CTF实验吧，部分密码学writeup

原创

0xJoEcO01 于 2019-05-23 17:34:16 发布 712 收藏 6

分类专栏： CTF 文章标签： CTF

本文链接：https://blog.csdn.net/weixin_43727556/article/details/90484723

1、这里没有key

```
解题链接： http://ctf5.shiyanbar.com:8080/4/index.html
```

点进去就会有一个弹窗出来

查看源码，看到一段密文，看起来像是VB加密

```
<html>
<head>
    <title>大家好</title>
    <meta http-equiv="Content-Type" content="text/html; charset=Utf-8" />
</head>
<body>
<br>
<br>
<center>
<script>
alert("这里没有key");
</script>
</center>
</body>
</html>

<!-- #@~^TgAAAA==']6*1iLa6++p'aXvfiLaa 6i[[avWi[[a *p[[6*!I'[6 cp'aXvXILa6 fp[:6+Wp[:XvWi[[6+XivRIAAA==^#~@ -->
```


VB**解密网站：https://www.dheart.net/decode/index.php

JScript/VBscript

JS/VBS/ASP

```
<!--
#@~^TgAAAA==’[6*liLa6++p’aXvfiLaa 6i[[avWi[[a *p[[6*!I’[6 cp’aXvXILa6 fp[:6+Wp[:XvWi[[
6+XivRIAAA==^#~@ -->
```

JS/VBS/ASP

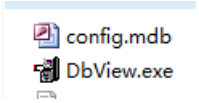
```
<!-- Encode@decode -->
```


**

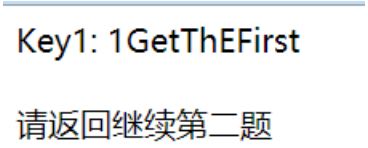
2、chinese hacker**

解题链接：http://ctf5.shiyanbar.com/web/2/

自行去下载这个查看数据库的软件



得到文件，查看数据库，拿到第一个key：INXW2ZLPNYZDAMJSMJQWE6I=
提交后出现第一个key



题目有点坑，提示的是4648 ———> 46=24 48=32 说明用base32进行解密

用base32对着一段进行解密：INXW2ZLPNYZDAMJSMJQWE6I=
解密后：Comeon2012baby
提交拿到Key2: 2tHEWinNer

**

3、困在栅栏里的凯撒

**

六行二列
N I
E y
Q d
{ s
e f
u }
解到：NEQ{etlydsf}

用凯撒加密位移15位

这里有个坑，把 CTF{tiXnshu}提交flag不正确
于是他要把里面‘X’替换成别的字母。
正确flag：CTF{tianshu}

**

4、我喜欢培根

**

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

点进去看到一大串的莫尔斯电码

−− −−− .−. ... .−.− ... ...−.− −.−. −− −−− .−.. ...−.− −... ...− − ...−.− −... .− −.−. −− −. ...−.− ... ...−.− −.−. −− −−− .−.. . .−. ...−.− −... −.−. −.−. −.−. −.−. −... −... −... −.−. −... −.−. −.−. −.−. −... −... −.−. −.−. −.−. −.−. −.−. −.−. −.−. −.−. −... −... −.−. −... −.−. −.−. −.−. −... −.−. −.−. −.−. −.−. −.−. / −.−. −... −.−. −.−. −.−. −... −.−. −.−. −.−. −... −.−. / −.−. −.−. −.−. −... −.−. −.−. −... −... −... −.−. −.−. −... −.−. −... −...

对其进行解密

回想到题目说道培根，猜测会不会有这样一种加密方式

用浏览器一查，果然有这样一种加密方式，只不过加密的字母只能是a和b

培根密码，又名**倍康尼密码**（英语：Bacon's cipher）是由法兰西斯·培根发明的一种隐写术。

中文名	培根密码	发明者	法兰西斯·培根
外文名	Bacon's cipher	属　性	隐写术
别　称	倍康尼密码	学　科	密码学

目录

原理

编辑

加密时，明文中的每个字母都会转换成一组五个英文字母。其转换依靠下表：

A/a	aaaaa	H/h	aabbb	O/o	abbba	V/v	babab
B/b	aaaab	I/i	abaaa	P/p	abbbb	W/w	babba
C/c	aaaba	J/j	abaab	Q/q	baaaa	X/x	babbb
D/d	aaabb	K/k	ababa	R/r	baaab	Y/y	bbaaa
E/e	aabaa	L/l	ababb	S/s	baaba	Z/z	bbaab

