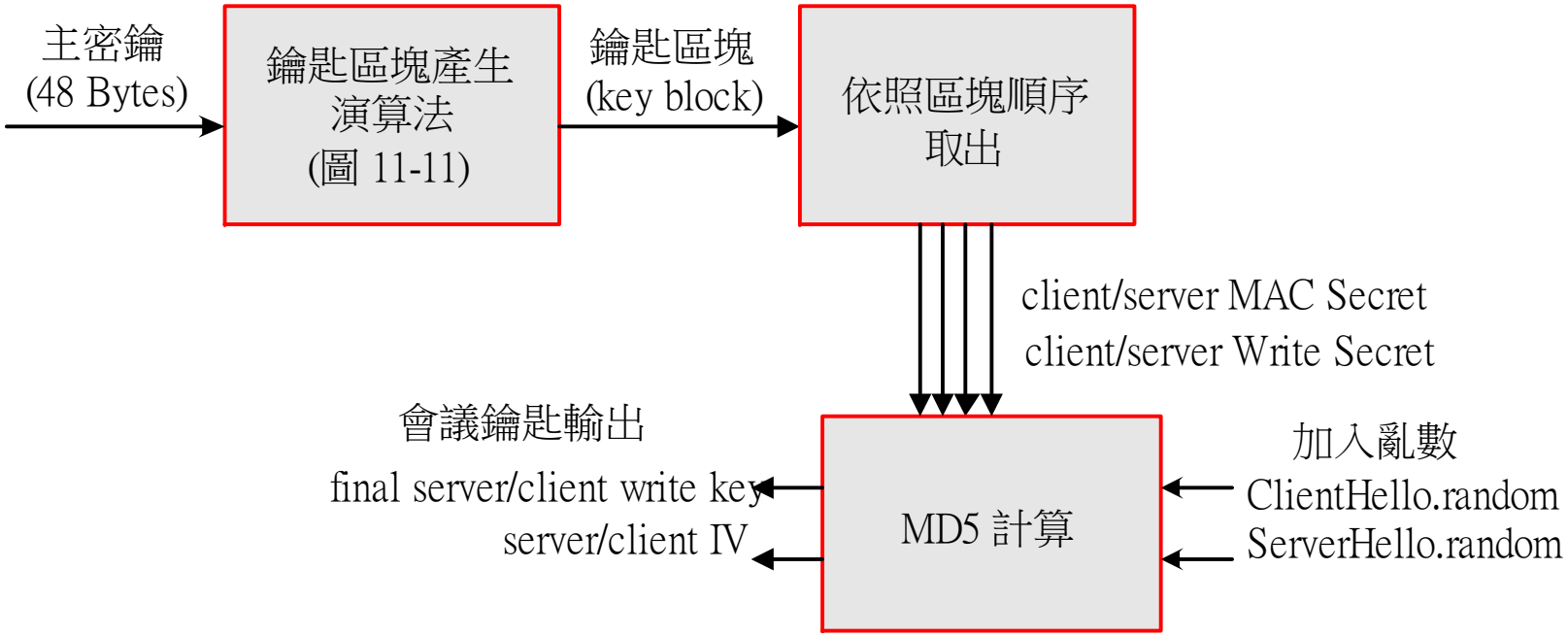
SSL 會議鑰匙的產生

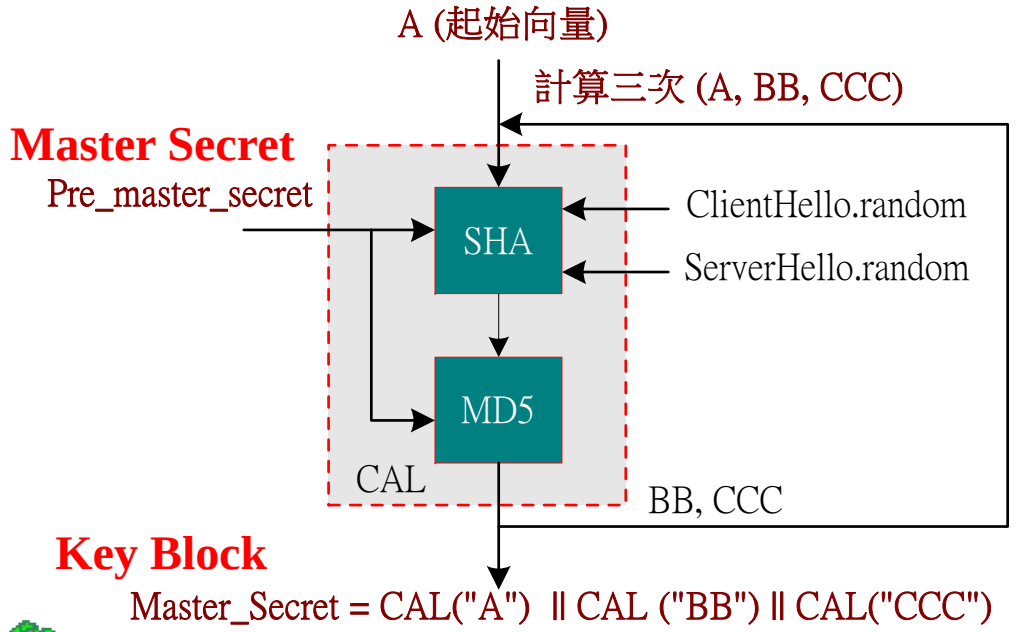
- 由『主密鑰』計算出各種『會議鑰匙』
- 計算步驟：



SSL 鑰匙區塊產生

- 鑰匙區塊 (Key Block) 計算

key_block = MD5(master_secret || SHA(“A”|| master_secret ||ClientHello.random || ServerHello.random)) ||MD5(master_secret || SHA(“BB”|| master_secret ||ClientHello.random || ServerHello.random)) ||MD5(pre_master_secret || SHA(“CCC”|| pre_master_secret || ClientHello.random || ServerHello.random)) || …..



SSL 計算相關鑰匙

- 加密套件的鑰匙參數：
  - client_write_MAC_secret [CipherSpec.hash_size]：客戶端計算 MAC 鑰匙的長度。
  - server_write_MAC_secret [CipherSpec.hash.size]：伺服端計算 MAC 鑰匙的長度。
  - client_write_secret [CipherSpec.key_material]：客戶端加密訊息鑰匙的長度。
  - server_write_secret [CipherSpec.key_material]：伺服端加密訊息鑰匙的長度。
- 計算相關鑰匙
  - 會議鑰匙：

    final_client_write_key = MD5(client_write_key || ClientHello.random || ServerHello.random)

    final_server_write_key = MD5(server_write_key || ServerHello.random || ClientHello.random)
  - CBC 加密套件 (含 IV)

    client_write_IV = MD5(ClientHello.random || ServerHello.random)

    server_write_IV = MD5(ServerHello.random || ClientHello.random)