CTF初学——攻防世界crypto新手练习区

原创

Sandra的三脚猫功夫 于 2021-08-04 10:02:28 发布 291 收藏 2
文章标签： 信息安全 密码学

目录

前言：本菜鸟是0基础初学，边学边记，文中若有不对的地方还请各位大佬不吝赐教。٩('ω')و

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。

解析：

根据题目可知这是一道base64解密加密的问题，直接使用在线解码工具，将下载的附件内容复制上去即可解码

答案：cyberpeace{Welcome_to_new_World!}

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

解析：

根据题目可知这是一道凯撒密码，由第一题可知，flag的格式为cyberpeace{}，下载本题附件后发现，格式好像有点相似，于是采取一一对应原则，将 oknqdbqmoq 和 cyberpeace 比对，发现字母偏移12位，于是，使用凯撒密码在线工具解密可得flag。

答案：cyberpeace{you_have_learned_caesar_encryption}

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{xxxxxxxxx},均为小写)

解析：

根据题目可知，这是一道摩斯密码，下载附件后，复制粘贴去解密，发现不符合格式，才反应过来摩斯密码是由-和.组成的，于是，我们将 1 用 - 替代，将 0 用 . 替代，将 空格 用 / 替代可得（我看其他wp好像没换空格，但我不换它就解不出来，很奇怪诶，难道是我人品不够好吗"(￣(エ)￣)ゞ）

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

使用在线摩斯密码解密工具即可得到flag 的内容，根据题目要求，将其转化为小写即可。

答案：cyberpeace{morsecodeissointeresting}

4.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}

解析：

下载附件后发现这串数字里好像只有0 1 2 4 8 这几个数字，百度之后发现原来这是云影密码，

原文作者链接：https://blog.csdn.net/syber_ko/article/details/103757533，截图如下

云影密码（01248码）

这种加密方式仅使用01248这5种数字来进行，其中0用来唯一表示间隔，其他数字用加法和表示替换密文。再使用数字1~26表示字母A~Z。
如：18 = 1+8 = 9 = I，1248 = 1+2+4+8 = 15 = O

特点：密文中仅存在01248,加密对象仅有字母

例：CRYPTO001
88421 0122 048 02244 04 0142242 0248 0122
23 5 12 12 4 15 14 5
W E L L D O N E
可知falg为WELLDONE

答案：cyberpeace{WELLDONE}

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。

解析：

由题目描述可知，这是栅栏密码，栏目数为5，使用栅栏密码在线工具解得flag

答案：cyberpeace{railfence_cipher_gogogo}

6.不仅仅是Morse

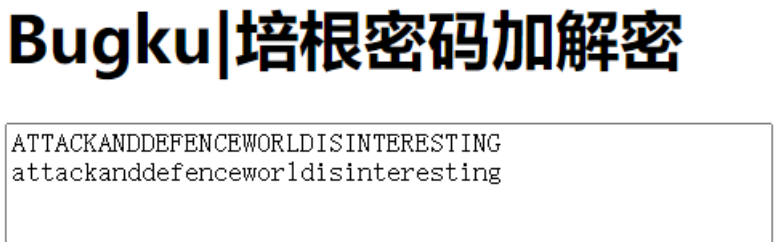
题目描述：“这个题目和我们刚刚做的那个好像啊但是为什么按照刚刚的方法做出来答案却不对呢”，你奇怪的问了问小鱼，“可能是因为还有一些奇怪的加密方式在里面吧，我们在仔细观察观察”。两个人 安安静静的坐下来开始思考，很耐心的把自己可以想到的加密方式一种种的过了一遍，十多分钟后两个人 异口同声的说“我想到了！”。一种食物,格式为cyberpeace{小写的你解出的答案}

解析：

看到附件内容，第一反应是摩斯密码，使用在线工具解得

MAY_BE_HAVE_ANOTHER_DECODEHHHHAAAAABAABBBAABBAAAAAAAAABAABABAAAAAAAABBABAAABBAAABBAABAAAABABAABAAABBABAAABAAABAABABBAABBBABAAABABABBAAABBABAAABAABAABAAAABBABBAABBAABAABAAABAABAABAABABAABBABAAAABBABAABBA

根据题目提示，“一种食物”加百度可以知道，它还有培根密码这种加密，于是我们将后面的所有A和B（因为培根密只由a和b组成）复制下来，使用大小写转换工具，转化为小写，再用培根密码在线工具解密可得flag。



答案：cyberpeace{attackanddefenceworldisinteresting}

7.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}

解析：

下载附件后，看到后缀是==，反应base64,在线工具解码得到一堆奇奇怪怪的东西，百度之后知道是Unicode，于是我们又使用Unicode在线工具解码得到一串字符，虽然没有等号做后缀，但我们还是第一反应base64,解码得到一串用/分隔开的数字，发现它们都小于128，于是，ASCII码在线工具一个个输入数字解码得到flag，找了好久也没找到那种可以一下子把整个一串数字一步到位解出来的，如果有哪位大佬找到的话，记得分享一下哟~Thanks♪(･ω･)ﾉ

