

实验吧密码学writeup

转载

dianzhao6995 于 2017-10-12 19:39:00 发布 240 收藏

文章标签: [密码学 php](#)

原文链接: <http://www.cnblogs.com/Acewipe/p/7631300.html>

版权

传统知识+古典密码 分值: 10

来源: 霜羽

难度: 易

参与人数: 1507人

Get Flag: 443人

答题人数: 602人

解题通过率: 74%

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}

看密信内容知道需要查看天干地支表

干支表

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

找出迷信内容对应的数字+60（一甲子）得到一串数字。对应ASCII码表得到字符串

XZSDMFLZ

不像flag, 在考虑题目中的古典加密, 无非就是凯撒、栅栏等组合加密（一种的得不到密文），爆破之后发现栅栏2栏，再凯撒得到

SHUANGYU

2.The Flash -14

The Flash-14 分值: 10

来源: 山南水北

难度: 易

参与人数: 2670人

Get Flag: 963人

答题人数: 1236人

解题通过率: 78%

这些数字都是什么呢~ 54433252224455342251522244342223113412

答案形式ctf{XXX}

观察密文, 所有数字均不大于5, 猜想可能是5*5矩阵字母表, 百度题目发现闪电侠第二季14集里有个矩阵表

	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

将密文两两为一对得到对应字符串 YSMWGTZOGVWGTOGHAOB

猜想可能还需要凯撒，于是尝试一下

凯撒密码

字符串:

+1	ztnxhuaphw xhuphibpc	+2	auoyivbqix yivqijoqd	+3	bvpzjwerjyz jwrjkdre	+4	cwqakxdszk akxsklesf	+5	dxrblyetla blytlmftg
+6	eyscmzfumb cmzumnguh	+7	fztdnagvnc dnavnohvi	+8	gaueobhwode obwopiwj	+9	hbvfpoixpe fpcxpqjxk	+10	icwgqdyqf gqdyqrkyl
+11	jdshrekzrg hrzrszlzm	+12	keyisflash isfastman	+13	lfzjtgmbtij tgbtunbo	+14	mgakuhncuj kuhcuvocp	+15	nhblviodyk lvidwvdpq
+16	oicmwjpewl mwjwxqer	+17	pjdncqfxm nckfxyrfs	+18	qkeoylr gyno ylgyzsgt	+19	rlfpzmshzo pzmhzathu	+20	smgqantiap qaniabuiv
+21	tnhrboujbq rbojbovjw	+22	uoisepvker sepkedwxx	+23	vpjtdqwdst dqldexly	+24	wqkuerxmet uermefymz	+25	xrlvfsynfu vfnfgzna

发现+12之后就是flag

3.奇怪的短信

奇怪的短信 分值: 10

来源: [Ayn](#) 难度: [易](#) 参与人数: [4715人](#) Get Flag: [2335人](#) 答题人数: [2558人](#) 解题通过率: [91%](#)

收到一条奇怪的短信:
335321414374744361715332
你能帮我解出隐藏的内容嘛?!
格式: CTF{xxx}

经过上一题试试两两拆分得到

33 53 21 41 43 74 74 43 61 71 53 32

想想短信联想到九宫格字母表前一个数字代表按键，后一个数字代表第几个字母，发现吻合这个规律

直接得到flag



根据QWE=ABC? 知道键盘加密

二. QWE=ABC
即把键盘上的字母按顺序对应ABC.

注意:红色的为明码(即你手中的密码)
黑色的就是对应的密码了.

