实验吧——密码学更新

原创

置顶 落花四月 于 2018-03-24 07:53:16 发布 2189 收藏 1
分类专栏： 密码学 文章标签： m'm'm'm'm'm'

本文链接：https://blog.csdn.net/qq_41187256/article/details/79673722

本篇文章包括四篇关于密码学方面的知识，并且都是实验吧的题目解析，以后我每天都会持续更新博客内容，请各位细心查看！

1：传统知识 + 古典密码

2:围在栅栏里的凯撒

3：古典密码

4：奇怪的短信

解题思路：看见这一题有年份，可以想到使用天干地支年份顺序表，

会得到相应的数字，信的背面有一个甲子（+60）；古典密码中有两个

一个是栅栏密码，一个是凯撒密码，慢慢试一下就可以得到答案！

1：先找到天干地支年份顺序表

六十年甲子（干支表）

1	2	3	4	5	6	7	8	9	10
甲子	乙丑	丙寅	丁卯	戊辰	己巳	庚午	辛未	壬申	癸酉
11	12	13	14	15	16	17	18	19	20
甲戌	乙亥	丙子	丁丑	戊寅	己卯	庚辰	辛己	壬午	癸未
21	22	23	24	25	26	27	28	29	30
甲申	乙酉	丙戌	丁亥	戊子	己丑	庚寅	辛卯	壬辰	癸巳
31	32	33	34	35	36	37	38	39	40
甲午	乙未	丙申	丁酉	戊戌	己亥	庚子	辛丑	壬寅	癸丑
41	42	43	44	45	46	47	48	49	50
甲辰	乙巳	丙午	丁未	戊申	己酉	庚戌	辛亥	壬子	癸丑
51	52	53	54	55	56	57	58	59	60
甲寅	乙卯	丙辰	丁巳	戊午	己未	庚申	辛酉	壬戌	癸亥

就可以得到

辛卯：28 + 60 =88

癸巳：30 + 60 =90

丙戌：23 + 60 =83

辛未：8 + 60 =68

庚辰：17 + 60 =77

癸酉：10 + 60 =70

己卯：16 + 60 =76

癸巳：30 + 60 =90

2:会想到ASCII码表转化

65	41	A	
66	42	B	
67	43	C	
68	44	D	
69	45	E	
70	46	F	
71	47	G	
72	48	H	
73	49	I	
74	4A	J	
75	4B	K	
76	4C	L	
77	4D	M	
78	4E	N	
79	4F	O	
80	50	P	

