MD5 訊息摘要

- **Message Digest (MD)**
  - **MIT 一系列雜湊演算法 (Ron Rivest 設計)**
  - **MD2 (RFC 1319) ：8 位元單晶片**
  - **MD4 (RFC 1320) ：32 位元/單晶片**
  - **MD5 (RFC 1321) ：32 位元主機**

MD5 運作原理

MD5 運作原理

- 區段演算：512 bits
- 雜湊值長度：128 bits
- 初始向量：128 bits