解密得到 rhasbenvaoylii

再结合题目栅栏解密和关键字爱 (love), 栅栏解密

6栏 rabnayosevol

7栏 rabnayiosevoli

倒序解密得到flag

6.奇怪的字符串

奇怪的字符串 分值: 10

来源: 实验吧 难度: 中 参与人数: 3313人 Get Flag: 1640人 答题人数: 1712人 解题通过率: 96%

信息保密的需求和实际操作自古有之, 与之相应的信息加密与解密也是历史悠久, 现有一段经过古典密码理论(不止一种)加密的密文, 内容如下:

89 51 82 109 89 50 86 122 97 71 107 61请找出这段密文隐藏的消息明文

直接ASCII码解密得到字符串Y3RmY2UzaGk=

看格式知道base64解密得到flag

7.疑惑的汉字

疑惑的汉字 分值：10

来源：实验吧

难度：易

参与人数：3152人

Get Flag：1771人

答题人数：1844人

解题通过率：96%

现有一段经过加密的密文，内容如下：王夫 井工 夫口 由中人 井中 夫夫 由中大。请找出这段密文隐藏的消息明文。
格式：CTF{ }

当铺密码解密

当铺密码：
这个密码比较简单，但是用起来比较复杂
简单来说是用汉字来表示数字
利用汉字出头的数量来表示数字。
如下：
1 2 3 4 5 6 7 8 9
由 中 人 工 大 王 夫 井 羊

得到数字67 84 70 123 82 77 125

ASCII码表解密得到flag

8.古典密码

古典密码 分值：10

来源：北邮天枢战队

难度：易

参与人数：4783人

Get Flag：1382人

答题人数：1595人

解题通过率：87%

密文内容如下{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}

请对其进行解密

提示：1.加解密方法就在谜面中

2.利用key值的固定结构

格式：CTF{ }

ASCII码表得到字符串OCU{CFTELXOUYDECTNGAHOHRNFNIENM}IOTA

列置换参考 http://blog.sina.com.cn/s/blog_e23a215b0102wazq.html

最后根据flag的格式得到flag

9.困在栅栏里的凯撒

困在栅栏里的凯撒 分值：10

来源：北邮天枢战队

难度：易

参与人数：4166人

Get Flag：1885人

答题人数：2028人

解题通过率：93%

小白发现了一段很6的字符：NIEyQd{seft}

栅栏6栏 NEQ{etlydsf}，再凯撒解密即可得到flag

10.奇妙的音乐

凯撒密码 加密与解密 栅栏密码 md5爆破

凯撒密码

字符串:

+1	IUSVAZKX	JVTWBALY	KWUXCEMZ	LKVYDCNA	MYWZEDOB
+6	NZXAFEPG	OAYBGFQD	PBZCHGRE	QCADIHSF	RDBEJITG
+11	SECFKJUH	TFDGLKVI	UGEHMLWJ	VHFINMXK	WIGJONYL
+16	XJHKFOZM	YKILQFAN	ZLJMRQBO	AMKNSRCP	BNLOTSDQ
+21	COMPUTER	DPNQVUFS	EQORWVGT	FRPSXWHU	GSQTYXIV

凯撒一跑得到+21COMPUTER为加密密钥

古典密码需要密钥加密的就只有那几种，最后试维吉尼亚密码发现可以得到flag

(不熟悉维吉尼亚加密的可以百度自行掌握，比较简单)

16.凯撒和某某加密

凯撒和某某加密 分值: 10

来源: Veneno

难度: 易

参与人数: 3203人

Get Flag: 673人

答题人数: 831人

解题通过率: 81%

aZZg/x\ZbavpZiEZp+n)o+

密文里面含有字母和符号，如果是凯撒加密的话，应该是整个ASCII码表的移动，列举全部结果发现最有可能是flag的

第6种可能: f_l4}a_gf{u_nJ_u0s.t0

看这个密文结构应该是栅栏加密，不过这儿的是栅栏加密的一种变种

将字符串每三个一组顺序排列可以得到

```
f_ =>f _  
l4} =>l 4 }  
a_ =>a _  
gf =>g f  
{u =>{ u  
_n =>_ n  
J_ =>J _  
u0 =>u 0  
s. =>s .  
t0 =>t 0
```

从上往下，从左往右一路看下来就得到flag

17.兔子你好

兔子你好 分值：10

来源：Veneno 难度：易 参与人数：2434人 Get Flag：1189人 答题人数：1271人 解题通过率：94%

U2FsdGVkX197ihEWFWSF8qzdJ/Y1GS6pieLsbQHFUA==

base64解密发现加了盐

百度发现有一种兔子算法加密的方式，在线解密即可得到flag

18.base? ?

