同餘算數- 乘法

- 同餘乘法 (Modular Multiplication)
  - 0 ~ 9 之間的同餘乘法 (modulo 10)
  - 假設 a = 8、b = 7、n=13，則運算程序如下：

    $(a \times b) \bmod n = (8 \times 7) \bmod 13 = 56 \bmod 13 = 4$
  - 具有：$((a \bmod n) \times (b \bmod n)) \bmod n = (a \times b) \bmod n$ 特性

×	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

同餘算數– 乘法

- 具有反向暗門特性
  - **0 ~ 9 之間的同餘乘法 (modulo 10)**
  - **適合的反向暗門：{1, 3, 7, 9}**
  - **K_E 與 K_D 互為反函數 (Y 與 Y^{-1})**
    - $y \times y^{-1} \bmod n \equiv 1$

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

- 加密與解密關係：範例
  - 參數：$K_E = 3$, $K_D = 7$, $M = 4$, $n=10$
  - 加密：

    $C = (K_E * M) \bmod n = (3* 4) \bmod 10 = 2$
  - 解密：

    $M' = (K_D * C) \bmod n = (7 *2) \bmod 10 = 4$

    = M