【CTF技巧总结】CRYPTO1

原创

LIU_Jessica 于 2020-01-13 15:15:55 发布 1479 收藏 5

分类专栏： CTF

本文链接：https://blog.csdn.net/weixin_45685619/article/details/103952263

攻防世界篇

---

1. base64

题目描述

元宵节灯谜是一种古老的传统民间观灯猜谜的习俗。 因为谜语能启迪智慧又饶有兴趣，灯谜增添节日气氛，是一项很有趣的活动。 你也很喜欢这个游戏，这不，今年元宵节，心里有个黑客梦的你，约上你青梅竹马的好伙伴小鱼， 来到了cyberpeace的攻防世界猜谜大会，也想着一展身手。 你们一起来到了小孩子叽叽喳喳吵吵闹闹的地方，你俩抬头一看，上面的大红灯笼上写着一些奇奇怪怪的 字符串，小鱼正纳闷呢，你神秘一笑，我知道这是什么了。

附件

```
Y3liZXJwZWFjZXtXZWxjb21lX3RvX25ld19Xb3JsZCF9
```

解题思路

由题目的名字可知，本题是base64使用的引出题目

百度搜索base64在线解密就可以获得解密后的答案

博主使用的网站是https://base64.supfree.net/

**由此我们可以了解一下

---

base64的相关特性

首先，Base64算不上是一种加密算法。

Base64是网络上最常见的用于传输8Bit字节代码的编码方式之一，它的目的是用ASCII中**定义的可见字符去表示任意的二进制数据**。之所以要这样做，是因为计算机中很多数据是只能通过可见字符去传输的（比如我们的网站网址，比如一些面向字符的网络协议如SMTP等），但是这些情景有时由需要去**传输二进制数据**。基于这样的需要，诞生了Base64.

简单来讲，Base64就是用下列总计64个字符：A-Z、a-z、0-9、+、/

去表示二进制数据。二进制数据以字节为组，一个字节8bit存在256个状态，而一个Base64字符只有64个状态。机智的人们于是规定，用每4个Base64字符去表示3个二进制字节，因为：
64 * 64 * 64 * 64 = 256 * 256 * 256

因此，Base64字符串的长度必然是4的整数倍。此外，由于二进制的字节数不一定是3的整数倍，所以Base64字符串在结尾是可能有空的。这些空的状态，Base64引入第65个字符去表示：