会得到：XZSDMFLZ

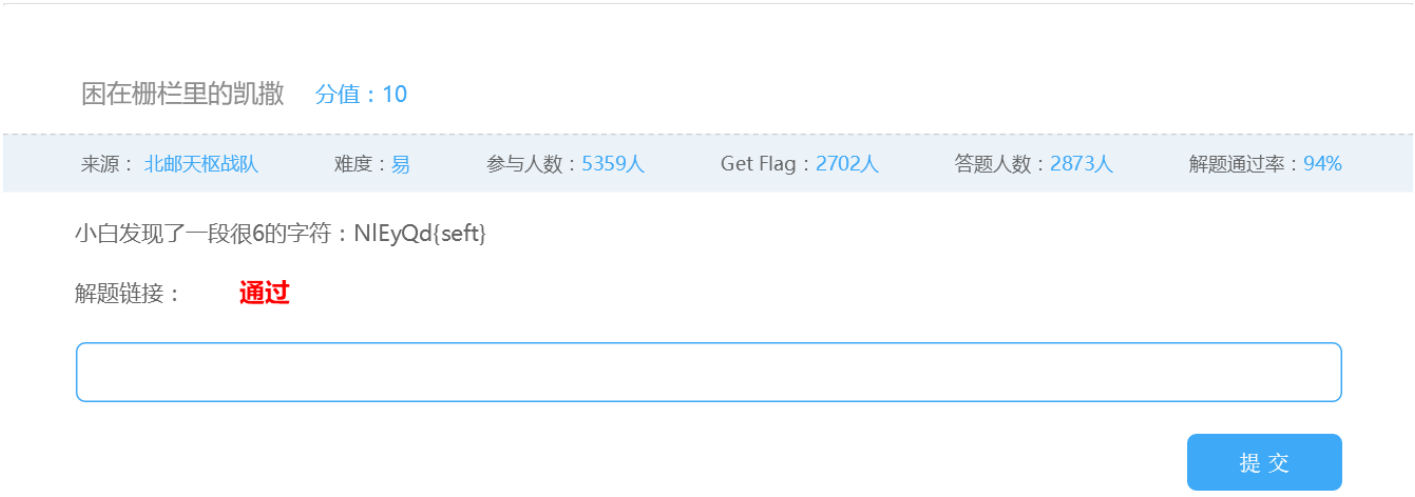
3：接着使用栅栏密码就可以了

4：慢慢试一下使用凯撒密码就可以了：

就可以得到答案可以拼写出来的就是答案:

CTF{SHUANGYU}

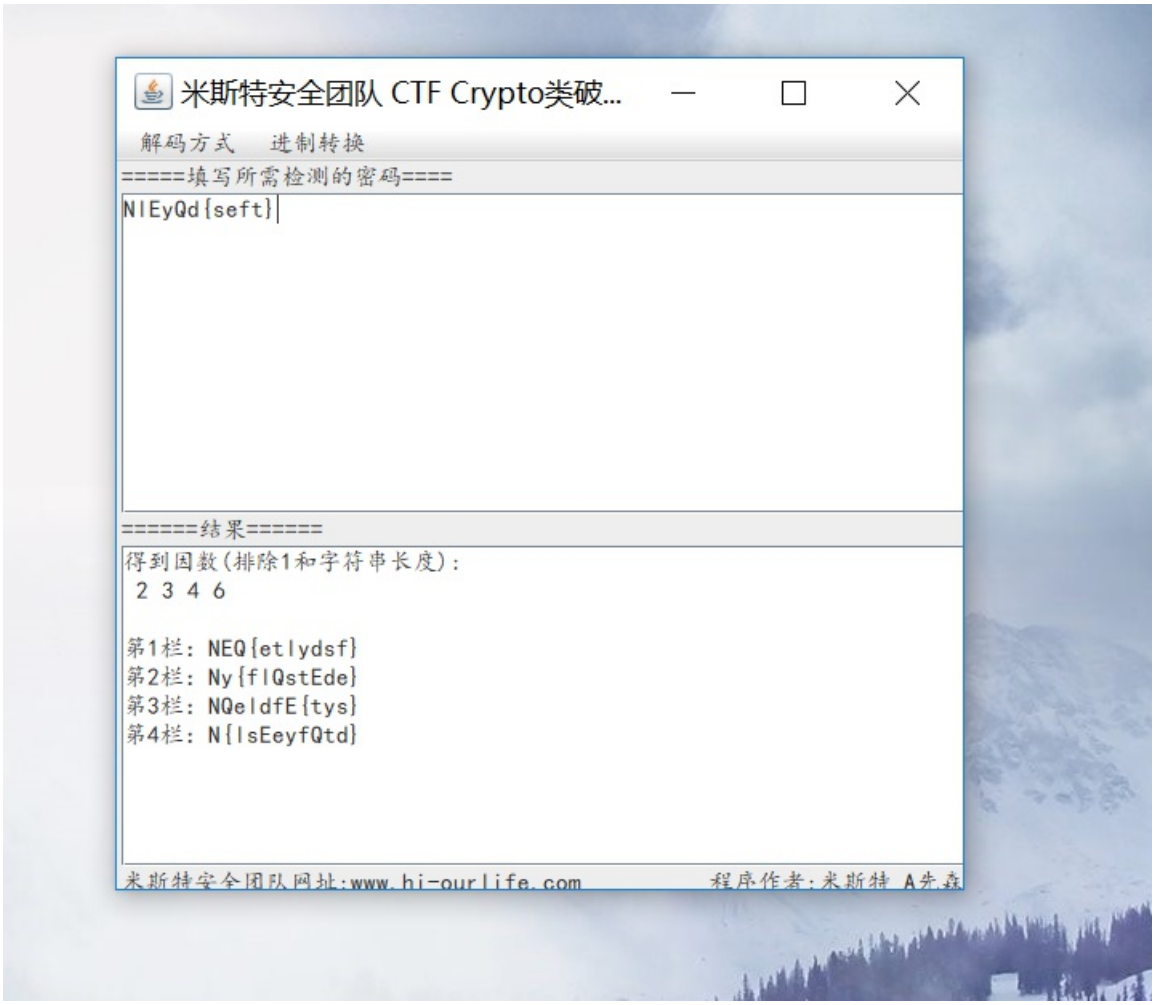
2:



