

攻防世界Crypto新手练习区0~6_writeup

原创

金帛 于 2022-03-25 19:20:05 发布 154 收藏

分类专栏: [攻防世界之Crypto](#) 文章标签: [CTF](#) [攻防世界](#) [XCTF](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/l2872253606/article/details/123721561>

版权



[攻防世界之Crypto](#) 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

目录

一. base64

二. Caesar

三. Morse

四. 幂数加密

五. Railfence

六. 不仅仅是Morse

一. base64

下载附件打开

```
af681321af224387a21c724! X +
1 Y3liZXJwZWJjZxtXZWxjb21lX3RvX25ld19Xb3JsZCF9|
```

得到一串编码, 根据题目提示, 应该是base64编码, 复制到在线网站解码得到

AmanCTF - BASE64编码解码

在线BASE64编码解码

```
Y3liZXJwZWJjZXtXZWxjb21lX3RvX25ld19Xb3JsZCF9
```

加密

解密

```
cyberpeace{Welcome_to_new_World!}
```

拿到flag

二. Caesar

下载附件打开

```
9f08657b76274fa3b64a8e5 × +
1 oknqdbqmoq{kag_tmhq_xqmdzqp_omqemd_qzodkbfuaz}
```

根据题目提示，这串编码应该就是凯撒编码(Caesar Code)，复制到在线工具解码，枚举解码得到

AmanCTF - 凯撒(Caesar)加密/解密

在线凯撒(Caesar)加密/解密

```
oknqdbqmoq{kag_tmhq_xqmdzqp_omqemd_qzodkbfuaz}
```

偏移量

加密

解密

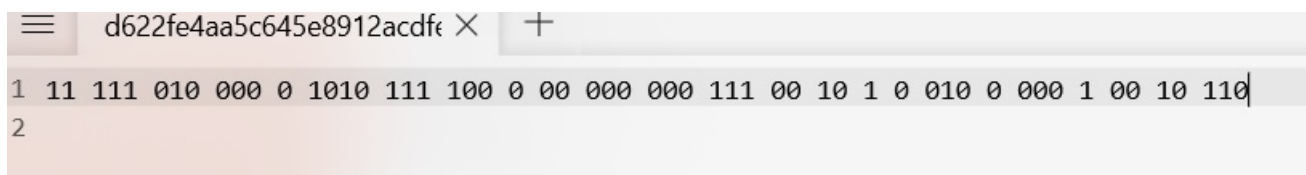
枚举

```
tbehushdth{brx_kdyh_ohduqhg_fdhvdu_hqtubswlrq}  
eadgtrgceg{aqw_jcxg_ngctpgf_ecguct_gpetarvkqp}  
dzcfsqfbdf{zpv_ibwf_mfbsofe_dbftbs_fodszqujpo}  
cyberpeace{you_have_learned_caesar_encryption}  
bxadqodzbd{xnt_gzud_kdzqmdc_bzdrzq_dmbqxoshnm}  
awzcpncyac{wms_fytc_jcypicb_aycyp_clapwnrgml}  
zvybombxzb{vlr_exsb_ibxokba_zxbpxo_bkzovmqflk}  
yuxanlawya{ukq_dwra_hawnjaz_ywaown_ajynulpekj}  
xtwzmkzvzx{tjp_cvqz_gzvmizy_xvznm_zixmtkodji}
```