所以很多的base64代码都是以=或者==结尾，为了编码的二进制字节数恰好被3给整除。

总结

一般情况下，一个合法的Base64，有着以下特征：字符串的长度为4的整数倍。

字符串的符号取值只能在A-Z, a-z, 0-9, +, /, =共计65个字符中，且=如果出现就必须在结尾出现。

答案

```
cyberpeace{Welcome_to_new_World!}
```

引用来源

---

https://zhidao.baidu.com/question/1706399918245898220.html

2.Caesar

题目描述

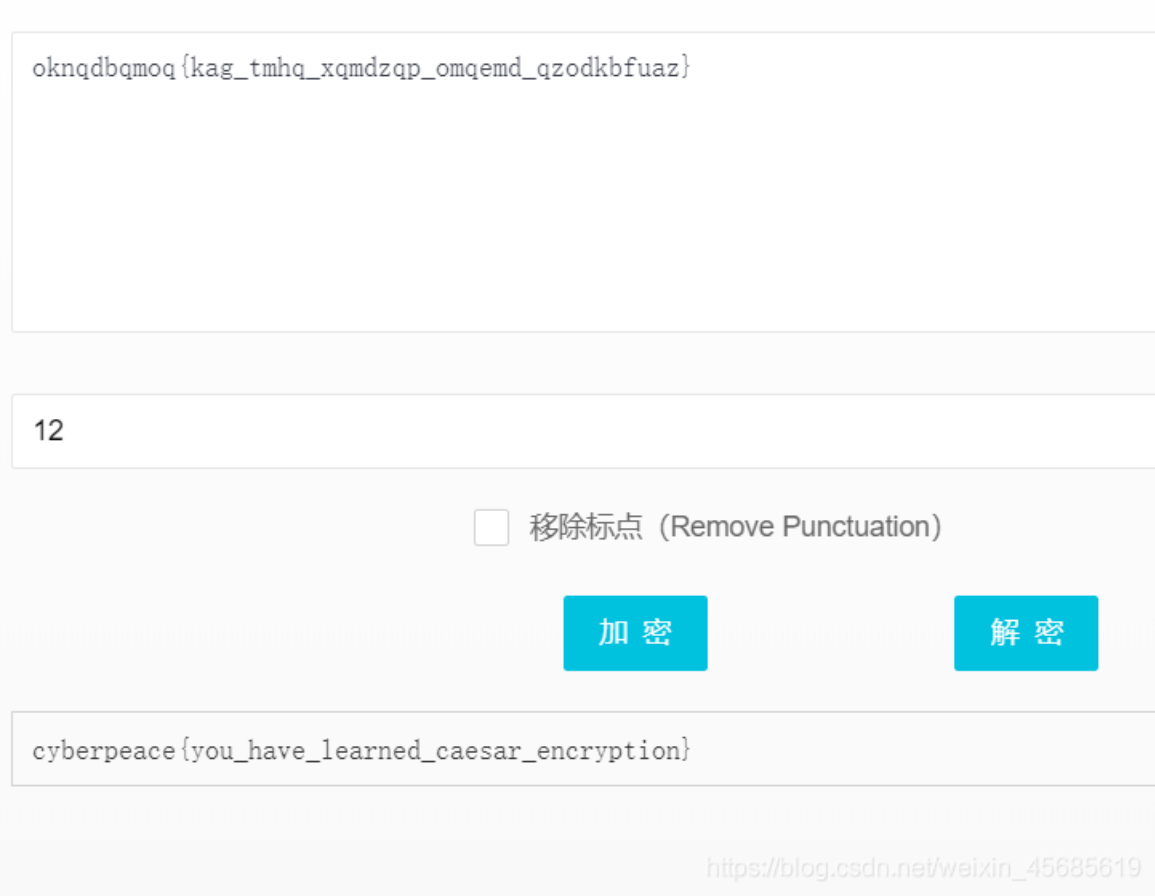
你成功的解出了来了灯谜，小鱼一脸的意想不到“没想到你懂得这么多啊！”你心里面有点小得意，“那可不是，论学习我没你成绩好轮别的我知道的可不比你少，走我们去看看下一个”你们继续走，看到前面也是热热闹闹的，同样的大红灯笼高高挂起，旁边呢好多人叽叽喳喳说个不停。你一看 大灯笼，上面还是一对字符，你正冥思苦想呢，小鱼神秘一笑，对你说道，我知道这个的答案是什么了

附件

```
oknqdbqmoq{kag_tmhq_xqmdzqp_omqemd_qzodkbfuaz}
```

解题思路

凯撒密码就是对原有密码的字母按照密钥进行平移，由于一共有26个英文字，故总共有26种密钥（0~25），我们可以采取暴力破解的方式，对26种密钥进行各自的检验。但是此处由于开始的字母为o，而我们的答案格式开始字母应该为c，因此，我们猜测密钥为12，经过检验实现猜想，采取在线凯撒密码破解的方式得到最终的答案。



!

博主所用的在线转换网址：http://www.nicetool.net/app/caesar.html

凯撒密码的相关特性详细叙述

在密码学中，恺撒密码（英语：Caesar cipher），或称恺撒加密、恺撒变换、变换加密，是一种最简单且最广为人知的加密技术。它是一种替换加密的技术，明文中的所有字母都在字母表上向后（或向前）按照一个固定数目进行偏移后被替换成密文。例如，当偏移量是3的时候，所有的字母A将被替换成D，B变成E，以此类推。
根据偏移量的不同，还存在若干特定的恺撒密码名称：
偏移量为10：Avocat(A→K)
偏移量为13：ROT13
偏移量为-5：Cassis (K 6)
偏移量为-6：Cassette (K 7)
恺撒密码的替换方法是通过排列明文和密文字母表，密文字母表示通过将明文字母表向左或向右移动一个固定数目的位置。例如，当偏移量是左移3的时候（解密时的密钥就是3）：
明文字母表：ABCDEFGHIJKLMNOPQRSTUVWXYZ；
密文字母表：DEFGHIJKLMNOPQRSTUVWXYZABC。