F/f	aabab	M/m	abbaa	T/t	baabb		
G/g	aabba	N/n	abbab	U/u	babaa		

加密者需使用两种不同字体，分别代表A和B。准备好一篇包含相同AB字数的假信息后，按照密文格式化假信息，即依密文中每个字母是A还是B分别套用两种字体。

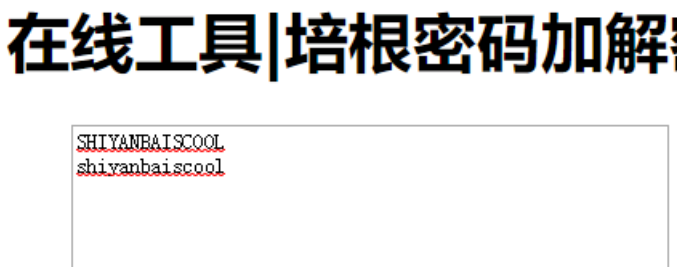
解密时，将上述方法倒转。所有字体一转回A，字体二转回B，以后再按上表拼回字母。

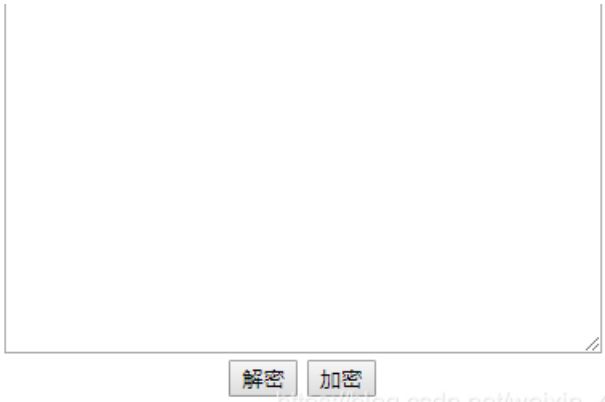
法兰西斯·培根另外准备了一种方法，其将大小写分别看作A与B，可用于无法使用不同字体的场合（例如只能处理纯文本时）。但这样比起字体不同更容易被看出来，而且和语言对大小写的要求也不太兼容。

