同餘算數－加法

- 同餘加法 (Modular Addition)
  - (a + b) mod n
  - 6+7≡3 或 13≡ 3 mod 10
  - 0 ~ 9 之間的同餘加法 (Modulo 10), n=10
  - 具有[(a mod n) + (b mod n)] mod n = (a + b) mod n
  - 驗證： [(48 mod 15) + (66 mod 15)] mod 15 = (48 + 66) mod 15
  - 左邊= [3+6]mod 15 = 9 右邊 = 114 mod 15 = 9

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

同餘算數－加法

- 具有反向暗門特性
  - $K_E + K_D = 10$
  - $(K_D + K_E) \bmod 10 \equiv 0$
  - $y + y^{-1} \bmod n \equiv 0$

公開鑰匙 (K_E)：	1	2	3	4	5	6	7	8	9
私有鑰匙 (K_D)：	9	8	7	6	5	4	3	2	1

- 驗證：
  - $K_E = 3$、$K_D = 7$、$(K_D + K_E) \bmod 10 \equiv 0$ 、 $n=10$
  - $M = 5$
  - 加密： $C = K_E + M = 3 + 5 = 8$
  - 解密：$M' = K_D + C = (7 + 8) \bmod n = 15 \bmod 10 = 5$
  - $M' = M$
  - 則 7 是 3 的反向按門。