RSA 演算法－同餘指數

- Rivest、Shamir 與 Adleman 公同發表
- 定義：
  - 明文：M
  - 密文：C
  - 加密：$C \equiv M^e \bmod n$
  - 解密：$M \equiv C^d \bmod n \equiv (M^e)^d \bmod n \equiv M^{ed} \bmod n$
  - 公開鑰匙：$K_U = \{e, n\}$
  - 私有鑰匙：$K_D = \{d, n\}$
  - 尋找出適合的 n、e 與 d
  - 給定 e, n 很難推論出 d，反之亦然。

RSA 演算法推論

- **(A) 推論 $M \equiv M^{ed} \bmod n$**
  - **給予兩個質數 p 與 q，並 n = p*q**
  - **假設 m 與 n 成為互質， gcd(m, n) = 1**
  - **由 Euler 定理：**
    - $m^{\phi(n)+1} \equiv m \bmod n$
    - 依照： **Euler's Totient 定理**，$\phi(n)=(p-1)(q-1)$ 其中 $n = pq$ 則：
    - $m^{\phi(n)+1} = m^{(p-1)(q-1)+1} \equiv m \bmod n$
  - **如果：m 與 n 互質的話（gcd(m, n) = 1）則：**
    - **gcd(m, n) =1 表示 m 與 n 之間無法整除**
    - **但 n = pq，如果 m/n = m/pq 不可以整除的話，則 m/p 與 m/q 是否可以或無法整除。**
    - **假設兩個條件：**
      - **m = pc**，其中 **c** 為任何整數，p 可以整除 m。
      - **gcd(m, p)≠1 與 gcd(m, q) =1**。

RSA 演算法推論

- 其中 gcd(m, q) =1，表示 m 與 q 之間是互質的關係：
  - 依照 Euler 定理：$a^{\phi(n)} \equiv 1 \bmod n$，則：
  - $m^{\phi(q)} \equiv 1 \bmod q$ ； 雙邊取 $\phi(q)$次方
  - 利用同餘運算規則：

    $[m^{\psi(q)}]^{\psi(p)} \equiv [1 \bmod q\ ]^{\psi(p)}$

    $m^{\psi(p)\times\psi(q)} \equiv 1 \bmod q$

    $m^{(p-1)\times(q-1)} \equiv 1 \bmod q$； 又$\psi(n) = (p-1)\times(q-1)$ 則：

    $m^{\phi(n)} \equiv 1 \bmod q$
  - $m^{\phi(n)} = 1 + kq$
  - 如果等號雙邊各乘以 m，其中 m = cp 與 n = pq，則：
  - $m[m^{\phi(n)}] = m[\ 1 + kq\ ]$； m=cp
  - $m^{\phi(n)+1} = m + kcpq = m + kcn$； pq=n
  - 相當於：m 除以 n，而得到的商是 kc、餘數是 m，因此，可改寫成：
  - $m^{\phi(n)+1} \equiv m \bmod n$; $m^{\phi(n)} \equiv 1 \bmod n$
  - 再利用：$a^{\phi(n)} \equiv 1 \bmod n$ 推導出：
  - $[m^{\psi(n)}]^k \equiv 1 \bmod n$； 雙編取 k 次方
  - $m^{k\psi(n)} \equiv 1 \bmod n$; $m^* m^{k\psi(n)} \equiv m^*[1 \bmod n]$
  - $m^{k\phi(n)+1} = m^{k(p-1)(q-1)+1} \equiv m \bmod n$

- 又 n = pq，且 p 與 q 皆為質數

  $M^{k\psi(n)+1} \equiv M \bmod n$

  給定：

  $ed = k\psi(n) + 1$

  則：

  $M^{ed} \equiv M \bmod n$ ；得到推演結果

  於是：

  $ed \equiv 1 \bmod \psi(n)$

  $d \equiv e^{-1} \bmod \phi(n)$