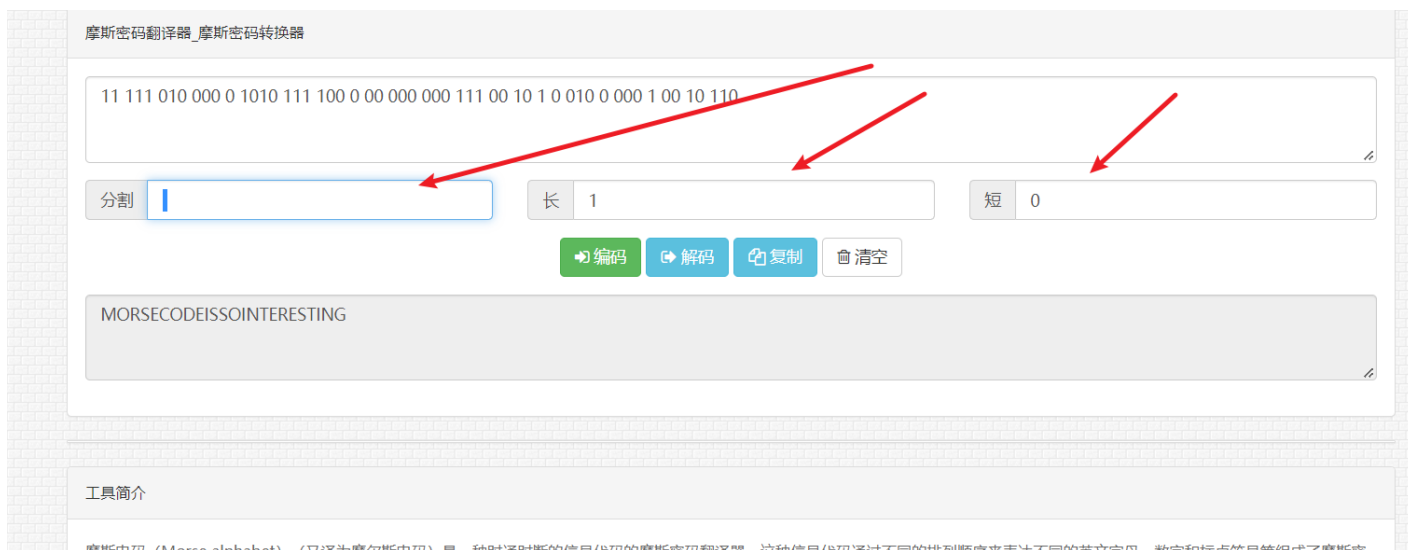
根据flag格式，cyberpeace开头的就是flag了

三. Morse

下载附件打开



根据题目提示，这串编码应该就是摩斯电码（Morse Code），只是把原有的.和_换成了1根0，找一下在线工具 [摩斯电码转换_摩斯密码翻译器-在线工具 \(all-tool.cn\)](#)



分别设置好后开始解码，然后再把解码后的大写字母换成小写字母，裹上flag的格式就是flag了

四. 幂数加密

根据提示，先百度一下幂数加密法

二进制数除了0和1的表示方法外，在由二进制转换成十进制的时候，还可以表示成2的N次方的形式。例如：

$$15=2^0+2^1+2^2+2^3$$

并且我们发现，任意的十进制数都可以用 2^n 或 $2^n+2^m+\dots$ 的形式表示出来，可以表示的单元数由使用的max n来决定。

$$\text{可表示的单元数}=2^{(n+1)}-1$$

二进制幂数加密法就是应用这个原理，由于英文字母只有26个字母，由公式可知，只要2的0、1、2、3、4、5次幂就可以表示31个单元。通过用二进制幂数表示字母序号数来加密。例如

明文: donotpullyoureggsinonebasket

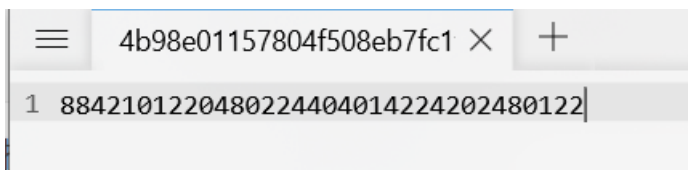
字母序号: 4 15 14 15 20 16 21 12 12 1 12 12 25 15 21 18 5 7 7 19 9 14 15 14 5 2 1 19 11 5 20

由于 $4=2^2$ 所以D加密之后是2; $15=2^0+2^1+2^2+2^3$ 所以O加密后是0123。同理得到上述明文的加密后的密文

密文: 2 0123/123 0123 24/4 024 23 23/0 23 23/034 0123 024 14/02 012 012 014/03 123 /0123 123 02/1 0 014 013 02 24

其中空格表示字母的间隔，/表示单词的间隔。

看懂后，打开下载的附件



给了一串数码，应该就是二进制幂数加密了，就是看他们是怎么分段的了，通过观察可以发现，数字0非常有效的隔绝了八组数字，再根据题目提示flag包裹的是八位大写字母，所以考虑用0分隔，这样以来就有

```
8842101220480224404014224202480122
88421 122 48 2244 4 142242 248 122
```

可又对应

不上表，考虑到让他们各位数相加

```
1 8842101220480224404014224202480122
2 88421 122 48 2244 4 142242 248 122
3 23 5 12 12 4 15 14 5
```

然后对应字母顺序，1代表A，4代表D，等

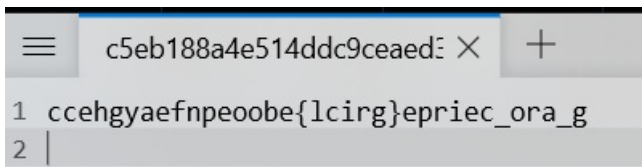
所有又有

```
1 8842101220480224404014224202480122
2 88421 122 48 2244 4 142242 248 122
3 23 5 12 12 4 15 14 5
4 W E L L D O N E
```

再根据提示，包裹上flag的提示得到flag，cyberpeace{WELLDONE}

五. Railfence

下载打开附件



根据题目描述

题目描述: 被小鱼一连将了两军，你心里更加不服气了。两个人一起继续往前走，一路上杂耍卖艺的很多，但是你俩毫无兴趣，直直的就冲着下一个谜題的地方去了。到了一看，这个谜面看起来就已经有点像答案的样子了，旁边还画着一张画，是一副农家小院的图画，上面画着一个农妇在栅栏里面喂5只小鸡，你嘿嘿一笑对着小鱼说这次可是我先找到答案了。

