數位資料加密原理 - 區塊加密

- 數位資料加密的做法：
  - 加密時：將明文分段加密後，再組合成密文序列。
    - $M = M_1 \| M_2 \| M_3 \cdots \| M_n$
    - 明文區塊依序進入加密器產生同樣大小的密文區塊。
    - 連結密文區塊成為加密後的密文。
    - $C = E_k(M) = E_k(M_1) \| E_k(M_2) \| \cdots \| E_k(M_n)$
  - 解密時：將密文分段解密後，再組合成明文序列。
- 基本演算法：
  - 乘積加密法 **(Product Ciphers)**
  - **Feistel** 加密法 。
- 傳統密碼系統的基礎。
  - 取代與換位加密法。
  - 加密器與解密器相同。

數位資料加密原理 - 區塊加密

- 運作程序：