实验吧CTF密码学部分题目总结

转载

adversity` 于 2018-03-11 18:06:46 发布 13360 收藏 23

1.变异凯撒 http://www.shiyanbar.com/ctf/2038

题目是 加密密文：afZ_r9VYfScOeO_UL^RWUc 格式：flag{ }
拿凯撒解密，栅栏解密一通乱试，并没有发现什么收获。后来看了大牛的博客才发现前四位Z_的ASCII码为97 102 90 95，题目说flag的格式为flag{} 前四位对应的ASCII码为102 108 97 103。这时可以看出加密方式是第一个字符的ASCII码减5，第二位的ASCII码减6，第三个减7，依次类推。这时写出解密代码。解出来的就是flag了。这里用C来写解密过程：

```
#include<stdio.h>
int main()
{
int i;
char a[30]="afZ_r9VYfScOeO_UL^RWUc";
for(i=0;a[i];i++)
{ a[i]=a[i]+i+5;
printf("%d",a[i]);
}
return 0;
}
```

即可得出flag。

2.try them all http://www.shiyanbar.com/ctf/1981

题目描述： 你已经找到一个包含密码的passwd文件。 一个未受保护的配置文件显示5948的盐。“管理员”用户的哈希密码看起来是81bdf501ef206ae7d3b92070196f7e98，试图暴力破解这个密码。
哈希密码，加密方式又是这种形式，首先想到md5加密。尝试之后得到sniper5948。提交，发现错误。再仔细看看题目，说显示5948的盐，所以尝试一下sniper发现就是正确答案。

3.奇怪的短信 http://www.shiyanbar.com/ctf/1920

题目描述：
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}
题目说收到的奇怪的短信，联想到手机键盘加密。即两两一组，第一个数字表示键盘上的第几个键，第二个数字表示对应键上的第几个字母。由此将其两两分组再对应字母得到flagissimple。到这作死了很多次尝试了大小写加空格各种方式，后来发现是自己想复杂了，答案就是CTF{flagissimple}，23333.

4.我喜欢培根 http://www.shiyanbar.com/ctf/1842

题目描述：

key: CTF{}

解题链接： http://ctf5.shiyanbar.com/crypto/enc1.txt

点开后发现是摩斯密码加密后的密文，在网上将摩斯密码转换成字符串为

MORSE..--.-IS..--.-COOL..--.-BUT..--.-BACON..--.-IS..--.-COOLER..--.-

DCCDCCCDDDCDCCCDDCCCCCCCCCCDDCDCCCCDCCCCC/CDCCCDCCDC/CCCDCCDDDCCDDDCCDCDD

摩斯很酷，培根更酷。联系后面的字符及题目信息想到培根密码，就是用a,b来为信息加密。所以将解密出的含c,d的字符串用C=A,D=B的方式进行表示 然后使用培根解密即可得到答案：AHIYANBA IS COOL

5.古典密码

http://www.shiyanbar.com/ctf/1870

题目描述：

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{ }

看到这个密文第一反应应该就是ASCII码了吧，对照ASCII码表得到OCU{CTFELXOUYDECTNGAHOHRNFIENM}IOTA。到这里就不知道该如何继续了。后来才知道这是列置换：

将明文按固定长m分组，即每行m个字母，在密钥控制下按某一顺序交换列，最后按列优先的顺序依次读出，即产生了密文。

原来字符串为35位。35=7*5

得到如下结果：

1 234567

OCU{CFT

ELXOUYD

ECTNGAH

OHRNFIE

NM}IOTA

key值的固定结构为CTF{}

故第2列打头或第5列打头，接下来是第7列，然后是第6列，考虑到“{”是第4列，考虑到“}”是最后一列

尝试后得到

1234567列转换为2764513

即为：

2764513

CTF{COU

LDYOUEX

CHANGET

HEINFOR

MATION}

CTF{COULDYOUEXCHANGETHEINFOR
MATION}

could you exchange the information?是一句完整的答案，从而解答成功

6.困在栅栏里的凯撒 http://www.shiyanbar.com/ctf/1867

题目描述：

小白发现了一段很6的字符：NlEyQd{seft}

分析一下题目，困在栅栏里的凯撒，会不会是先栅栏后凯撒。一共有12个字符，很六的意思是不是六个为一组，一共分两栏？尝试一下，先栅栏得到

NEQ{ETIYDSF}。然后再用凯撒解密，列出所有解密方式，发现有一个字符串炒鸡熟悉

CTF{tianshu}。提交发现这个就是答案啦。

先写这么多，等再做写题目就再更。感谢大牛牛们的博客啦，一起加油吧。。。