RSA 推論結果歸類

- 推論結果歸類
  - RSA 演算法相關參數
    - p 與 q 兩質數：自行選擇的私有值。
    - n=pq：計算而得的公開值。
    - 選擇 e，需滿足 gcd(ψ(n), e)=1；1 < e <ψ(n)：自選公開值。（一般都固定值 3 或其他數值）
    - 依 $ed \equiv 1 \bmod \psi(n)$ ；$d \equiv e^{-1} \bmod \psi(n)$：計算出私有值。
    - 公開鑰匙：$K_U = \{e, n\}$
    - 私有鑰匙：$K_D = \{d, n\}$

RSA 推論結果歸類

- 產生鑰匙範例假設參數：
  - 1. 選定兩個質數，p = 7、q = 17。
  - 2. 計算 n = pq = 7 × 17 = 119。
  - 3. 計算ψ(n) = (p-1) × (q-1) = 6 × 16 = 96。
  - 4. 選定 e，但必須滿足 gcd(e, ψ(n)) =1，則選擇 e =5，因與 96 互質。
  - 5. 選定 d，但必須滿足 de ≡1 mod 96，且 d < 96。
  - 則：d*5 ≡1 mod 96； d*5 = 1 + 96 *k，k=1, 2,3 …
  - 由 k=1, 2, 3, 4, .. 開啟測試， 當 k=4，d * 5 = 1 +96*4 = 1 + 384 = 385
    則d = 385/5 = 77，
  - 則 e * d = 77×5 = 385 ≡1 mod 96（385 除以 96，得到餘數為 1）。
  - 經過上述推演得到：
    - 公開鑰匙：K_U = {e, n} = {5, 119}
    - 私有鑰匙：K_R = {d, n} = {77, 119}