实验吧Crypto

原创

我是一个没有感情的熊猫 于 2018-01-22 15:19:28 发布 2217 收藏
分类专栏： CTF 信息安全 文章标签： CTF 密码学

本文链接：https://blog.csdn.net/windy_hui/article/details/79129377


CTF 同时被 2 个专栏收录
5 篇文章 0 订阅
订阅专栏


信息安全
8 篇文章 1 订阅
订阅专栏

1. 传统知识+古典密码

题目链接：http://www.shiyanbar.com/ctf/1991

解开这道题，我们需要了解中国传统文化,以下为六十甲子顺序表

六十甲子顺序表

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

通过这个表格我们可以得出辛卯，癸巳，丙戌，辛未，庚辰，癸酉，己卯，癸巳分别对应的是28,30,23,8,17,10,16,30。由于题目中说+甲子，所以得到88,90,83,68,77,70,76,90，对照ascii码表我们得到X,Z,S, D,M, F,L,Z，在对其进行栅栏以及凯撒解密即可以得到我们的flag。

2. 奇怪的短信

题目链接：http://www.shiyanbar.com/ctf/1920

收到一条奇怪的短信:

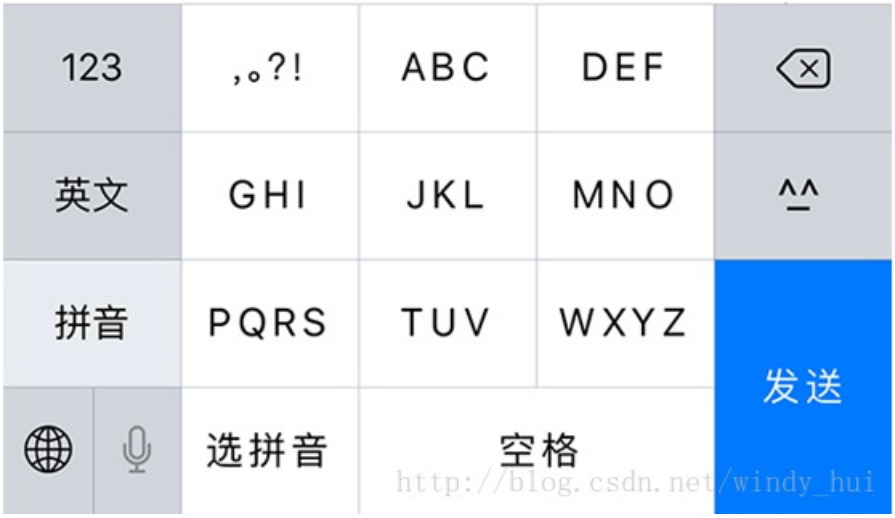
335321414374744361715332

你能帮我解出隐藏的内容嘛？！

这道题不得不说不用九宫格输入法的喵酱们很难想到

其实他就是33 53 21 41 43 74 7443 61 71 53 32

分别对照九宫格（白色部分）第三个格子第三个字符



例如 33对应的是F ，53对应的是L，以此类推便可以拿到flag

3. 围在栅栏中的爱

题目链接：http://www.shiyanbar.com/ctf/1917

拿到这道题我们很容易的就可以想到摩斯码，使用在线转换工具即可得到：KIQLWTFCQGNSOO，接下来我们对其进行栅栏以及凯撒解密即可得到flag。

4. 疑惑的汉字

题目链接：http://www.shiyanbar.com/ctf/1876

王夫 井工 夫口 由中人 井中 夫夫 由中大

看到这个题文，我们很容易就可以想到当铺密码，所谓的当铺密码即看一个字有多少笔画出头，以王为例，我们可以得到6，以此类推得到其他字符所对应的数字，通通过ascii码表进行转换，再使用基本解码思路便可以得到flag。

5. 古典密码

题目链接：http://www.shiyanbar.com/ctf/1870

密文内容如下{79 67 85 123 67 7084 69 76 88 79 85 89 68 69 67 84 78 71 65 72 79 72 82 78 70 73 69 78 77 125 7379 84 65}请对其进行解密.、

题目中已经明确指明了这是一道古典密码题目，那我们就采用这个思路解题就可以得到flag了

6. 困在栅栏里的凯撒

题目链接：http://www.shiyanbar.com/ctf/1867

小白发现了一段很6的字符：NIEyQd{seft}看到这段字符，很容易联想到栅栏解密，再进行凯撒解密得到flag

7. 奇妙的音乐

题目链接：http://www.shiyanbar.com/ctf/1862

这道题与前边的第三题类似，均是摩斯码题目，摩尔斯电码morsecode 它由两种基本信号和不同的间隔时间组成：短促的点信号“·”，读“滴”（Di）；保持一定时间的长信号“—”，读“嗒”（Da）。间隔时间：滴，1t；嗒，3t；滴嗒间，1t；字符间，3t；字间，7t。我们即可以得到摩斯码，再进行转换，解密即可得到flag