培根密码本质上是将二进制信息通过样式的区别，加在了正常书写之上。培根密码所包含的信息可以和用于承载其的文章完全无关。

把原来的字母都替换掉

再对培根密码进行解密





flag：CTF{SHIYANBA IS COOL}

**

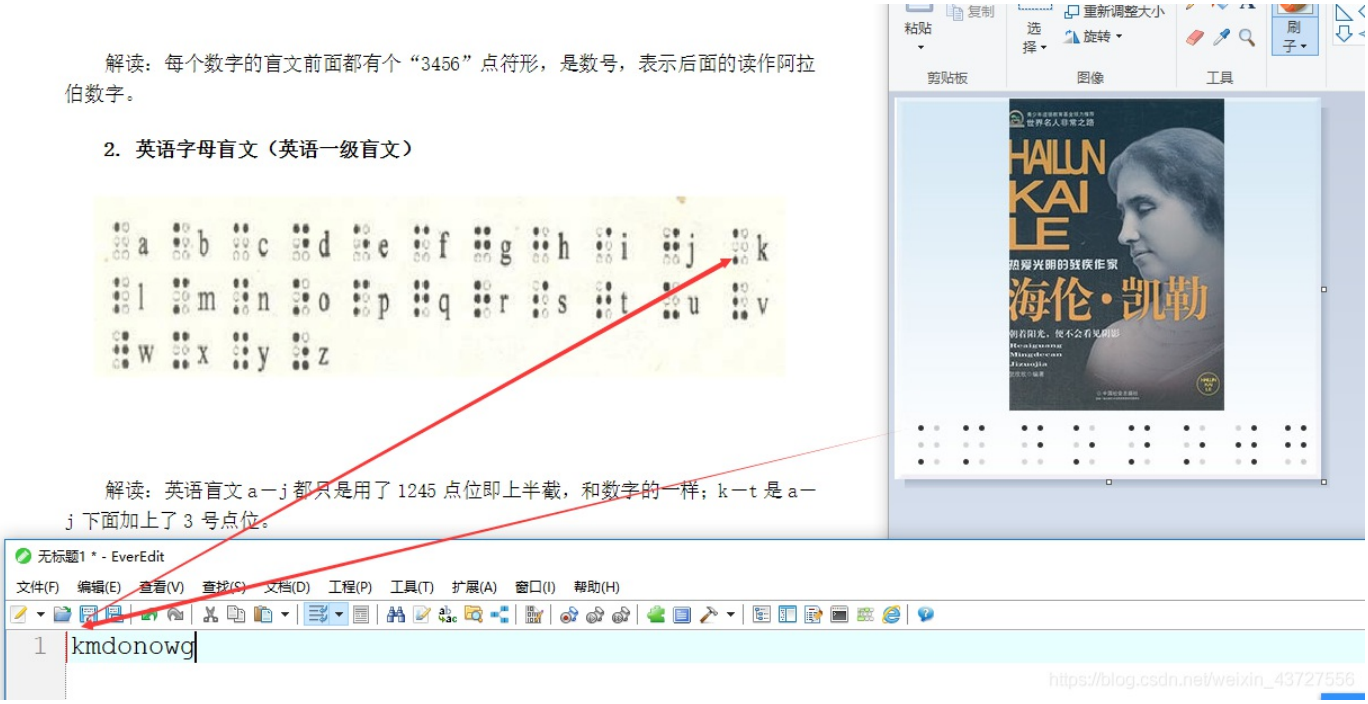
5、奇妙的音乐

**

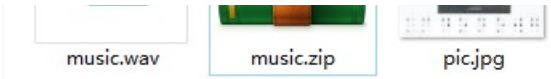
据说flag就藏在这段音乐中，请仔细听。

格式：CTF{}

解题链接： http://ctf5.shiyanbar.com/crypto/123.zip
下载后得到两个东西，一个是图片一个是加了密的压缩包
打开图片看到了海伦凯勒的图片，下面有一串密文
我们都知道海伦凯勒是盲人，可以联想到盲文，以前我对盲文也有点印象，见过。
于是查盲文



解压出来了一个音频文件



用Audacity这个工具打开，把莫尔斯电码给搞出来

莫尔斯电码

Morse code

-.-. - ..-. .— .—. . .. —— —.. —... ...— ..— ..—.. ..— ...— -.. —..

