果要向前移动1位，则等同于向后移动25位，位移选择为25即可。

下面开始做题

”困在栅栏里的凯撒“，应该是先栅栏解密，再凯撒解密。因为直接先凯撒好像没有规律。

想到最后结果开头应该是CTF或flag。所以栅栏解密时，花括号前有三个或四个字母

栅栏密码加密解密

NlEvQd{seft}

每组字数 6 加密 解密

NEQ{etlydsf}

然后再凯撒解密

凯撒密码加密解密

NEQ{etlydsf}

位移 11 加密 解密

CTF{tianshu}

得到flag了。。。。

Crypto2：变异凯撒

变异凯撒　分值：10

来源：实验吧　难度：易　参与人数：11788人　Get Flag：4766人　答题人数：5188人　解题通过率：92%

加密密文：afZ_r9VYfScOeO_UL^RWUc
格式：flag{}

解题链接：

提交

格式是flag{}，与密文的ASCII比较发现

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
1		97	102	90	95	114	57	86	89	102	83	99	79	101	79	95	85	76	94	82	87	85	99	
2	密文	a	f	Z	_	r	9	V	Y	f	S	c	O	e	O	_	U	L	^	R	W	U	c	
3	格式	f	l	a	g	{																	}	
4		102	108	97	103	123	67	97	101	115	97	114	95	118	97	114	105	97	116	105	111	110	125	
5		5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	
6																								
7																								
8		数字是每个字符对应的ascii的十进制数值																						
9		前五个字母是给出规律:黑色数字-浅蓝数字=紫色																						
10		紫色数字是递增的，增值为1												弟弟不会php和python只能用这个表示一下了										
11		后面的红色数字是根据规律用暗红色数字+橙色数字求出的，求出后再对应填出												希望可以解释清楚										
12		相应的字符																						
13		最终结果为																						
14		f[redacted]																						

一步一步比较： flag{Caesar_variation}

这样就得到flag了。。

Crypto3：密文 rot13

密文 rot13　分值：10

来源：2014HCTF　难度：易　参与人数：6747人　Get Flag：2893人　答题人数：3058人　解题通过率：95%

57R9S980RNOS49973S757PQO9S80Q36P （md5不解密）

解题链接：

提交

先了解一下

rot13的相关知识

ROT5、ROT13、ROT18、ROT47 编码是一种简单的码元位置顺序替换暗码。此类编码具有可逆性，可以自我解密，主要用于应对快速浏览，或者是机器的读取，而不让其理解其意。

ROT5 是 rotate by 5 places 的简写，意思是旋转5个位置，其它皆同。下面分别说说它们的编码方式：
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，例如当前为0，编码后变成5，当前为1，编码后变成6，以此类推顺序循环。
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，例如当前为A，编码后变成N，当前为B，编码后变成O，以此类推顺序循环。
ROT18：这是一个异类，本来没有，它是将ROT5和ROT13组合在一起，为了好称呼，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，例如当前为小写字母z，编码后变成大写字母K，当前为数字0，编码后变成符号_。用于ROT47编码的字符其ASCII值范围是33－126，具体可参考ASCII编码。

于是rot13解码，得到最终结果

感悟

总结又使我收获好多，题比较基础，不过可以借此了解一下移位编码的基础知识。继续努力！！！

小白进阶ing。。。。。。。。。