CTF HW11

b05902127 劉俊緯

Part 1

flag{--~~ *H0w I|v3 m1s5ed y0u* ~~--}

- 因為我們知道$m^{\phi} = 1$，而power function那邊多%n，因此就可以用這個方法和判斷是不是1來leak出給的power指數有沒有超過n。
- 接下來就是一般的二分搜。
- 但是這個時候會遇到一個小問題：就是powerfuncion因為RSA所以還會多%一個大N。
- 因此這個時候只要多乘一個倍率讓N不會影響到小n即可。