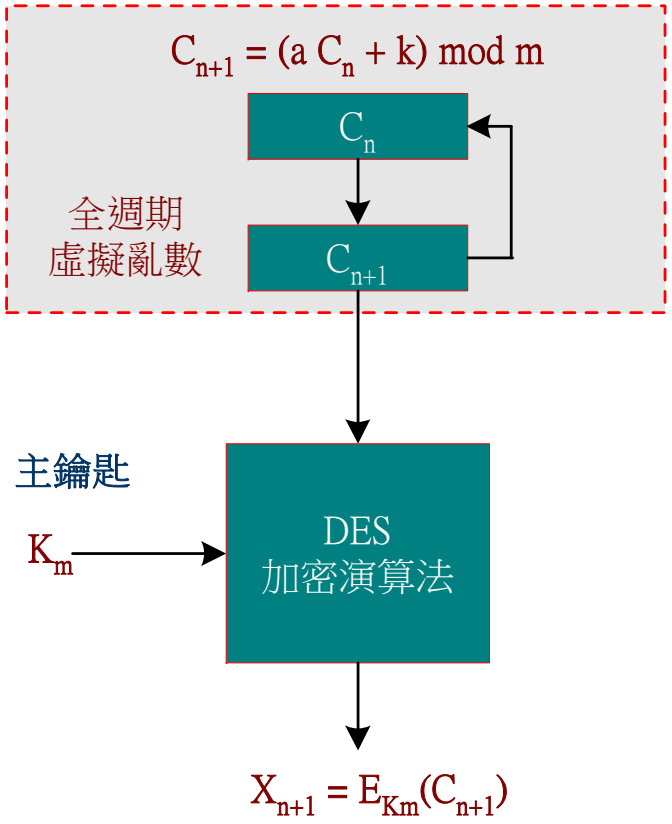
DES 亂數產生

- **DES 加密法的亂數產生**
  - 初始亂數：全週期虛擬亂數產生。
  - 採用 DES 演算法
  - 加密鑰匙的保護
- 全週期 (Full Period) 函數：

$$X_{n+1} = (a\ X_n + c) \bmod 2^{32}-1$$



ANSI 亂數產生

- **ANSI 亂數產生**
  - ANSI X9.17 標準
  - 採用 3DES 演算法
  - 輸入參數：日期/時間與上一次運算結果。
  - 加密鑰匙：112 bits 。
  - 亂數輸出：64 bits。
  - 演算法輸出：

$$R_i = 3DES_{K1||K2}\,[Vi \oplus 3DES_{K1||K2}\,[DT_i]]$$

$$V_{i+1} = 3DES_{K1||K2}\,[R_i \oplus 3DES_{K1||K2}\,[DT_i]]$$