

# 护网杯2020初赛 密码writeup

原创

syheliel 于 2020-10-28 08:45:10 发布 198 收藏

分类专栏: [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/qq\\_39642801/article/details/109325279](https://blog.csdn.net/qq_39642801/article/details/109325279)

版权



[CTF 专栏收录该内容](#)

7 篇文章 0 订阅

订阅专栏

## 2EM

$$tmp1 = pbox1(pt) \oplus nbox1(key) \quad tmp2 = nbox2(pbox1(pt)) \oplus nbox2(key) \oplus key$$

其中  $pbox2(pbox1(key)) \oplus nbox2(key) \oplus key$  在 key 不变时固定, 考虑用攻击 onetime-padding 的方式攻击该方案

## signsystemTask

代码审计后发现在传入明文, 返回签名的过程中没有对  $input \bmod N$ , 故可传入  $secret + k * N$  绕过对  $input == secret$  的比较, 从而获取 secret 的签名