[hw0x0a] writeup

莊翔旭, woolninesun, b04902083

Yet_Another_Oracle

發現和 lab0x0a 差不多，只是回傳的 bits 數量變多，可以使用 LSB bytes Oracle Attack。

script 的 LSB_search 是想構造任意回傳 bits 數量都可以解的方法，也能夠用在 lab0x0a 上

ref: ctf wiki 選擇明密文攻擊 - rsa-byte-oracle