# 同餘算數－指數

- 同餘指數 (Modular Exponentation)
  - 譬如 a =4、b=6、n=13，則運算程序如下：

    $a^b \bmod n = 4^6 \bmod 13 = 4096 \bmod 13 = 1$
  - 具有 $(a \bmod n)^b \bmod n = a^b \bmod n$ 特性
  - 0～9 之間 mod 10 的運算結果($x^y \bmod 10$)

| $x^y$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 1 | 2 | 4 | 8 | 6 | 2 | 4 | 8 | 6 | 2 |
| 3 | 1 | 3 | 9 | 7 | 1 | 3 | 9 | 7 | 1 | 3 |
| 4 | 1 | 4 | 6 | 4 | 6 | 4 | 6 | 4 | 6 | 4 |
| 5 | 1 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| 6 | 1 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| 7 | 1 | 7 | 9 | 3 | 1 | 7 | 9 | 3 | 1 | 7 |
| 8 | 1 | 8 | 4 | 2 | 6 | 8 | 4 | 2 | 6 | 8 |
| 9 | 1 | 9 | 1 | 9 | 1 | 9 | 1 | 9 | 1 | 9 |

# 同餘算數－指數

- 具有反向暗門特性
  - 加密與解密鑰匙關係 ：**{1, 3, 7, 9}**

    $y \times y^{-1} \bmod n \equiv 1$

| | | | | |
|---|---|---|---|---|
| •公開鑰匙 ($K_E$)： | •1 | •3 | •7 | •9 |
| •私有鑰匙 ($K_D$)： | •1 | •7 | •3 | •9 |

  - 範例：
    - P =8, $K_E$ = 3, $K_D$ = 7 , n=10
    - 加密：

      密文 $C = P^{Ke} \bmod n = 8^3 \bmod 10 \equiv 2 \bmod 10$；則密文為 2。
    - 解密：

      明文 $P = C^{Kd} \bmod n = 2^7 \bmod 10 \equiv 8 \bmod 10$；則明文為 8。