base?? 分值：10

来源：Justatest 难度：易 参与人数：2554人 Get Flag：525人 答题人数：618人 解题通过率：85%

YMFZZTY0D3RMD3RMMTIZ

这一串到底是什么！！！！为什么这么像base32却不是！！！！

明文的md5值为16478a151bdd41335dcd69b270f6b985

知道md5爆破就可以得到密文，发现其实密文全部大写就是YMFZZTY0D3RMD3RMMTIZ

将密文base64解密即可得到flag

19.NSCTF crypto200

NSCTF crypto200 分值：20

来源：2015NSCTF真题 难度：中 参与人数：3790人 Get Flag：585人 答题人数：600人 解题通过率：98%

小绿在黑进一台服务器后，在root文件夹下找到了一张图片，据说图片中有root的密码，您能帮他找到吗？

将图片保存后在stegsolve打开

变换之后得到一张二维码图片



扫码没法应，颜色翻转后再扫得到flag

20.NSCTF crypto50

NSCTF crypto50 分值: 10

来源: 2015NSCTF真题

难度: 易

参与人数: 4048人

Get Flag: 691人

答题人数: 774人

解题通过率: 89%

神秘的字符串: U2FsdGVkX1+qtU8KEGmMJwGgKcPUK3XBTdM+KhNRLHSCQL2nSXaW8++yBUkSylRp

看格式知道AES加密，解密得到flag



提交不对，应该还有凯撒移位加密，flag头应该是NSCTF开头，解密得到flag

21.黑客叔叔（雨袭团）1.01

最简单的加密方式 by:p0tt1

dW1mcGJsamhhd3Jmcm14aHoxOXptZj1tZWducml3NDV4M2RvbmhxfDaxfDAzfDA3fCt8KzF8KzN8Kzd8MIsxfDirMnwyKzZ8Mis3fDirOXwzKzB8MyszfdMrN3wzKzh8Mys5fD98

base64解密得到

umfplbjhawrfmrxhz19zmf9megnrmw45x3donhq|01|03|07|+|+1|+3|+7|2+1|2+2|2+6|2+7|2+9|3+0|3+3|3+7|3+8|

猜想应该是要部分字母变大写 规律是:

|01|03|07| 表示第1,3,7位

|+1|+3|+7|表示第11,13,17位

|2+1|2+2|2+6|2+7|2+9|表示第21,22,26,27,29位

|3+0|3+3|3+7|3+8|3+9|表示第30,33,37,39位

上面标记位数全部大写之后base64解密得到flag

22.黑客叔叔雨袭团 (1.02)

黑客叔叔 (雨袭团) 内部交流题 (第一季1.0.2) 分值: 20

来源: 黑客叔叔p0tt1

难度: 中

参与人数: 3870人

Get Flag: 342人

答题人数: 378人

解题通过率: 90%

详见题目

U2FsdGVkX18vmjE0tvWk69T女B神u9inuiNmM3rBhsu6tXzLhu+

iofwuHNHq3YtDKs8Z1YLvSZuUY+

mxLRK07+

m254R5YTCW8yzzgD+

mGwWfGRgqmPKdD你xA等等

看格式应该属于3des加密, 不过里面有文字, 将文字换成/, “等等”换成“==”, (别问我为什么, 格式告诉我的) 然后兔子解密 (rabbit算法) 即可

23.密文 rot-13

密文 rot13 分值: 10

来源: 2014HCTF

难度: 易

参与人数: 4090人

Get Flag: 1122人

答题人数: 1219人

解题通过率: 92%

57R9S980RNOS49973S757PQO9S80Q36P (md5不解密)

