




第二届BMZCTF公开赛CRYPTO的签到

原创

沐一·林  于 2022-02-03 21:19:32 发布  236  收藏 1

分类专栏: [CTF 密码学](#) 文章标签: [ctf](#)

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/xiao__1bai/article/details/122778912

版权



[CTF 同时被 2 个专栏收录](#)

167 篇文章 6 订阅

订阅专栏



[密码学](#)

51 篇文章 1 订阅

订阅专栏

第二届BMZCTF公开赛CRYPTO的签到

打开附件发现一串密文:

```
56465a7757464977546d464e656b354b5632786b5346457862336c4f4d4842485632785a4d6c5a47556c46554d557057556a464e656c5a466146465756444135554651774f5642525054303d
```

直接用 ciphey 智能分析看看：

```
└─$ ciphey -t 56465a7757464977546d464e656b354b5632786b5346457862336c4f4d4842485632785a4d6c5a475
56c46554d557057556a464e656c5a466146465756444135554651774f5642525054303d
Possible plaintext: '56465a7757464977546d464e656b354b5632786b5346457862336c4f4d4842485632785a4d
6c5a47556c46554d557057556a464e656c5a466146465756444135554651774f5642525054303d' (y/N): n
Possible plaintext: '56465z7757464977546w464v656y354y5632786y5346457862336x4u4w4842485632785z4w
6x5z47556x46554w557057556z464v656x5z466146465756444135554651774u5642525054303w' (y/N): n
Possible plaintext: 'w3034505252465u477156455531444657564641664z5x656v464z655750755w45564x65574
z5x6w4z5872365842484w4u4x6332687546435y6872365y453y656v464w6457794647577z56465' (y/N): n
Possible plaintext: 'd3034505252465f477156455531444657564641664a5c656e464a655750755d45564c65574
a5c6d4a5872365842484d4f4c6332687546435b6872365b453b656e464d6457794647577a56465' (y/N): n
Possible plaintext: 'flag{Flag_Is_Nothing}' (y/N): y
```

```
The plaintext is a Capture The Flag (CTF) Flag
Formats used:
1 hexadecimal cypt_or_decrypt == "decrypt"
2 base64 data = base64.b64decode(data)
3 utf8 key = bytes(key1, encoding="utf8")
4 base64 enc = rc4cipher.new(key)
5 utf8 res = enc.decrypt(data)
6 base32
utf8Plaintext: "flag{Flag_Is_Nothing}"
```

CSDN @沐一·林

直接得到flag。

解毕！

敬礼！