ctf密码学习题总结

转载

cyxl0509 于 2020-10-21 12:30:27 发布 2042 收藏 5
分类专栏： CRYPTO
原文链接：https://www.cnblogs.com/levelstrcpy/p/9939720.html

1.变异凯撒

加密密文：afZ_r9VYfScOeO_UL^RWUc
格式：flag{ }

一看题中说的是凯撒加密，我就赶快使用工具列出了所有的组合，然而发现没有一个是我想要的。

于是乎，又重新审题，说的是变异凯撒，看来不能轻敌，得自己动手尝试喽！

我先找出加密密文前四个字母的ASCII码分别为97 102 90 95

又写出了flag对应的ASCII码分别为102 108 97 103

发现他们分别相差5 6 7 8

这样就找到规律了，懒得一个一个去查找ASCII码，写个代码解密出来：

```
#include<stdio.h>
int main(){
char c[]= "afZ_r9VYfScOeO_UL^RWUc";
for(int i = 0;c[i]!='\0';i++){
    c[i]=c[i]+i+5;
}
printf("%s",c);
}
```

得到flag{Caesar_variation}

2.传统知识+古典密码分值：10

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}

看到了一些年份，就在网上找出来了一份顺序表

六十甲子顺序表

顺序	干支	顺序	干支
1	甲子	16	己卯
2	乙丑	17	庚辰
3	丙寅	18	辛巳
4	丁卯	19	壬午
5	戊辰	20	癸未
6	己巳	21	甲申
7	庚午	22	乙酉
8	辛未	23	丙戌
9	壬申	24	丁亥
10	癸酉	25	戊子
11	甲戌	26	己丑
12	乙亥	27	庚寅
13	丙子	28	辛卯
14	丁丑	29	壬辰
15	戊寅	30	癸巳

六十甲子顺序表

顺序	干支	顺序	干支
31	甲午	46	己酉
32	乙未	47	庚戌
33	丙申	48	辛亥
34	丁酉	49	壬子
35	戊戌	50	癸丑
36	己亥	51	甲寅
37	庚子	52	乙卯
38	辛丑	53	丙辰
39	壬寅	54	丁巳
40	癸卯	55	戊午
41	甲辰	56	己未
42	乙巳	57	庚申
43	丙午	58	辛酉
44	丁未	59	壬戌
45	戊申	60	癸亥

根据表找出不同年份对应的数字，背面说+甲子，于是在每个数字上面再加了60，得到

88 90 83 68 77 70 76 90

根据这些数字，我们的第一反应当然是ASCII，于是找出它对应的字符

XZSDMFLZ

于是用工具先进行栅栏解密、再凯撒解密得到flag

3.try them all分值：10

You have found a passwd file containing salted passwords. An unprotected configuration file has revealed a salt of 5948. The hashed password for the 'admin' user appears to be 81bdf501ef206ae7d3b92070196f7e98, try to brute force this password.

题中提到哈希密码，将81bdf501ef206ae7d3b92070196f7e98进行MD5解密（https://www.somd5.com/），得到sniper5948

再将5948的盐去掉，得到Flag.

4.robomunication分值：10

We recorded the following file between two robots. Find out what evil things they are plotting, and recover their secret key!

解题链接： http://ctf5.shiyanbar.com/crypto/robomunication/robo.rar

打开链接听音乐，啵哔哔哔.....，一听就是摩斯密码，用Audacity，根据波的宽度，宽的为-，短的为.，写出来后在这里（https://www.ctftools.com/down/）解密get flag。

5.奇怪的短信分值：10

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}

题中说了是短信，就想到了手机.....九键输入法！

两两分组，33指的是第3个按键上的第三个字母，也就是F，，以此类推，就得到Flag.

6.围在栅栏中的爱分值：10

最近一直在好奇一个问题，QWE到底等不等于ABC？

-.- .. --.- .-.. .-- - ..-. -.-. --.- --. -. ... --- ---

flag格式：CTF{xxx}

首先看到摩斯电码转化为对应的符号，kiqlwtfcqgnsoo

然后题中说了QWE等不等于ABC，而QWE分别为键盘中第一行前三个字母，然后我们就想到将键盘中的字母依次与ABCDEFG替换，得到rhasbenvaoylii

题中又说了围在栅栏中的爱，于是我们就试着用栅栏解密找出love。

发现在七栏中，逆序输出得到flag.

7.疑惑的汉字分值：10

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{ }

看到这样的汉字，就想到了当铺密码。

当铺密码 就是一种将中文和数字进行转化的密码，算法相当简单:当前汉字有多少笔画出头，就是转化成数字几。

题目中的汉字： 王夫 井工 夫口 由中人 井中 夫夫 由中大

转换为数字：67 84 70 123 82 77 125

对照ASCII码，get flag.

8.古典密码分值：10

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{ }

看到了数字，将其进行十进制解码（https://www.jb51.net/tools/zhuanhuan.htm?spm=a2c4e.11153940.blogcont333129.5.57da1656KJDtYs）OCU{CFTELXOUYDECTNGAHOHRNFIENM}IOT

看到字符串中有CTF，就想到了栅栏密码，35个字符，将其分为5行7列

OCU{CFT
ELXOUYD
ECTNGAH
OHRNFIE
NM}IOTA

在进行列置换，

CTF{COU
LDYOUEX
CHANGET
HEINFOR
MATION}

连起来就得到Flag.

9.困在栅栏里的凯撒分值：10

小白发现了一段很6的字符：NlEyQd{seft}

先用栅栏得：NEQ{etlydsf}

再用凯撒得到：CTF{tianshu}

10.Decode分值：10

flag格式:ctf{}

解题链接： http://ctf5.shiyanbar.com/crypto/Readme.txt

首先将十六进制解码转换为字符（https://www.sojson.com/hexadecimal.html）

得到url编码

%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
%45%4b%4d%54%45%32%43%6a%45%78%4d%51%6f%78%4d%54%55%4b%4d%54%41%30%43%6a%4
%4f%54%63%4b%4d%54%45%77%43%6a%6b%34%43%6a%6b%33%43%6a%45%78%4e%41%3d%

再将url编码在http://tool.chinaz.com/Tools/Unicode.aspx解得

MTE5CjEwMQoxMDgKOTkKMTExCjEwOQoxMD
EKMTE2CjExMQoxMTUKMTA0CjEwNQoxMjEK

在进行base64解密得119 101 108 99 111 109 *101 116 111 115 104 105 121 97 110 98 97 114*

最后根据ASCII码转换为字符，得到Flag。