实验吧CTF密码学Writeup

原创

凌云网络之昂chan 于 2018-08-11 13:52:28 发布 3473 收藏 7
分类专栏： 网络安全 文章标签： CTF 密码学

1、变异凯撒

对照ASCii码，差值递增a-f f-l Z-a _-g

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 0000						ASCII控制字符 0001						ASCII打印字符 0010		ASCII打印字符 0011		ASCII打印字符 0100		ASCII打印字符 0101		ASCII打印字符 0110		ASCII打印字符 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

2、传统知识+古典密码

六十甲子表

辛卯，癸巳，丙戌，辛未，庚辰，癸酉，己卯，癸巳

28+60 30+60 23+60 8+60 17+60 10+60 16+60 30+60

88 90 83 68 77 70 76 90

X Z S D M F L Z

栅栏解密 XMZFSLDZ 凯撒解密 SHUANGYU

3、try them all

加salt MD5解密

MD5解密网站：https://www.somd5.com/

sniper5948 -5948（salt）

4、rsarsa

p,q,e 解出d，n 工具：RSA-Tool 2 by tE!

再用c,d,n解出来 工具：Big Integer Calculator

5、robomunication

考验听力的时候到了，bo po分别代表- .

6、The Flash-14

看钢铁侠14集中有个密码表

其实就是矩阵加密

	1	2	3	4	5
1	A	B	C/K	D	E
2	F	G	H	I	J
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

5443325222445534225152224434222311341 2

YSMWGTZOGVWGTOGHAOB

凯撒解密KEYISFLASHISFASTMAN

7、奇怪的短信

手机键盘加密：

335321414374744361715332

FLAGISSIMPLE

8、RSAROLL

19换位十六进制13 分解质因数N 求出私钥d96849619 工具：RSA-Tool 2 by tE!

用私钥d，密文c，和N解出明文 工具：Big Integer Calculator

9、围在栅栏中的爱

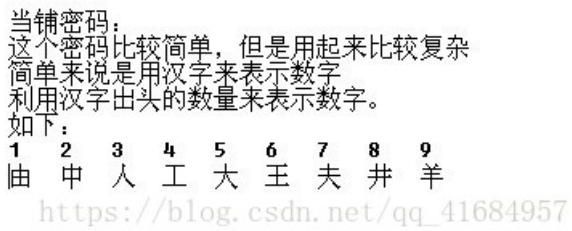
QWE到底等不等于ABC?

电脑键盘加密：电脑键盘上的Q=A，W=B，E=C,R=D.....依次类推

QWERTYUIOPASDFGHJKLZXCVBNM

ABCDEFGHIJKLMNOPQRSTUVWSYZ
-.- .. --.- .-.. .-- - ..-. -.-. --.- --. -. ... --- ---
摩斯解密KIQLWTFCQGNSOO
键盘解密rhasbenvaoylii
倒序　　iilyoavnebsahr
栅栏解密 iloveshiyanbar

10、疑惑的汉字
当铺密码



王夫 井工 夫口 由中人 井中 夫夫 由中大
67 84 70 123 72 77 125
C T F { H M }

11、古典密码
79 67 85 123 67 70 84 69 76 88 79 85 89 68
69 67 84 78 71 65 72 79 72 82 78 70 73 69
78 77 125 73 79 84 65
OCU{CFTELXOYDECTNGAHOHRNFIENM}IOTA
列置换
ctf{cou
ldyouex
changet
heinfor
mation}
CTF{COULDYOUEXCHANGETHEINFORMATION}

12、困在栅栏里的凯撒
NlEyQd{seft}
凯撒解密 CaTnFs{htui}
栅栏加密 ctf{tianshu}

13、奇妙的音乐
用工具Audacity看频谱 粗代表-细代表.
莫斯电码解密

14、Fair-Play

fair-play加密 Decrypt

解密网址：http://rumkin.com/tools/cipher/playfair.php

Alphabet Key: The quickbrown fox jumps over the lazy dog

Your message:ihxo{smzdodcikmodcismzd}

15、我喜欢培根

-- --- .-. ... . ..--.- .. ..--.- -.-. --- --- .-.. ..--.- -... ..- - ..--.- -... .- -.-. --- -. ..--.- .. ..--.- -.-. --- --- .-.. . .-. ..--.- -.. -.-. -.-. -.. -.-. -.-. -.-. -.. -.. -.. -.-. -.. -.-. -.-. -.-. -.. -.. -.-. -.-. -.-. -.-. -.-. -.-. -.-. -.. -.-. -.-. -.-. -.-. -.-. -.-. -.-. -.-. -.-. -.-. / -.-. -.. -.-. -.-. -.-. -.. -.-. -.-. -.. -.-. / -.-. -.-. -.-. -.. -.-. -.-. -.. -.. -.. -.-. -.-. -.. -.. -.. -.-. -.-. -.. -.-. -.. -..

