亂數的應用與特性

- 亂數 (Random Number) 的應用
  - 產生通訊鑰匙
  - 演算法參數
  - 計數器
  - 交叉確認
- 『虛擬亂數』（Pseudo-random Number）的特性：
  - 隨機性
  - 不可預測性

典型亂數產生器

- 線性同餘法

  $X_{n+1} = (a X_n + c) \bmod m$

- 四個參數：

  m 模數（Modulos）：m > 0；最好是夠大的質數。

  a 乘數（Multiplier）：0 ≦ a ＜ m。

  c 增量（Increment）：0 ≦ c ＜ m。

  X_0 起始值，或稱種子（Seed）：0 ≦ X_0 ＜ m。

- 範例：m=13, a=2, c=1, X_0 = 1 則：
  - $X_1 = (aX_0 + c) \bmod 13 = (2*1 + 1) \bmod 13 = 3$
  - $X_2 = (aX_1 + c) \bmod 13 = (2*3 + 1) \bmod 13 = 7$
  - $X_3 = (aX_2 + c) \bmod 13 = (2*7 + 1) \bmod 13 = 2$
  - $X_4 = (aX_3 + c) \bmod 13 = (2*2 + 1) \bmod 13 = 5$
  - $X_5 = (aX_4 + c) \bmod 13 = (2*5 + 1) \bmod 13 = 11$
  - $X_6 = (aX_5 + c) \bmod 13 = (2*11 + 1) \bmod 13 = 10$
  - $X_7 = (aX_6 + c) \bmod 13 = (2*10 + 1) \bmod 13 = 8$
  - $X_8 = (aX_7 + c) \bmod 13 = (2*8 + 1) \bmod 13 = 4,$
  - $X_9 = (aX_8 + c) \bmod 13 = (2*4 + 1) \bmod 13 = 9, 6, 1, 3, 7, 2, \cdots.$

$C_{n+1} = (a C_n + k) \bmod m$