**郭又嘉**

**AosoraKuo**

**B06705020**

[**Mandalorian**](https://edu-ctf.csie.org/problems/40)

這題是一個進化版的LSB Oracle Attack

原本在上課教的是mod2的版本

而這題是mod16

不過我們還是可以慢慢地把數字越來越大的情況推上去

在2的時候是分成前半和後半

16的時候就是1/16, 2/16…

例如假設m落在[n/16, 2n/16]區間

我們可以推導出16m會落在[n, 2n]之間

然後就要%n%16

因為16m落在[n, 2n]區間

因此16m%n可以寫成16m – n

🡪(16m – n) % 16 🡪 -n % 16

當落在的區間越後面-n要乘的數就越大

而這個結果就是他回傳的值

所以我們可以就由他傳回來的推回去他原本落在哪個區間

也就是area\_start\_with

最後再將上下界透過迴圈縮在一起

最後就會得到一個數字

在將他轉成bytes就可以拿到FLAG了