答案

```
cyberpeace{you_have_learned_caesar_encryption}
```

引用来源

https://baike.baidu.com/item/%E6%81%BA%E6%92%92%E5%AF%86%E7%A0%81/4905284?fromtitle=%E5%87%AF%E6%92%92%E5%AF%86%E7%A0%81&fromid=1336345&fr=aladdin
https://blog.csdn.net/chengqiuming/article/details/82077723

3.Morse

题目描述

小鱼得意的瞟了你一眼，神神气气的拿走了答对谜语的奖励，你心里暗暗较劲 想着下一个谜题一定要比小鱼更快的解出来。不知不觉你们走到了下一个谜题的地方，这个地方有些奇怪。 上面没什么提示信息，只是刻着一些0和1，感觉有着一些奇怪的规律，你觉得有些熟悉，但是就是想不起来 这些01代表着什么意思。一旁的小鱼看你眉头紧锁的样子，扑哧一笑，对你讲“不好意思我又猜到答案了。”(flag格式为cyberpeace{xxxxxxxxxx},均为小写)

附件

```
11 111 010 000 0 1010 111 100 0 00 000 000 111 00 10 1 0 010 0 000 1 00 10 110
```

解题思路

题目中仅有两个符号，可以知道很可能是摩尔斯电码的表示形式，将1改成'-'，将0改成'.' 然后将数字间的空格变成/ 借助在线转换工具可以将他们转换。
（有的网站可以直接指定空格，长，短的符号，就可以直接输入再输出）

博主用的是http://www.all-tool.cn/Tools/morse/?&rand=1ff7bfeba41520628987802b81d161c6

转换后得

```
MORSECODEISSOINTERESTING
```

由题意可知，所需答案应都为小写，再转换一下即可

摩尔斯电码介绍

摩尔斯电码（又译为摩斯密码，Morse code）是一种时通时断的信号代码，通过不同的排列顺序来表达不同的英文字母、数字和标点符号。

答案

```
cyberpeace{morsecodeissointeresting}
```

引用来源

---

https://baike.baidu.com/item/%E6%91%A9%E5%B0%94%E6%96%AF%E7%94%B5%E7%A0%81/1527853?fr=aladdin

4.混合编码

题目描述

经过了前面那么多题目的历练，耐心细致在解题当中是 必不可少的品质，刚巧你们都有，你和小鱼越来越入迷。那么走向了下一个题目，这个题目好长 好长，你知道你们只要细心细致，答案总会被你们做出来的，你们开始慢慢的尝试，慢慢的猜想 ，功夫不负有心人，在你们耐心的一步步的解答下，答案跃然纸上，你俩默契一笑，相视击掌 走向了下面的挑战。格式为cyberpeace{小写的你解出的答案}

附件

```
JiM3NjsmIzEyMjsmIzY5OyYjMTIwOyYjNzk7JiM4MzsmIzU2OyYjMTIwOyYjNzc7JiM2ODsmIzY5OyYjMTE4OyYjNzc7JiM4NDsmIzY1OyYjNTI7
JiM3NjsmIzEyMjsmIzEwNzsmIzUzOyYjNzY7JiMxMjI7JiM2OTsmIzEyMDsmIzc3OyYjODM7JiM1NjsmIzEyMDsmIzc3OyYjNjg7JiMxMDc7JiMx
MTg7JiM3NzsmIzg0OyYjNjU7JiMxMjA7JiM3NjsmIzEyMjsmIzY5OyYjMTIwOyYjNzg7JiM1NjsmIzEyMDsmIzc3OyYjODQ7JiM2OTsmIzExODsm
IzExODsmIzc5OyYjODQ7JiM5OTsmIzExODsmIzc3OyYjODQ7JiM2OTsmIzUwOyYjNzY7JiMxMjI7JiM2OTsmIzEyMDsmIzc4OyYjNTY7JiM1Nzsm
IzExODsmIzc4OyYjODM7JiM5OTsmIzExODsmIzc3OyYjODQ7JiM2OTsmIzEyMDsmIzc4OyYjNTY7JiM1MzsmIzc4OyYjNTA7JiM5OTsmIzExODsm
IzExOTsmIzc3OyYjNzM7JiM2OTsmIzEyMDsmIzc2OyYjMTIyOyYjNjk7JiMxMTk7JiM3NzsmIzY3OyYjNTY7JiMxMjA7JiM3NzsmIzY4OyYjMTAz
OyYjNTY7JiMxMjA7JiM3NzsmIzY4OyYjMTAzOyYjMTE4OyYjNzc7JiM4NDsmIzY1OyYjNTY7JiMxMjA7JiM3NzsmIzY4OyYjMTE5Ow==
```

