RSA 參數問題

- (A) 選擇 p 與 q 條件
  - n = p * q
  - 選擇條件：
    - p 與 q 的長度不要相差太多，兩者大小都應介於 10^{75} 到 10^{100} 之間。
    - (p-1) 與 (q-1) 都應該含有一個很大的質因數。
    - gcd(p-1, g-1) 的值，應該很小。
- (B) 選擇 e 與 d 的條件
  - {e, n} 為公開鑰匙
  - {d, n} 為私有鑰匙
  - 選擇因素： $ed \equiv 1 \bmod \psi(n)$
  - 選擇方式：
    - 先選擇 p 與 q，之後再選擇 e，但選擇 e 的條件是必須滿足與 (p-1)(q-1) 的質數關係。
    - 先選擇 e，之後再選擇 p 與 q，但選擇條件是必須滿足 e 與 (p-1)(q-1) 之間是質數的關係。
  - 一般採用先選 e，並固定為 3。

RSA 安全性

- 攻擊 RSA 演算法的方法
  - 暴力攻擊法
  - 數學攻擊法：因數分解法
- 因數分解攻擊法
  - 有三種攻擊法：
    - 將 n 分解成兩個質因數 p 與 q：如此便可以計算出 $\psi(n) = (p-1)(q-1)$，並且一般 e 都採用某一固定值（如 e =3），接著可以計算出 $d \equiv e^{-1} \bmod \psi(n)$。
    - 由 n 計算出 $\psi(n)$：不必先算出 p 和 q，可以尋找出 $d \equiv e^{-1} \bmod \psi(n)$。
    - 直接找出 d：不必先計算出 $\psi(n)$。