注意到关键词栅栏跟5，所以密文应该就是栅栏密码，复制到解码网站解码

转换前: x

ccehgyaefnpeoobe{lcirg}epriec_ora_g

栏目数: 5 删除待加密内容空格

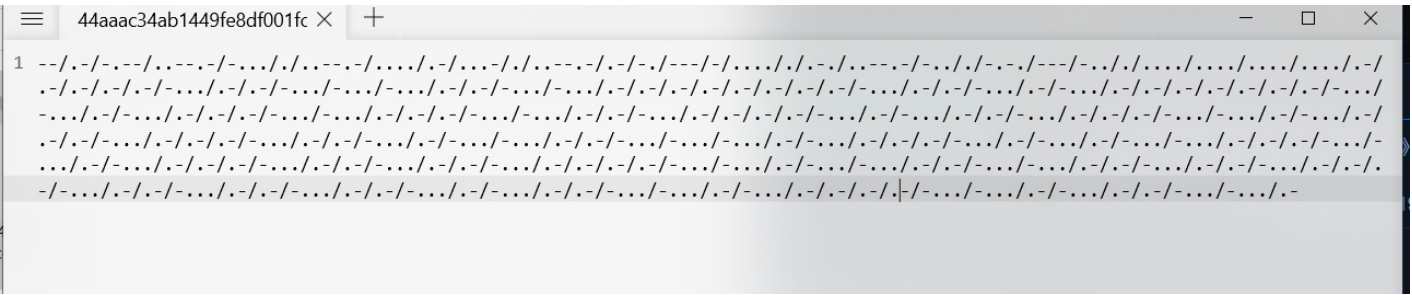
转换后:

cyberpeace{railfence_cipher_gogogo}

拿到flag

六. 不仅仅是Morse

下载打开附件



这一看就是摩斯密码，打开在线网站解码



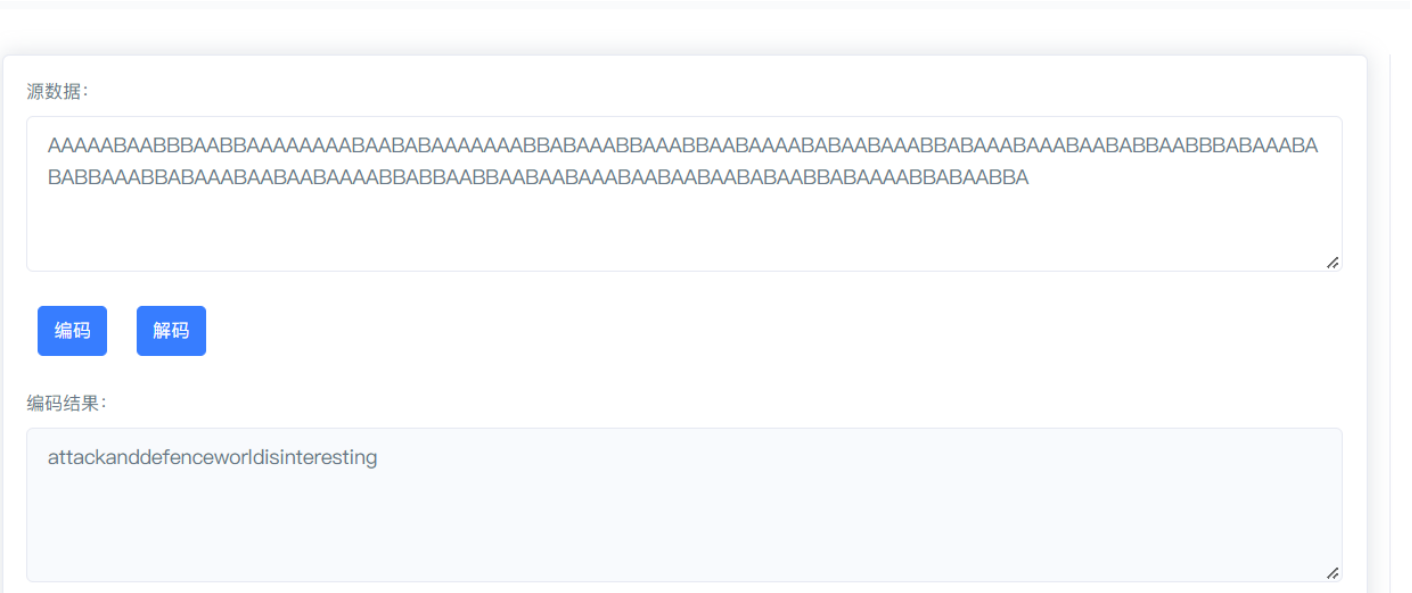
解码后有一串英文提示，也许存在其他编码，后面那串全是abab的，所以先百度一下ab在线解码，发现

培根密码 - Baconian Cipher - 在线工具网

<https://wtool.com.cn/baconian.html>

2020-11-27 · 培根密码以它的发明者弗朗西斯·培根爵士的名字命名。Baconian 密码是一个密码，其中每个字母被 5 个字符的序列替换。在原始密码中，这些是'A'和'B'的序列，例如字...

题目也提示了一种食物，所以把只含有AB的编码复制进去解密看看



没想到居然解密成功了，接着裹上flag的形式就拿到flag了