解题思路

由结尾的两个==，我们可以知第一重解密应该是从base64开始。
利用上面给出的网址工具，我们可以得

```
&#76;&#122;&#69;&#120;&#79;&#83;&#56;&#120;&#77;&#68;&#69;&#118;&#77;&#84;&#65;&#52;&#76;&#122;&#107;&#53;&#76;&
#122;&#69;&#120;&#77;&#83;&#56;&#120;&#77;&#68;&#107;&#118;&#77;&#84;&#65;&#120;&#76;&#122;&#69;&#120;&#78;&#105
;&#56;&#120;&#77;&#84;&#69;&#118;&#79;&#84;&#99;&#118;&#77;&#84;&#69;&#50;&#76;&#122;&#69;&#120;&#78;&#105;&#56;
&#53;&#78;&#121;&#56;&#53;&#79;&#83;&#56;&#120;&#77;&#68;&#99;&#118;&#79;&#84;&#99;&#118;&#77;&#84;&#69;&#119;&#
76;&#122;&#69;&#119;&#77;&#67;&#56;&#120;&#77;&#68;&#65;&#118;&#77;&#84;&#65;&#120;&#76;&#122;&#69;&#119;&#77;&#
105;&#56;&#120;&#77;&#68;&#69;&#118;&#77;&#84;&#69;&#119;&#76;&#122;&#107;&#53;&#76;&#122;&#69;&#119;&#77;&#83;&
#56;&#120;&#77;&#84;&#107;&#118;&#77;&#84;&#69;&#120;&#76;&#122;&#69;&#120;&#78;&#67;&#56;&#120;&#77;&#68;&#103;
&#118;&#77;&#84;&#65;&#119;
```

由上面特殊得代码形式，我们可以认识一种新的加密形式 **Unicode**
这种加密形式的特点，后面会进行介绍
由Unicode的在线转换工具（博主用的http://tool.chinaz.com/Tools/Unicode.aspx）
我们可以得unicode码转换为ASCII的代码

```
LzExOS8xMDEvMTA4Lzk5LzExMS8xMDkvMTAxLzExNi8xMTEvOTcvMTE2LzExNi85Ny85OS8xMDcvOTcvMTEwLzEwMC8xMDAvMTAxLzEwMi8xMDEv
MTEwLzk5LzEwMS8xMTkvMTExLzExNC8xMDgvMTAw
```

最后再进行一次base64的转换，可得

```
/119/101/108/99/111/109/101/116/111/97/116/116/97/99/107/97/110/100/100/101/102/101/110/99/101/119/111/114/108/1
00
```

我们可知，将次ASCII码转换为字母即可。
这个没什么捷径了，我是对照ASCII码的表格挨个对照找出的。

Unicode介绍

---

https://blog.csdn.net/hezh1994/article/details/78899683这一篇文章讲的很详细，希望一起参考学习。

答案

```
cyberpeace{welcometoattackanddefenceworld}
```

5.Railfence

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题的地方去了。 到了一看，这个谜面看起来就已经有点像答案了样子了，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。

