計算機安全 HW2 Writeup

- Real name: 張瀚文
- Nickname on course website: Hwww
- Student ID: b07505027.

RSA

解法

這題的關鍵是 `n = p * q1 * q2` ，根據題目 `generate.py` ，猜測q1, q2的數量級大約與p相同，所以$n \approx 12p^3$，推估$p \approx \sqrt[3]{n} \approx 10^{154}$。把$n$看作$p$的函數$n(p)$，$n(p)$會是遞增的，所以試著二分搜$p$，手測一下，左界$l = 10^{154}$，右界$r = 2 * 10^{154}$，程式跑一下就搜出答案了
（見 `RSA/solve.py` ）

心得

這題剛開始不確定p, q1, q2會不會相近，也不確定next_prime會不會讓搜尋變很慢，剛開始就放棄暴搜，想找講義有沒有解法。後來找不到可用的解法，試試看暴搜，沒想到速度滿快的 ~

LSB

解法

這題跟講義上的LSB Oracle Attack 範例差不多，差別只在講義上的 oracle 是 mod 2，而這題的 oracle 是 mod 3，因此，修改一下推論，可得

$$
\begin{aligned}
&\lfloor \lfloor 3m \rfloor_n \rfloor_3 = \lfloor 3m \rfloor_3 = 0, && if\ m \in [0, n/3) \\
&\lfloor \lfloor 3m \rfloor_n \rfloor_3 = \lfloor 3m - n \rfloor_3 = 1, && if\ m \in [n/3, 2n/3) \\
&\lfloor \lfloor 3m \rfloor_n \rfloor_3 = \lfloor (3m - 2n) \rfloor_3 = 2, && if\ m \in [2n/3, n)
\end{aligned}
$$

程式碼為 `LSB/solve.py` ，主要是修改講義中GitHub上LSB範例程式碼，將2改成3，2倍改成3倍，結果的2種情況改成3種情況，調整一下LR即可。因為改成3後有些細節沒有調得很好，有機率會沒搜中，但多試幾次即可。

心得

因為這題跟講義上的類似，觀念也沒有特別難懂，所以很快就解出來了 ~