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)

SSL 鑰匙產生範例

- 鑰匙產生範例
  - SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5
  - 選用鑰匙區塊的次序：

    client_write_MAC_secret = key_block[0,.., 15]   (128 bit)

    server_write_MAC_secret = key_block[16, …, 31]   (128 bit)

    client_write_key = key_block[32, …, 36]   (40 bit)

    server_write_key = key_block[37, …, 41]   (40 bit)
  - 加密鑰匙計算：

    final_client_write_key = MD5(client_write_key || ClientHello.random || ServerHello.random) [0. …, 15] (128 bit)

    final_server_write_key = MD5(server_write_key || ServerHello.random ||

    ClientHello.random) [0, …, 15] (128 bit)

    client_write_IV = MD5(ClientHello.random || ServerHello.random) [0, …, 7]

    server_write_IV = MD5(ServerHello.random || ClientHello.random) [0, …, 7]

    (64 bit)