

CTF-变异凯撒

原创

[RyanWang0000](#)



于 2019-10-21 10:48:56 发布



277



收藏

分类专栏: [CTF-crypt](#) 文章标签: [CTF vrypt](#)

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/qq_32350719/article/details/102630423

版权



[CTF-crypt](#) 专栏收录该内容

3 篇文章 0 订阅

订阅专栏

题目来源: buuCTF-crypto-变异凯撒



先用常规的凯撒密码试试看

<https://planetcalc.com/1434/>

这个网址很方便, 可以一次凯撒密码的26种情况一次性列举出来, 比较方便

Transformation	
Transformation	Transformed text
ROT0	afZ_r9VYfScOeO_UL^RWUc
ROT1	bgA_s9WZgTdPfP_VM^SXVd
ROT2	chB_t9XAhUeQgQ_WN^TYWe
ROT3	diC_u9YBiVfRhR_XO^UZxf
ROT4	ejD_v9ZCjWgSiS_YP^VAYg
ROT5	fkE_w9ADkXhTjT_ZQ^WBZh
ROT6	glF_x9BEIYiUkU_AR^XCAi
ROT7	hmG_y9CFmZjVIV_BS^YDBj
ROT8	inH_z9DGnAkWmW_CT^ZEck
ROT9	jol_a9EHoBIXnX_DU^AFDI

https://blog.csdn.net/qq_32350719

没有找到有用的信息

联想到题目的名字, 变异凯撒, 正常手段行不通

应该会对移位的位数这里下绊子

找一张ascii表看一下

十进制	二进制	符号	十进制	二进制	符号	十进制	二进制	符号	十进制	二进制	符号
0	0000 0000	NUL	32	0010 0000	[空格]	64	0100 0000	@	96	0110 0000	`
1	0000 0001	SOH	33	0010 0001	!	65	0100 0001	A	97	0110 0001	a
2	0000 0010	STX	34	0010 0010	"	66	0100 0010	B	98	0110 0010	b
3	0000 0011	ETX	35	0010 0011	#	67	0100 0011	C	99	0110 0011	c
4	0000 0100	EOT	36	0010 0100	\$	68	0100 0100	D	100	0110 0100	d
5	0000 0101	ENQ	37	0010 0101	%	69	0100 0101	E	101	0110 0101	e
6	0000 0110	ACK	38	0010 0110	&	70	0100 0110	F	102	0110 0110	f
7	0000 0111	BEL	39	0010 0111	'	71	0100 0111	G	103	0110 0111	g
8	0000 1000	BS	40	0010 1000	(72	0100 1000	H	104	0110 1000	h
9	0000 1001	HT	41	0010 1001)	73	0100 1001	I	105	0110 1001	i
10	0000 1010	LF	42	0010 1010	*	74	0100 1010	J	106	0110 1010	j
11	0000 1011	VT	43	0010 1011	+	75	0100 1011	K	107	0110 1011	k
12	0000 1100	FF	44	0010 1100	,	76	0100 1100	L	108	0110 1100	l
13	0000 1101	CR	45	0010 1101	-	77	0100 1101	M	109	0110 1101	m
14	0000 1110	SO	46	0010 1110	.	78	0100 1110	N	110	0110 1110	n
15	0000 1111	SI	47	0010 1111	/	79	0100 1111	O	111	0110 1111	o
16	0001 0000	DLE	48	0011 0000	0	80	0101 0000	P	112	0111 0000	p
17	0001 0001	DC1	49	0011 0001	1	81	0101 0001	Q	113	0111 0001	q
18	0001 0010	DC2	50	0011 0010	2	82	0101 0010	R	114	0111 0010	r
19	0001 0011	DC3	51	0011 0011	3	83	0101 0011	S	115	0111 0011	s
20	0001 0100	DC4	52	0011 0100	4	84	0101 0100	T	116	0111 0100	t
21	0001 0101	NAK	53	0011 0101	5	85	0101 0101	U	117	0111 0101	u
22	0001 0110	SYN	54	0011 0110	6	86	0101 0110	V	118	0111 0110	v
23	0001 0111	ETB	55	0011 0111	7	87	0101 0111	W	119	0111 0111	w
24	0001 1000	CAN	56	0011 1000	8	88	0101 1000	X	120	0111 1000	x
25	0001 1001	EM	57	0011 1001	9	89	0101 1001	Y	121	0111 1001	y
26	0001 1010	SUB	58	0011 1010	:	90	0101 1010	Z	122	0111 1010	z
27	0001 1011	ESC	59	0011 1011	;	91	0101 1011	[123	0111 1011	{
28	0001 1100	FS	60	0011 1100	<	92	0101 1100	\	124	0111 1100	
29	0001 1101	GS	61	0011 1101	=	93	0101 1101]	125	0111 1101	}
30	0001 1110	RS	62	0011 1110	>	94	0101 1110	^	126	0111 1110	~
31	0001 1111	US	63	0011 1111	?	95	0101 1111	_	127	0111 1111	DEL

结合题目给的提示、

变异凯撒.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助

加密密文: afZ_r9VYfScOeO_UL^

格式: flag{ }

发现从 a 到 f 移动了5位

从 f 到 l 移动了6位

从 Z 到 a 移动了7位

从 _ 到 g 移动了8位

以此类推, 发现了规律

上脚本

```
msg='afZ_r9VYfScOeO_UL^RWUc'
offset=5
flag=""
for i in msg:
    flag+=chr(ord(i)+offset)
    offset+=1
print(flag);
```

运行结果

flag{Caesar_variation}