

ctf攻防世界crypto新手区

原创

[none-self](#) 于 2021-04-11 11:51:22 发布 169 收藏 1

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/weixin_53617146/article/details/115593437

版权

前言

之前的文章讲了几道MISC的题目，今天就讲一讲crypto
许多人再问crypto是什么，简单的来说就是密码学
多说不如来几道题目看看。

1.base64

下载附件后发现有一串字符串
Y3liZXJwZWJjZXtXZWxjb21lX3RvX25ld19Xb3JsZCF9
虽然后面没有等号，但是题目已经告诉我们是base64
不要犹豫，放到base64解码就能得到答案。

2.Caesar

下载后又得到一串字符。
oknqdbqmoq{kag_tmhq_xqmdzqp_omqemd_qzodkbfuaz}
这次题目又告诉我们的解密方式了，凯撒密码。
位移12即可

oknqdbqmoq{kag_tmhq_xqmdzqp_omqemd_qzodkbfuaz}

位移 12 加密 解密

cyberpeace{you_have_learned_caesar_encryption}

https://blog.csdn.net/weixin_53617146

3.Morse

下载附件后打开是一串摩斯密码，拿去解密即可

cyberpeace{morsecodeissointeresting}

用 · 表示0，-表示0
11 111 010 000 0 1010 111 100 0 00 000 000 111 00 10 1 0 010 0 000 1 00 10 110
m o r s e c o d e i s s o i n t e r e s t i n g
-> morsecodeissointeresting
cyberpeace{morsecodeissointeresting}

4.Railfence

下载附件打开得到

ccehgyaefnpeoobe{lcirg}epriec_ora_g

栅栏密码加密/解密

明文:	cyberpeace{railfence_cipher_gogogo}
-----	-------------------------------------

栏数:	5
-----	---

[加密](#) [解密](#)

密文:	ccehgyaefnpeoobe{lcirg}epriec_ora_g
-----	-------------------------------------

栅栏密码(Rail-fence Cipher)就是把要加密的明文分成N个一组，然后把每组的第1个字符组合，每组第2个字符组合...每组的第N(最后一个分组可能不足N个)个字符组合，最后把他们全部连接起来就是密文。

https://blog.csdn.net/weixin_53617146

5.幂数加密

首先base64解密

然后进行unicode编码转换

接着再进行一次base64解密

最后在ascii解密

加上格式Cyberpeace{welcometoattackanddefenceworld}