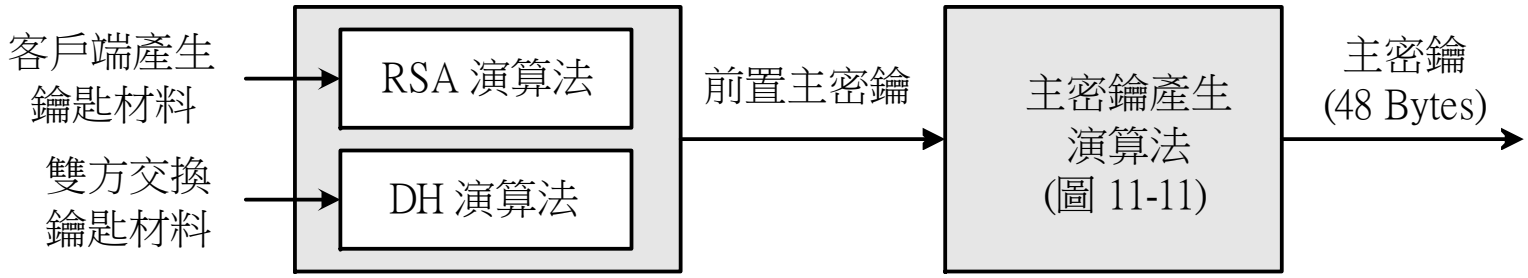
SSL 主密鑰的計算

- 由 **Pre-master Secret** 計算出 **Master Secret**



主密鑰的計算

- 計算公式：(各種演算法都相同)
  - Mster_secret = MD5(pre_master_secret || SHA(“A”|| pre_master_secret || ClientHello.random || ServerHello.random)) || MD5(pre_master_secret || SHA(“BB”|| pre_master_secret || ClientHello.random || ServerHello.random)) || MD5(pre_master_secret || SHA(“CCC”|| pre_master_secret || ClientHello.random || ServerHello.random))