编 码　　解 码

ctfwpei08732?23dz

**

6、Decode

**

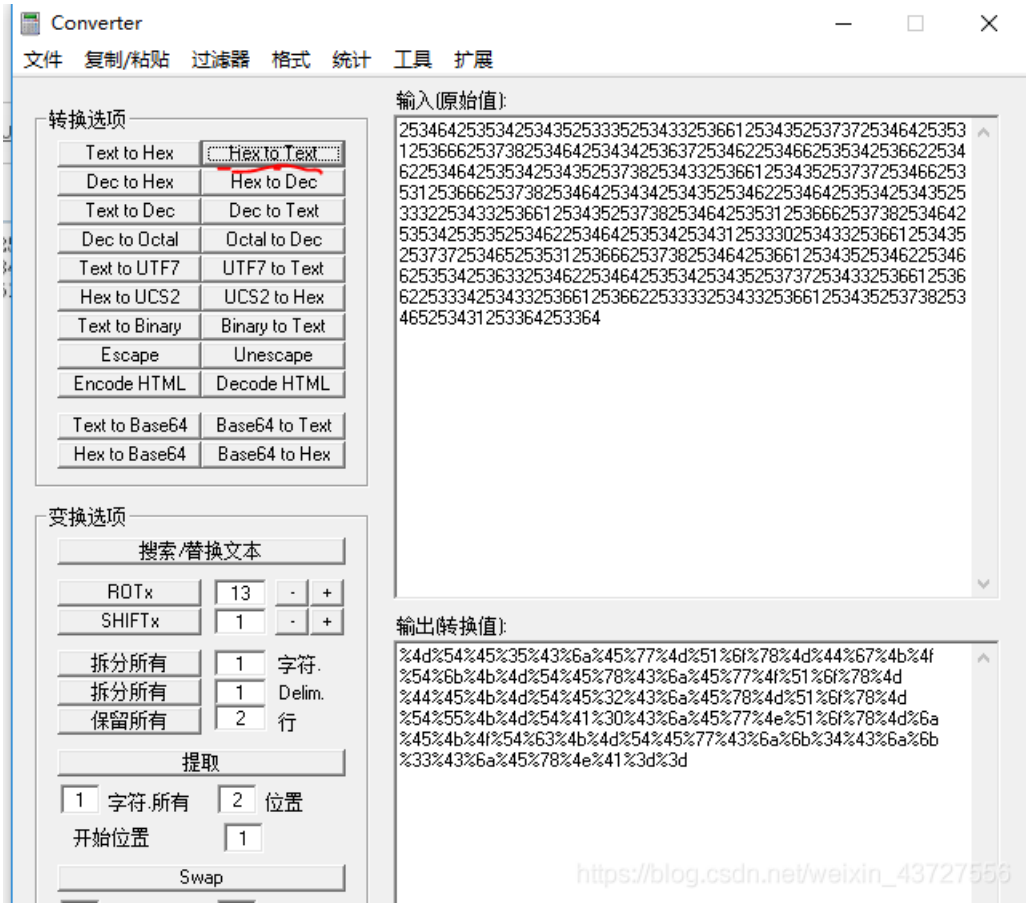
flag格式:ctf{}

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

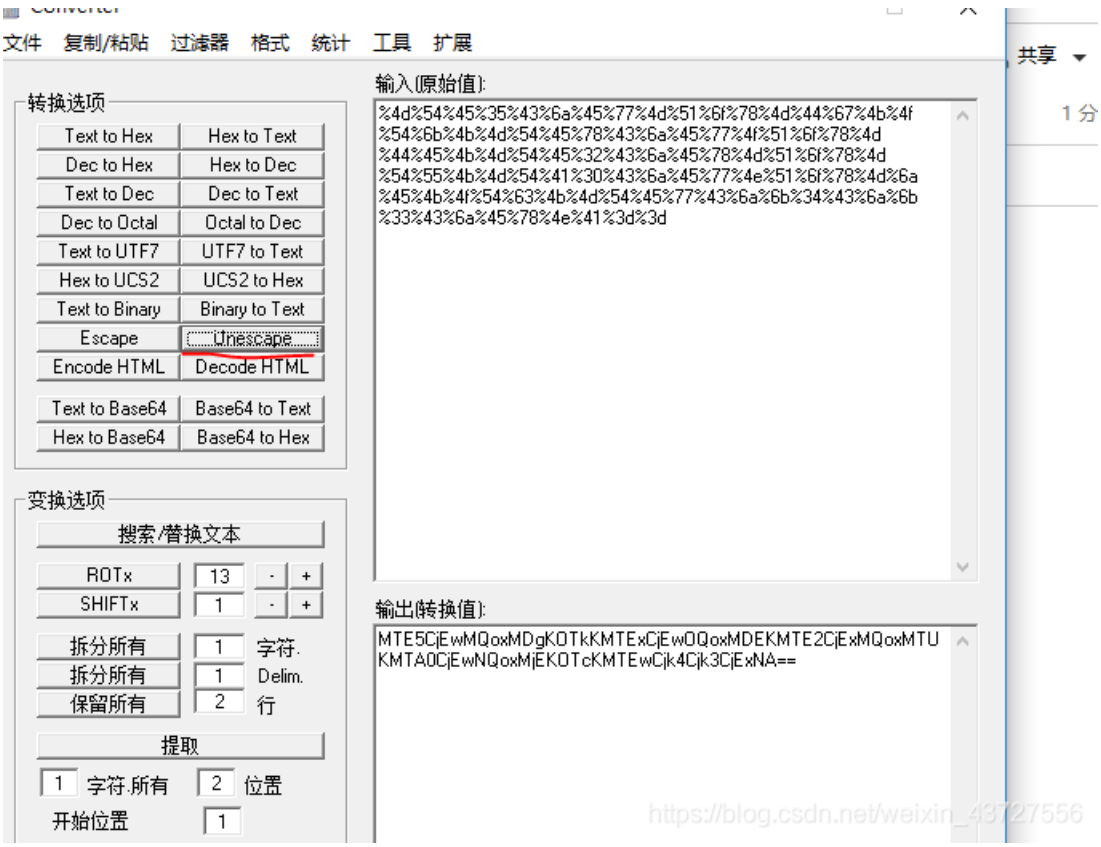
点进去是一大串16进制编码

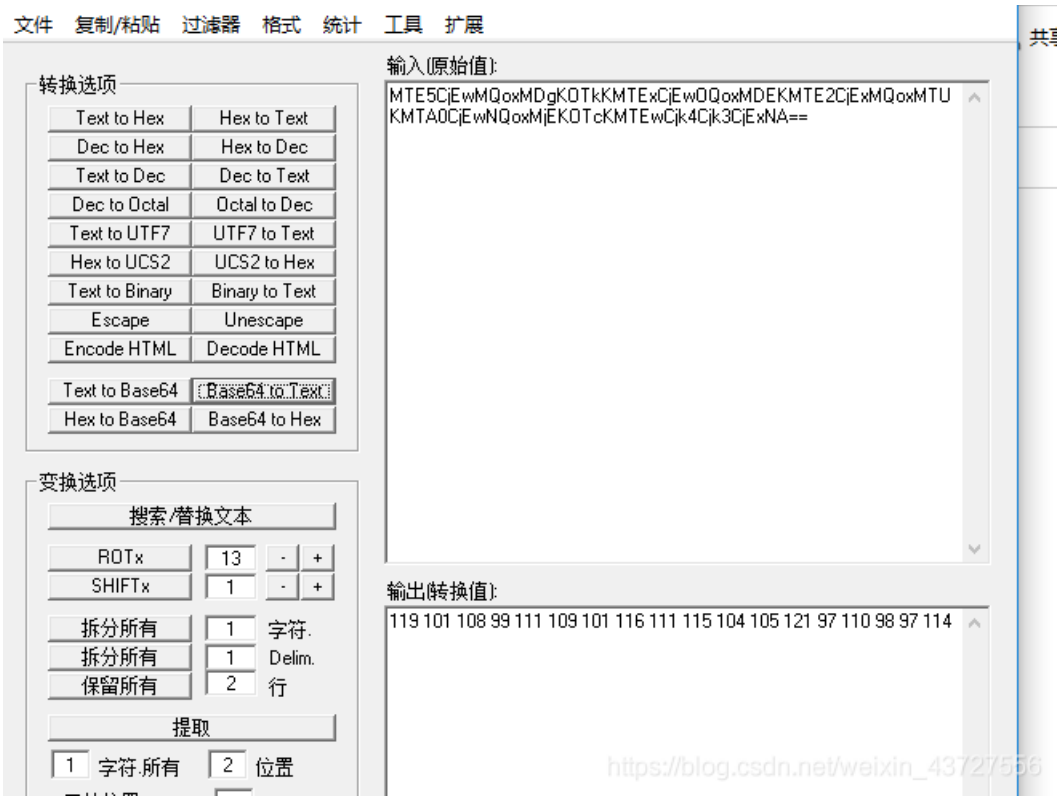
0x25346425353425343525333525343325366125343525373725346425353125366625373825346425343425363725346225346625353425366225346225346425353425343525373825343325366125343525373725346625353125366625373825346425343425343525346225346425353425343525333225343325366125343525373825346425353125366625373825346425353425353425346225346425353425343125333025343325366125343525373725346525353125366625373825346425361253435253462253466253534253633253462253464253534253437253733253661253662253334253433253661253662533332534332536612536622533332534332536612534352537382534652534312533640253364

将十六进制转换成文本



输出的结果，可以用Unescape编码解，得到一串base64





ascii码解码，得到flag