rot13解密即可得到flag

24.keyboard

BHUK,LP TGBNHGYT BHUK,LP UYGBN TGBNHGYT BHUK,LP BHUK,LP TGBNHGYT BHUK,LP TGBNHGYT UYGBN

键盘上画图得到字母, 就是flag

25.古典密码的安全性不高, 但仍然十分美妙, 请破译下面的密文

古典密码的安全性不高，但仍然十分美妙，请破译下面的密文 分值：10

来源：强网杯CTF 难度：易 参与人数：4217人 Get Flag：864人 答题人数：1000人 解题通过率：86%

本题 flag 并非 flag(可见字符) 的形式

Os drnuzearyuwn, y jtkjzoztzoes douwlr oj y ilzwex eq lsdexosa kn pwodw tsozj eq ufyzozlzbz yrl rlufydlx pozv douwlrzlbz, ydderxosa ze y rlatfyr jnjzli; mly gfbmw vla xy wbfnsy symmyew (mly vrwm qrvvrf), hlbew rd symmyew, mebhsymw rd symmyew, vbomeyew rd mly lxrzy, lfk wr dremj. Mly eyqybyze kyqbhjyew mly myom xa hyedrevbn lf bfzyewy wgxwmbngmbrf. Wr mly dsln bw fl_2jyf-k3_jgl-vb-v1_1

字频分析得到

```
0 -2.814 ?l fog?vryoe?sg, e h?dhv?v?v?rl f??sao ?h e ?avsrb rc alfrb?ly dg ?s?fs ?l?vh rc ?ne?lvaiv eoa oa?nefab ??vs f??saovaiv, effrob?ly v ^
e oay?neo hghva?: the units may be single letters (the most common), pairs of letters, triplets of letters, mi?tures of the above,
and so forth. The receiver deciphers the te?t by performing an inverse substitution. So the flag is ni_2hen-d3_hul-mi-ma_a
```

26.凯撒是罗马共和国杰出的军事统帅

凯撒是罗马共和国杰出的军事统帅 分值：10

来源：西普学院 难度：中 参与人数：4748人 Get Flag：1631人 答题人数：1786人 解题通过率：91%

MGAKUZKRWZGWAWCP

凯撒解密得到flag

27.摩擦摩擦

摩擦摩擦 分值：10

来源：西普学院 难度：易 参与人数：4368人 Get Flag：1522人 答题人数：1608人 解题通过率：95%

"....."

解题链接：<http://ctf5.shiyanbar.com/crypto/1/beiai.html> 通过

摩尔斯电码解密得到flag

28.最近听说刘翔离婚了

最近听说刘翔离婚了 分值：10

来源：西普学院 难度：易 参与人数：4652人 Get Flag：1518人 答题人数：1636人 解题通过率：93%

kyssmlxeei{ipeu}

栅栏解密得到flag

29.最近在论证一个问题，到底是先有鸡还是先有蛋

最近在论证一个问题，到底是先有鸡还是先有蛋 分值：10

来源：西普学院 难度：易 参与人数：4046人 Get Flag：1198人 答题人数：1288人 解题通过率：93%

ljm,lo 3wsdr4 6tghu7

解题链接：<http://ctf5.shiyanbar.com/crypto/1/dan.html> 通过

简单键盘加密，键盘画画

30.一段奇怪的代码

一段奇怪的代码 分值：30

来源：西普学院 难度：难 参与人数：4501人 Get Flag：1472人 答题人数：1495人 解题通过率：98%

哎！怎么出题的，都提示到家门口了

Tips asp, encode

一段奇怪的代码

```
#@~^EQAAAA==VXlj4UmkaYAUmKN3bAYAAA==^#~@
```

这段代码解密之后就是key

百度asp encode，网站在线解密即可得到flag

31.这里没有key

这里没有key 分值：10

来源：西普学院 难度：易 参与人数：5500人 Get Flag：1909人 答题人数：2018人 解题通过率：95%

你说没有就没有啊，俺为啥要听你的啊

点开有提示框大家好，不管直接看源代码，发现

```
<!-- #@~^TgAAAA=='[6*liLa6++p' aXvfiLaa6i[[avWi[[a*p[[[6*!I' [6cp' aXvXILa6fp[:6+Wp[:XvWi[[[6+XivRIAAA==^#~@ -->
```

明显的vbscript encode

丢控制台解密即可得到flag

转载于：<https://www.cnblogs.com/Acewipe/p/7631300.html>