这道题我们也可以用声音解密软件看出其波形图得到摩斯码进而拿到小旗子

8. Fair-Play

题目链接：http://www.shiyanbar.com/ctf/1852

这道题题目其实已经告诉了我们要采用的解码方案，即playfair密码

以下仅介绍具体方法，解题过程以此类推

编制密码表

第一步是编制密码表。在这个5*5的密码表中，共有5行5列字母。第一列（或第一行）是密钥,其余按照字母顺序。密钥是一个单词或词组，若有重复 字母，可将后面重复的字母去掉。当然也要把使用频率最少的字母去掉。如：密钥是Live and learn,去掉后则为liveandr。如果密钥过长可占用第二列或行。

如密钥crazy dog，可编制成

C	D	F	M	T
R	O	H	N	U
A	G	I(J)	P	V
Z	B	K	Q	W
Y	E	L	S	X

整理明文

第二步整理明文。将明文每两个字母组成一对。如果成对后有两个相同字母紧挨或最后一个字母是单个的，就插入一个字母X（或者Q）。

如，communist，应成为co,mx,mu,ni,st。

编写密文

最后编写密文。对明文加密规则如下：

1 若p1 p2在同一行，对应密文c1 c2分别是紧靠p1 p2 右端的字母。其中第一列被看做是最后一列的右方。如，按照前表，ct对应dc

2 若p1 p2在同一列，对应密文c1 c2分别是紧靠p1 p2 下方的字母。其中第一行被看做是最后一行的下方。

3 若p1 p2不在同一行，不在同一列，则c1 c2是由p1 p2确定的矩形的其他两角的字母（至于横向替换还是纵向替换要事先约好，或自行尝试）。如，按照前表，wh对应ku或 uk。

如，依照上表，明文where there islife,there is hope.

可先整理为：WH ER ET HE RE IS LIFE TH ER EI SH OP EX

然后密文为：KU YO XD OL OY PL FKDL FU YO LG LN NG LY

将密文变成大写，然后几个字母一组排列。

如5个一组就是KUYOX DOLOY PLFKD LFUYO LGLNN GLY

解密编辑

Playfair解密算法首先将密钥填写在一个5*5的矩阵中（去Q留Z），矩阵中其它未用到的字母按顺序填在矩阵剩余位置中，根据替换矩阵由密文得到明文。

对密文解密规则如下：

1 若c1 c2在同一行，对应明文p1 p2分别是紧靠c1 c2 左端的字母。其中最后一列被看做是第一列的左方。

2 若c1 c2在同一列，对应明文p1 p2分别是紧靠c1 c2 上方的字母。其中最后一行被看做是第一行的上方。

3 若c1 c2不在同一行，不在同一列，则p1 p2是由c1 c2确定的矩形的其他两角的字母。其实就是反其道而行之。

9. 我喜欢培根

题目链接：http://www.shiyanbar.com/ctf/1842

同样打开连接还是一段摩斯密码，我们对其进行在线转换得到MORSE..--.-IS..--.-COOL..--.-BUT..--.-BACON..--.-IS..--.-COOLER..--.-
DCCDCCCDDDCDCCCDDCCCCCCCCCDDCDCCCCDCCCCC/CDCCCDCCDC/CCCDCCDDDCCDDDCCD

我们看到了morse is cool butbacon is cooler 以及一串字符

在这里我们要用培根密码解码

所谓的培根密码是一种本质上用二进制数设计的，没有用通常的0和1来表示，而是采用a和b表示的加密方法。

这个就是培根密码的一种表示方法，至于另一种表示方法大家可以问度娘，根据培根密码对其解密即get 到flag。

10.decode

题目链接：http://www.shiyanbar.com/ctf/1831

打开解题链接可以看到一大串字符，我们对其进行十六进制转字符—>url解码 —>base64解码 最后ascii码转字符即可get 到flag

11.杯酒人生

题目链接：http://www.shiyanbar.com/ctf/1826

这道题不多说了，进行凯撒解密很快就可以得到flag

12.NSCTFcrypto50

题目链接：http://www.shiyanbar.com/ctf/1758

思路AES解密接着凯撒解密即可

13.密文rot 13

题目链接：http://www.shiyanbar.com/ctf/728

题目中已经说的很清楚了md5不解密，那就不要再去用md5解了

我们对其进行直接解密就好，这道题的答案是没有格式的，所以不要怀疑人生。

14.keyboard

题目链接：http://www.shiyanbar.com/ctf/61

这道题挺有意思的，就是要看我们的脑洞够不够大，题目中说了，这道题跟键盘有关，那我们一定要很好的利用这个提示，其实就是……在键盘上画画.ok拿到flag

15.最近在论证一个问题是先有鸡还是先有蛋

题目链接：http://www.shiyanbar.com/ctf/37

这道题目其实也是跟键盘有关系的,嘿嘿就说到这看键盘，ok

16.这里没有key

题目链接: http://ctf5.shiyanbar.com:8080/4/index.html

点开解题连接，审查网页元素我们便可以看到一串字符<!--
#@~^TgAAAA==‘[6*liLa6++p'aXvfiLaa6i[[avWi[[a*p[[6*!l'[6cp'aXvXlLa6fp[:6+Wp[:XvWi[[6+XivRlAAA==^#~@-->
对他进行解码即可得到flag