答案： cyberpeace{welcometoattackanddefenceworld}

8.easy_RSA

题目描述：解答出来了上一个题目的你现在可是春风得意，你们走向了下一个题目所处的地方 你一看这个题目傻眼了，这明明是一个数学题啊！！！可是你的数学并不好。扭头看向小鱼，小鱼哈哈一笑，让你在学校里面不好好听讲现在傻眼了吧~来我来！三下五除二，小鱼便把这个题目轻轻松松的搞定了。flag格式为cyberpeace{小写的你解出的答案}

解析：

由题目提示可知，这是一道RSA算法题，根据算法提示计算，可以得出flag

RSA算法的具体描述如下： [5]

（1）任意选取两个不同的大素数p和q计算乘积 $n=pq, \varphi(n)=(p-1)(q-1)$ [5]；

（2）任意选取一个大整数e，满足 $gcd(e, \varphi(n))=1$，整数e用做加密钥（注意：e的选取是很容易的，例如，所有大于p和q的素数都可用） [5]；

（3）确定的解密钥d，满足 $(de) mod \varphi(n)=1$，即 $de=k\varphi(n)+1, k \geq 1$ 是一个任意的整数；所以，若知道e和 $\varphi(n)$，则很容易计算出d [5]；

（4）公开整数n和e，秘密保存d [5]；

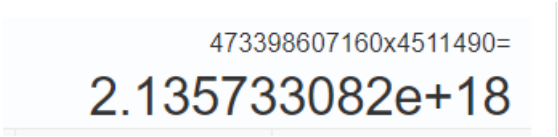
（5）将明文m（m<n是一个整数）加密成密文c，加密算法为 [5]

$$c=E(m)=m^e modn$$

（6）将密文c解密为明文m，解密算法为 [5]

$$m=D(c)=c^d modn$$

但是我用计算器算出来总是这样子的，请各位大佬指点一二（有的wp是用python脚本解的，别问，问就是还没学python）



答案：cyberpeace{125631357777427553}

9.easychallenge

题目描述：你们走到了一个冷冷清清的谜题前面，小鱼看着题目给的信息束手无策，丈二和尚摸不着头脑，你嘿嘿一笑，拿出来了你随身带着的笔记本电脑，噼里啪啦的敲起来了键盘，清晰的函数逻辑和流程出现在 了电脑屏幕上，你敲敲键盘，更改了几处地方，运行以后答案变出现在了电脑屏幕上。

解析：

下载附件后发现是.pyc，打不开，然后去瞅了一眼其他作者的wp，发现这个在线工具真的好好用，不用写一大串的代码，直接打开文件就可以解决

请选择pyc文件进行解密。支持所有Python版本

选择文件 未选择任何文件

```
def encode2(ans):
      s = ''
      for i in ans:
            x = ord(i) + 36
            x = x ^ 36
            s += chr(x)

      return s


def encode3(ans):
      return base64.b32encode(ans)

flag = ' '
print 'Please Input your flag:'
flag = raw_input()
final = 'UC7KOWVXWVNKNIC2XCXKHKK2W5NLBKNOUOSK3LNNVWW3E==='
if encode3(encode2(encode1(flag))) == final:
      print 'correct'
else:
      print 'wrong'
```


后面就有点玄乎了，有的说base64解密，有的说base32解密，然而我两种都试了一下，都没解出来o((⊙﹏⊙))o，然后我就懵圈了，有会的大佬麻烦教教孩子吧，谢谢！

答案：cyberpeace{interestinghhhhh}

10.转轮机加密

题目描述：你俩继续往前走，来到了前面的下一个关卡，这个铺面墙上写了好多奇奇怪怪的 英文字母，排列的的整整齐齐，店面前面还有一个大大的类似于土耳其旋转烤肉的架子，上面一圈圈的 也刻着很多英文字母，你是一个小历史迷，对于二战时候的历史刚好特别熟悉，一拍大腿：“嗨呀！我知道 是什么东西了！”。提示：托马斯·杰斐逊。 flag，是字符串，小写。

解析：

此题奉上大佬的解析：https://www.freesion.com/article/2154834489/#11

答案：fireinthehole

11.Normal_RSA

题目描述：你和小鱼走啊走走啊走，走到下一个题目一看你又一愣，怎么还是一个数学题啊 小鱼又一笑，hhhh数学在密码学里面很重要的！现在知道吃亏了吧！你哼一声不服气，我知道数学 很重要了！但是工具也很重要的，你看我拿工具把他解出来！你打开电脑折腾了一会还真的把答案 做了出来，小鱼有些吃惊，向你投过来一个赞叹的目光

解析：

还是奉上大佬的wp:

https://www.jianshu.com/p/c43776370840

https://blog.csdn.net/hippotomons/article/details/102672851

答案：PCTF{256b_i5_m3dium}

12.easy_ECC

题目描述：转眼两个人又走到了下一个谜题的地方，这又是一种经典的密码学加密方式 而你刚好没有这个的工具，你对小鱼说“小鱼我知道数学真的很重要了，有了工具只是方便我们使用 懂了原理才能做到，小鱼你教我一下这个缇努怎么做吧！”在小鱼的一步步带领下，你终于明白了ECC 的基本原理，成功的解开了这个题目，两个人相视一笑，快步走向了下一个题目所在的位置。flag格式为cyberpeace{x+y的值}

解析：

我是废物，老规矩，奉上大佬wp：https://blog.csdn.net/Ryannn_/article/details/102708011

答案：cyberpeace{19477226185390}