分号分成三段，空格隔开

DCCDCCCDDDCDCCCDDCCCCCCCCCCDDCDCCCCDCCCCC

shiyanba

CDCCCDCCDC

is

CCCDCCDDDCCDDDCCDCDD

cool

培根密码

C换成A，D换成B

16、Decode

0x25346425353425343525333525343325366125343525373725346425353125366625373825346425343425

十六进制转字符

%4d%54%45%35%43%6a%45%77%4d%51%6f%78%4d%44%67%4b%4f%54%6b%4b%4d%54%45%78%4

UTF-8 --

MTE5CjEwMQoxMDgKOTkKMTExCjEwOQoxMDEKMTE2CjExMQoxMTUKMTA0CjEwNQoxMjEKOTcKMTEw

base64

119 w

101 e

108 l

99 c

111 o

109 m

101 e

116 t

111 o

115 s

104 h

105 i

121 y

97 a

110 n

98 b

97 a

114 r

17、RSA实践

p=473398607161，q=4511491，e=17

e转换成十六进制11

解出d=125631357777427553　工具：RSA-Tool 2 by tE!

18、杯酒人生

HTRUZYJW 凯撒解密COMPUTER

维吉尼亚加密 dzarevmgjsdsylmxpddxhvmgns

19、凯撒和某某加密

先凯撒解密再栅栏

对照ASCII码表移位

20、神秘字母

解题思路：看到矩阵想到的是希尔密码加密，将字母变换得{1-26：a-z}

d o u z j u w g n 对应 4 15 21 26 10 21 23 7 14

l g s i l s o a y 12 7 19 9 12 19 15 1 25

求逆矩阵 1 -2

0 1

然后用逆矩阵与密码相乘mod26得：

1 -2 * 4 = -20 mod26 对应 f

0 1 12 12 l

1 -2 * 15 = 1 mod26 对应 a

0 1 7 7 g

明文：flagis hillissoeasy所以simCTF{hillissoeasy }

21、base??

md5值为16478a151bdd41335dcd69b270f6b985

在线解MD5 base64wtfwtf123

22、js

用谷歌浏览器打开查看源码将eval替换为console.log回车出现一个javascript代码将其中的unicode编码转为字符即为结果

23、NSCTF crypto50

U2FsdGVkX1+qtU8KEGmMJwGgKcPUK3XBTdM+KhNRLHSCQL2nSXaW8++yBUkSylRp

AES解密网站：http://tool.oschina.net/encrypt

flag{DlSJV_Hej_UdShofjyed}

凯撒解密 NSCTF_Rot_EnCryption

24、密文 rot13

57R9S980RNOS49973S757PQO9S80Q36P

rot13解密57e9f980eabf49973f757cdb9f80d36c

25、数码管（反过来）

数码管加密原理：https://wenku.baidu.com/view/07f7fd503d1ec5da50e2524de518964bce84d255.html
红+白共阳极1 红 0 白 1
蓝+白共阴极0 蓝 1 白 0

26、他的情书

F12查看源码，不要相信眼睛要相信爱
找到标签为eye的代码console.log出现提示框urldecode，再找到标签为love的代码，将url编码解密得到一个html代码，将其中的js部分放到console控制台解密，得到一个js函数，运行函数，得到"soroki.php?l0vau="等于号后面少个值，推测是pass2，输出pass2的值加到等号后面，转到http://ctf5.shiyanbar.com/crypto/4/soroki.php?l0vau=FoRevEr得到一个base64编码得到in2 say:I love you Forever!The Girl say: zqc{fkqtl_fp_yfd_py}将zqc{fkqtl_fp_yfd_py}凯撒解密得ctf{intwo_is_big_sb}

27、古典密码的不安全性

置换密码可以通过词频统计暴力破解
Os drnuzearyuwn, y jtkjzoztzoes douwlr oj y ilzwex eq lsdexosa kn pwodw tsozj eq ufyoszlbz yrl rlufydlx pozw douwlrzlbz, ydderxosa ze y rlatfyr jnjzli
https://quipqiup.com/在线解密 In cryptography, a substitution cipher is a method of encoding by which units of plaintext are replaced with ciphertext, according to a regular system
mjy gfbmw vla xy wbfnsy symmyew (mjy vrwm qrvvrf), hlbew rd symmyew, mebhsymw rd symmyew, vbomgeyw rd mjy lxrzy, lfk wr dremj. Mjy eyqybzye kyqbhjyew mjy myom xa hyedrevbfn lf bfzyewy wgxwmbmgmbrf. Wr mjy dsln bw f1_2jyf-k3_jg1-vb-vl_l
在线解密为 So the flag is n1_2hen-d3_hu1-mi-ma_a

28、最近在论证一个问题，到底是先有鸡还是先有蛋

ljm,lo 3wsdr4 6tghu7
看电脑键盘被圈住的字母

29、压缩的问题

用winhex把十六进制写进去，用winwar压缩，解压密码为：65H-71H用hashatb查看文件SHA-1值

30、keyboard

提示：和键盘有关
BHUK,LP TGBNHGYT BHUK,LP UYGBN TGBNHGYT BHUK,LP BHUK,LP TGBNHGYT BHUK,LP TGBNHGYT UYGBN
空格隔开的一个个字母，看电脑键盘上的形状

31、这里没有key

f12查看源码，找到奇怪的一段代码<!--
#@~^TgAAAA==[6*liLa6++p'aXvfiLaa6i[[avWi[[a*p[[6*!l'[6cp'aXvXlLa6fp[:6+Wp[:XvWi[[6+XivRlAAA==^#~@ -->
encode解密得到
https://www.jb51.net/tools/onlinetools/jiemi/jsendecode.htm
Encode@decod&#x65
unicode解密得到Encode@decode
解密网站：http://tool.chinaz.com/tools/unicode.aspx