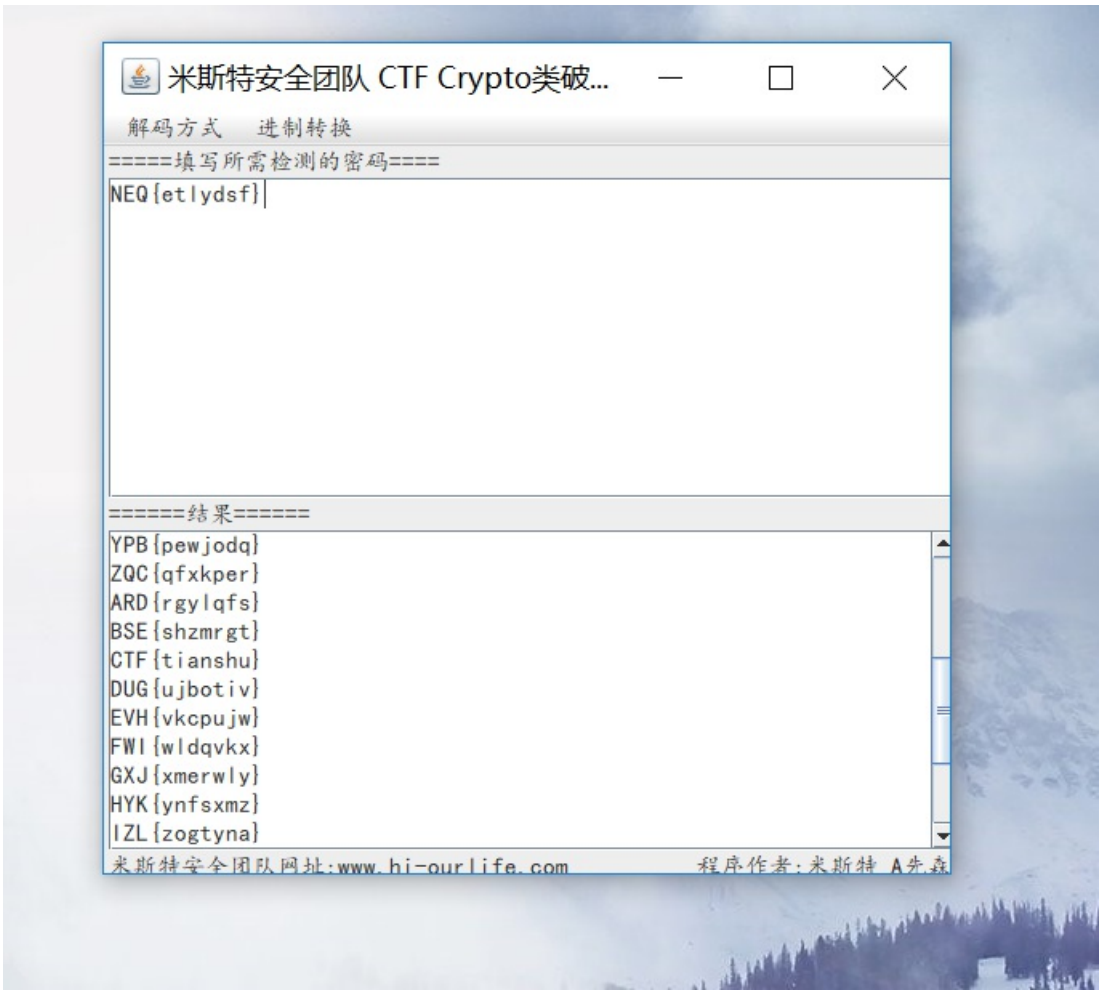
围在栅栏里的凯撒

解题思路：首先使用栅栏密码解密然后凯撒解密

首先使用栅栏解密



然后凯撒解密

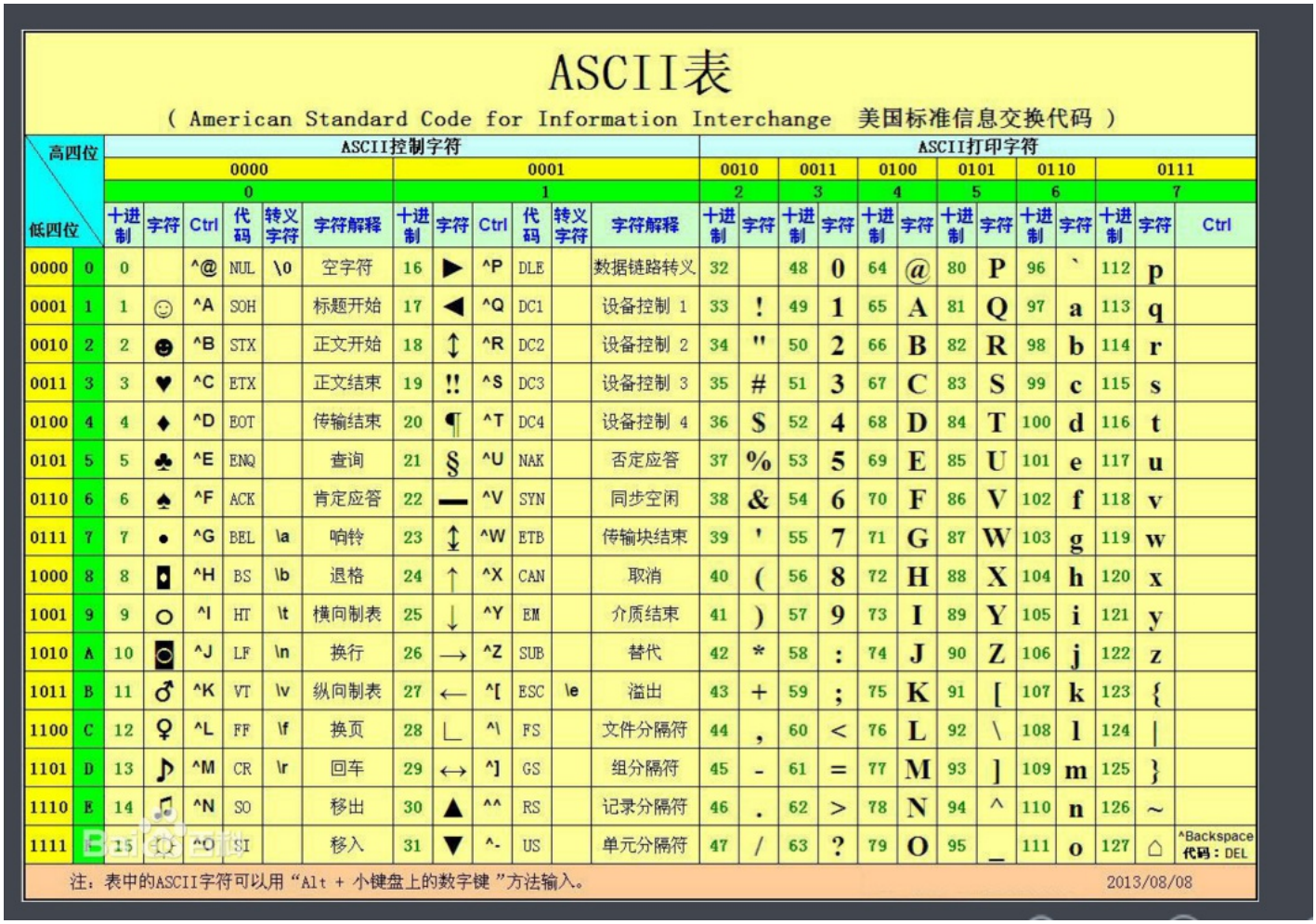


找到有明显表示的，那么答案就是：**CTF{tianshu}**

3：

古典密码：

解题思路：数字肯定是要转化为字母的，需要使用ASCII码表的



ASCII表

(American Standard Code for Information Interchange 美国标准信息交换代码)