17. 变异凯撒

给出一串字符afZ_r9VYfScOeO_UL^RWUc

首先想到ASCII，对照给出字符串以及flag{}的ASCII值

a	f	Z	_
97	102	90	95
f	l	a	g
102	108	97	103
5	6	7	8

Get到规律运行一下得到flag

```c
#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);
}
```


18.trythem all

You have found a passwd file containingsalted passwords. An unprotected configuration file has revealed a salt of5948. The hashed password for the 'admin' user appears to be81bdf501ef206ae7d3b92070196f7e98, try to brute force this password.

关键词salted，md5，很容易get到flag

19.trivial

Anunlocked terminal is displaying the following:
Encryption complete, ENC(???,T0pS3cre7key) = Bot kmws mikferuigmzf rmfrxrwqeabs perudsf! Nvm kda ut ab8bv_w4ue0_ab8v_DDU
You poke around and find this interesting file.

打开附件是一段代码，分析代码其实是加密解密的方法，而题目中已经给出了明文密文和秘钥，只需要修改代码即可得到flag

```python
#!/usr/bin/env python
import sys

alphaL = "abcdefghijklnmopqrstuvqxyz"
alphaU = "ABCDEFGHIJKLMNOPQRSTUVQXYZ"
num    = "0123456789"
keychars = num+alphaL+alphaU
key = 'T0pS3cre7key'
ciphertext = 'Bot kmws mikferuigmzf rmfrxrwqe abs perudsf! Nvm kda ut ab8bv_w4ue0_ab8v_DDU'

plaintext = ""
for i in range(len(ciphertext)):
    rotate_amount = keychars.index(key[i%len(key)])
    if ciphertext[i] in alphaL:
        enc_char = ord('a') + (ord(ciphertext[i]) - ord('a') - rotate_amount) % 26
    elif ciphertext[i] in alphaU:
        enc_char = ord('A') + (ord(ciphertext[i]) - ord('A') - rotate_amount) % 26
    elif ciphertext[i] in num:
        enc_char = ord('0') + (ord(ciphertext[i]) - ord('0') - rotate_amount) % 10
    else:
        enc_char = ord(ciphertext[i])
    plaintext = plaintext + chr(enc_char)
print(plaintext)
```


20.rsarsa

Mathis cool! Use the RSA algorithm to decode the secret message, c, p, q, and e areparameters for the RSA algorithm.

P=964842302901051567659055174001042653494573763923573980064398935203985250729849139956l0

Q=11874843837980297032092405848653656852760910154543380907650040190704283358909208578251

e= 65537

c=832082989951746041747735902982036393605400248712561268928896613457424033149298619391 00

UseRSA to find the secret message

题目中已经把提示全部给出，只要知道RSA算法就ok，自己写个脚本跑一下get到flag。

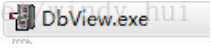
21.robomunication

Werecorded the following file between two robots. Find out what evil things theyare plotting, and recover their secret key!

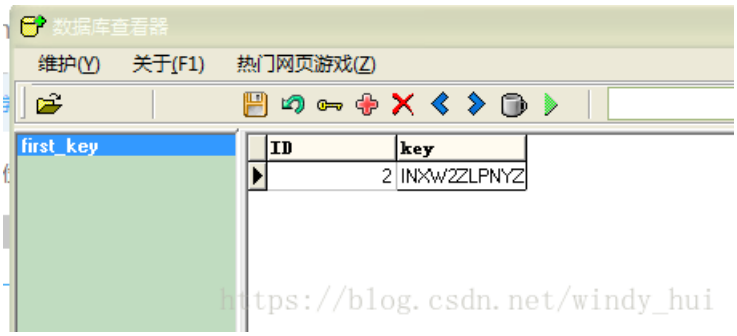
考验听力的时间到了，自己来拿flag吧。

22.chinese hacker

这道题官方给的难度评定是难，其实做起来很简单

去get数据库文件，但是打开其需要密码，这时我们使用数据库查看器 

这个软件就可以，百度上有很多下载资源，因为我们不知道密码，所以点击破解密码在进行连接，get到key1



提交key1后返回flag一部分，看到这串keyINXW2ZLPNYZDAMJSMJQWE6I=，因为结尾有=第一反应base64，但是没有成功，再尝试一次base 32得到code 2，提交后返回code2，将两个code用+连接即可得到flag

未完待续