CTF<密码学> writeup 传统知识+古典密码

转载

weixin_30609331 于 2019-04-30 14:04:00 发布 113 收藏
文章标签： python 密码学
原文链接：http://www.cnblogs.com/Dancing-Fairy/p/10795635.html

小明某一天收到一封密信，信中写了几个不同的年份

辛卯，癸巳，丙戌，辛未，庚辰，癸酉，己卯，癸巳。

信的背面还写有“+甲子”，请解出这段密文。

key值：CTF{XXX}

百度可以查到有关传统知识

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

可以得到年份 list = [28,30,23,8,17,10,16,30]

+甲子，意为加60年，新的list = [88,90,83,68,77,70,76,90]

这些数字相隔不大，很容易联想到ascii码的对应的字符值：

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		0100		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	⌂	^Backspac 代码：DEL

栅栏密码python 代码：

```
list = [28,30,23,8,17,10,16,30]
i=0
while i<len(list):
    list[i]+=60
    i+=1
s=""
i=0
while i<len(list):
    s+=chr(list[i])
    i+=1
print s
#s='abcdefgh'
fac = [x for x in range(1,len(s))]
i=1
print fac
for j in range(len(fac)):
    str1=''
    for i in range(fac[j]):
        k=0
        while i+k<len(s):
            str1+=s[i+k]
            k+=fac[j]
    print str1
```

进行一轮栅栏算法解密得到的结果：

XZSDMFLZ

XSMLZDFZ

XDLZMZSF

XMZFSLDZ

XFZLSZDM

XLZZSDMF

XZZSDMFL

发现没有什么特别规律，然后对每一个进行凯撒解密，python代码如下：

```
i=0
s=input("Input the string:")
s.upper()
for j in range(25):
    str1=''
    for i in range(len(s)):
        str1+=chr((ord(s[i])-64+j)%26+64)
    print str1
```

当试到第4个字符串时：

XM@FSLD@

YNAGTMEA

@OBHUNFB

APCIVOGC

BQDJWPHD

CREKXQIE

DSFLYRJF

ETGM@SKG

FUHNATLH

GVIOBUMI

HWJPCVNJ

IXKQDWOK

JYLREXPL

K@MSFYQM

LANTG@RN

MBOUHASO

NCPVIBTP

ODQWJCUQ

PERXKDVR

QFSYLEWS

RGT@MFXT

SHUANGYU

TIVBOH@V

UJWCPIAW

VKXDQJBX

flag就是SHUANGYU

转载于:https://www.cnblogs.com/Dancing-Fairy/p/10795635.html