高四位 / 低四位		ASCII控制字符											ASCII打印字符												
		0000						0001					0010		0011		0100		0101		0110		0111		
		0						1					2		3		4		5		6		7		
		十进制	字符	Ctrl	代码	转义字符	字符解释	十进制	字符	Ctrl	代码	转义字符	字符解释	十进制	字符	十进制	字符	十进制	字符	十进制	字符	十进制	字符	十进制	字符	Ctrl
0000	0	0		^@	NUL	\0	空字符	16	▶	^P	DLE		数据链路转义	32		48	0	64	@	80	P	96	`	112	p	
0001	1	1	☺	^A	SOH		标题开始	17	◀	^Q	DC1		设备控制 1	33	!	49	1	65	A	81	Q	97	a	113	q	
0010	2	2	☻	^B	STX		正文开始	18	↕	^R	DC2		设备控制 2	34	"	50	2	66	B	82	R	98	b	114	r	
0011	3	3	♥	^C	ETX		正文结束	19	‼	^S	DC3		设备控制 3	35	#	51	3	67	C	83	S	99	c	115	s	
0100	4	4	♦	^D	EOT		传输结束	20	¶	^T	DC4		设备控制 4	36	$	52	4	68	D	84	T	100	d	116	t	
0101	5	5	♣	^E	ENQ		查询	21	§	^U	NAK		否定应答	37	%	53	5	69	E	85	U	101	e	117	u	
0110	6	6	♠	^F	ACK		肯定应答	22	▬	^V	SYN		同步空闲	38	&	54	6	70	F	86	V	102	f	118	v	
0111	7	7	•	^G	BEL	\a	响铃	23	↨	^W	ETB		传输块结束	39	'	55	7	71	G	87	W	103	g	119	w	
1000	8	8	◘	^H	BS	\b	退格	24	↑	^X	CAN		取消	40	(	56	8	72	H	88	X	104	h	120	x	
1001	9	9	○	^I	HT	\t	横向制表	25	↓	^Y	EM		介质结束	41	)	57	9	73	I	89	Y	105	i	121	y	
1010	A	10	◙	^J	LF	\n	换行	26	→	^Z	SUB		替代	42	*	58	:	74	J	90	Z	106	j	122	z	
1011	B	11	♂	^K	VT	\v	纵向制表	27	←	^[	ESC	\e	溢出	43	+	59	;	75	K	91	[	107	k	123	{	
1100	C	12	♀	^L	FF	\f	换页	28	∟	^\	FS		文件分隔符	44	,	60	<	76	L	92	\	108	l	124	|	
1101	D	13	♪	^M	CR	\r	回车	29	↔	^]	GS		组分隔符	45	-	61	=	77	M	93	]	109	m	125	}	
1110	E	14	♫	^N	SO		移出	30	▲	^^	RS		记录分隔符	46	.	62	>	78	N	94	^	110	n	126	~	
1111	F	15	☼	^O	SI		移入	31	▼	^-	US		单元分隔符	47	/	63	?	79	O	95	_	111	o	127	⌂	^Backspace 代码：DEL

注：表中的ASCII字符可以用“Alt + 小键盘上的数字键”方法输入。 2013/08/08

将Ascii码转换为字母，得到OCU{CFTELXOUYDECTNGAHOHRNFIENM}IOTA
古典密码中最基础的加密法：列置换，加密：将明文按固定长m分组，即每行m个字母，在密钥控制下按某一顺序交换列，最后按列优先的顺序依次读出，即产生了密文。
原来字符串为35位。35=7*5
得到如下结果：
1 234567

OCU{CFT
ELXOUYD
ECTNGAH
OHRNFIE
NM}IOTA

key值的固定结构为CTF{}
故第2列打头或第5列打头，接下来是第7列，然后是第6列，考虑到“{”是第4列，考虑到“}”是最后一列
尝试后得到
1234567列转换为2764513
即为：
2764513

CTF{COU
LDYOUEX
CHANGET
HEINFOR
MATION}

那么答案就是：CTF{COULDYOUEXCHANGETHEINFORMATION}

4：

奇怪的短信：

解题思路：这个属于手机密码。

一般手机密码有一些比较明显的标志：奇数位没有0，偶数位没有5，这样就可以对照手机上面的键盘得到答案；

33 5321 41 43 74 74 43 61 71 53 32拆分出这样就可以了，对照下面的表格

得到答案：CTF{flagissimple}