附件

```
ccehgyaefnpeoobe{lcirg}epriec_ora_g
```

解题思路

由题目我们可知这是栅栏密码的形式，经过尝试后发现这是WWW型的栅栏密码形式，由在线转换工具得(博主所用为http://www.atoolbox.net/Tool.php?Id=777)

栅栏密码介绍

https://blog.csdn.net/qinying001/article/details/96134356

答案

```
cyberpeace{railfence_cipher_gogogo}
```

7.不仅仅是Morse

题目描述

“这个题目和我们刚刚做的那个好像啊但是为什么按照刚刚的方法做出来答案却不对呢”，你奇怪的问了问小鱼，“可能是因为还有一些奇怪的加密方式在里面吧，我们在仔细观察观察”。两个人 安安静静的坐下来开始思考，很耐心的把自己可以想到的加密方式一种种的过了一遍，十多分钟后两个人 异口同声的说“我想到了！”。一种食物,格式为cyberpeace{小写的你解出的答案}

附件

解题思路

长得就很摩尔斯！先进行摩尔斯电码转化，可得

```
MAY_BE_HAVE_ANOTHER_DECODEHHHHAAAAABAABBBAABBAAAAAAAAABAABABAAAAAAAABBABAAABBAAABBAABAAAABABAABAAABBABAAABAAABAABA
BBAABBBABAAABABABBAAABBABAAABAABAABAAAABBABBAABBAABAABAAAABAABAABABAABBABAAAABBABAABBA
```

解出来之后竟然还得到了嘲笑还哈哈哈
我们提取出来可用得部分 是

```
AAAAABAABBBAABBAAAAAAAAABAABABAAAAAAAABBABAAABBAAABBAABAAAABABAABAAABBABAAABAAABAABABBAABBBABAAABABABBAAABBABAAABA
ABAABAAAABBABBAABBAABAABAAABAABAABABAABBABAAAABBABAABBA
```

然后就引入了一种新得解密方法 培根密码
具体介绍附在后面了
经过在线转换工具（https://tool.bugku.com/peigen/）这个工具带着大写小写都有的结果，爱了!

培根密码介绍

培根密码实际上就是一种替换密码，根据所给表一一对应转换即可加密解密 。它的特殊之处在于：可以通过不明显的特征来隐藏密码信息，比如大小写、正斜体等，只要两个不同的属性，密码即可隐藏。
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。
以下一段包含了'steganography'，正常字体是A，粗体是B：
To encode**a**message **e**ach letteroft**hepl**aintextis replaced by **a gr**oup of fiveofthe letters'A'or 'B'.

答案

```
cyberpeace{attackanddefenceworldisinteresting}
```

9.幂数加密

题目描述

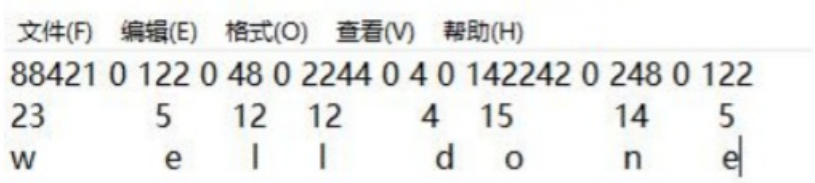
你和小鱼终于走到了最后的一个谜题所在的地方，上面写着一段话“亲爱的朋友， 很开心你对网络安全有这么大的兴趣，希望你一直坚持下去，不要放弃 ，学到一些知识， 走进广阔的安全大世界”，你和小鱼接过谜题，开始了耐心细致的解答。flag为cyberpeace{你解答出的八位大写字母}

附件

```
884210122048022440401422420248012 2
```

解题思路

由0做分割，是云影密码的形式
云影的基本形式就是将各个零相隔得部分相加
最后对照ASCII码得出最终得结果



云影密码简介

我的个人理解就是以2的n次幂的各个数加和的形式表示出各个数，然后用这些数字加和的形式对应各个字母或者符号的ASCII码，最终得到最终的结果

答案

```
cyberpeace{WELLDONE}
```

引用来源

https://adworld.xctf.org.cn/task/writeup?type=crypto&id=5120&number=5&grade=0&page=1