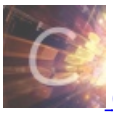
护网杯2020初赛 密码writeup

原创

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

分类专栏： CTF

本文链接：https://blog.csdn.net/qq_39642801/article/details/109325279



2EM

$tmp1 = pbox1(pt) \oplus pbox1(key) tmp2 = pbox2(pbox1(pt)) \oplus$

其中$pbox2(pbox1(key)) \oplus pbox2(key) \oplus key$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 mod N,故可传入secret + k*N绕过对input == secret 的比较，从而获取secret的签名