Cryptographic Computations

Cryptographic Computations

- ‘Server hello message’ inform the cipher suite selected by the server
  - Key exchange
  - Authentication
  - Encryption
  - MAC algorithms
  - Compression algorithm
  - Random values are exchanged in the hello messages
- Shared master secret agreed on key exchange is used in the generation of cryptographic parameters

Computing the Master Secret

- Premaster secret is converted into the master secret
- Same algorithm is used to convert for all key exchange methods
- In order to create the master secret, a premaster secret is first exchanged between two parties and then the master secret is calculated from it.
- The master secret is always exactly 48 bytes (384 bits) shared between the client and server
- But the length of the premaster secret is not fixed and will vary depending on the key exchange method
- There are two ways for the exchange of the premaster secret:
  - *RSA (private key public key)*
  - *Diffie–Hellman (Discrete logarithmic principles)*

Computing the Master Secret

- The client and server then compute the master secret as follows:

```
master_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))
```

Computing the Master Secret

ClientHello.random and ServerHello.random are the two nonce values exchanged in the initial hello messages

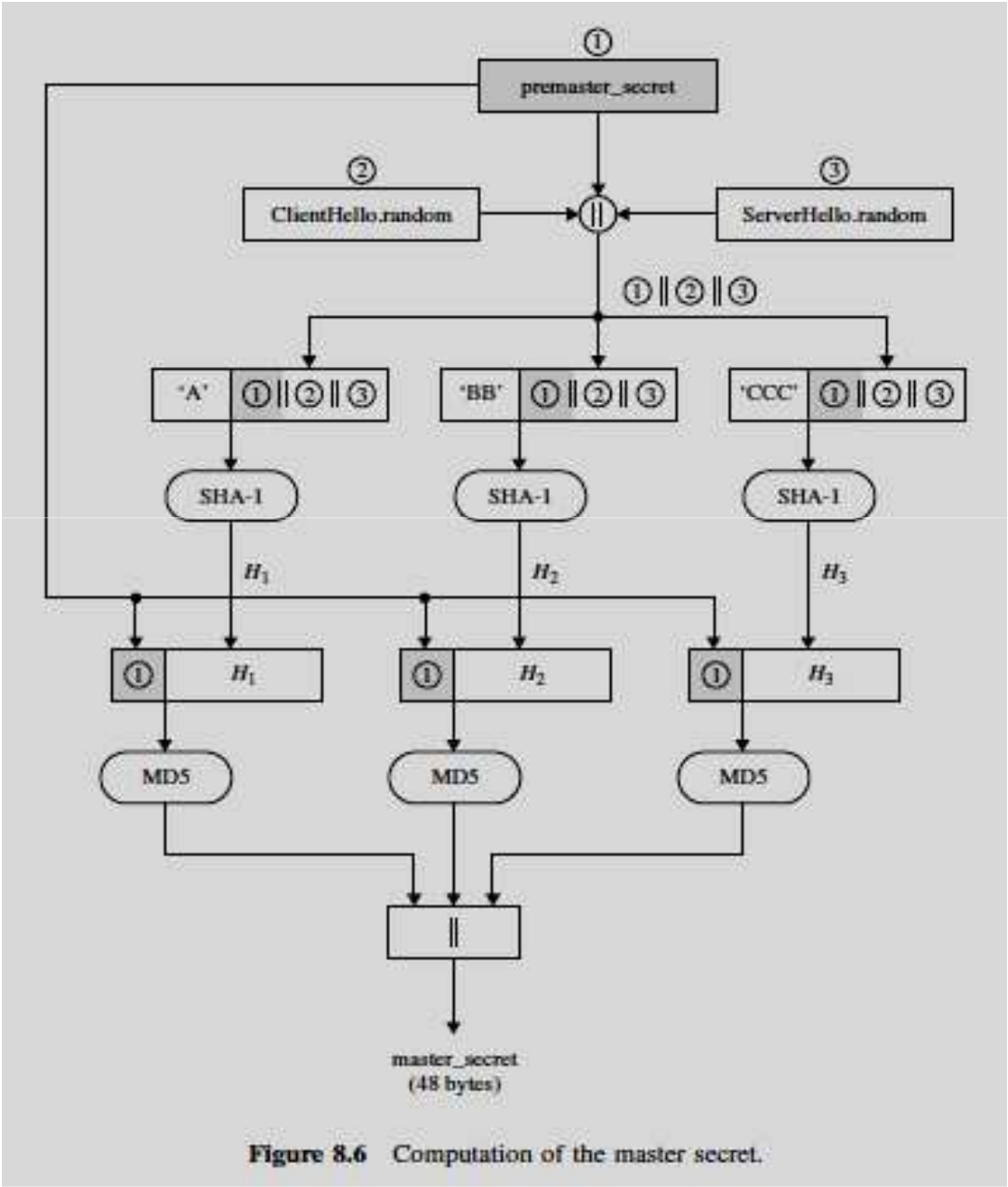

Figure 8.6 Computation of the master secret.

Converting the Master Secret into Cryptographic Parameters

- CipherSpec specifies the bulk data encryption algorithm and a hash algorithm used for MAC computation, and defines cryptographic attributes such as the hash size
- Note that the generation of the key block from the master secret uses the same format for generation of the master secret from the premaster secret
- To generate the key material, the following is computed:

```
key_block = MD5(master_secret||SHA('A'||master_secret||
              ServerHello.random||ClientHello.random))||
            MD5(master_secret||SHA('BB'||master_secret||
              ServerHello.random||ClientHello.random))||
            MD5(master_secret||SHA('CCC'||master_secret||
              ServerHello.random||ClientHello.random))||...
```

Converting the Master Secret into Cryptographic Parameters

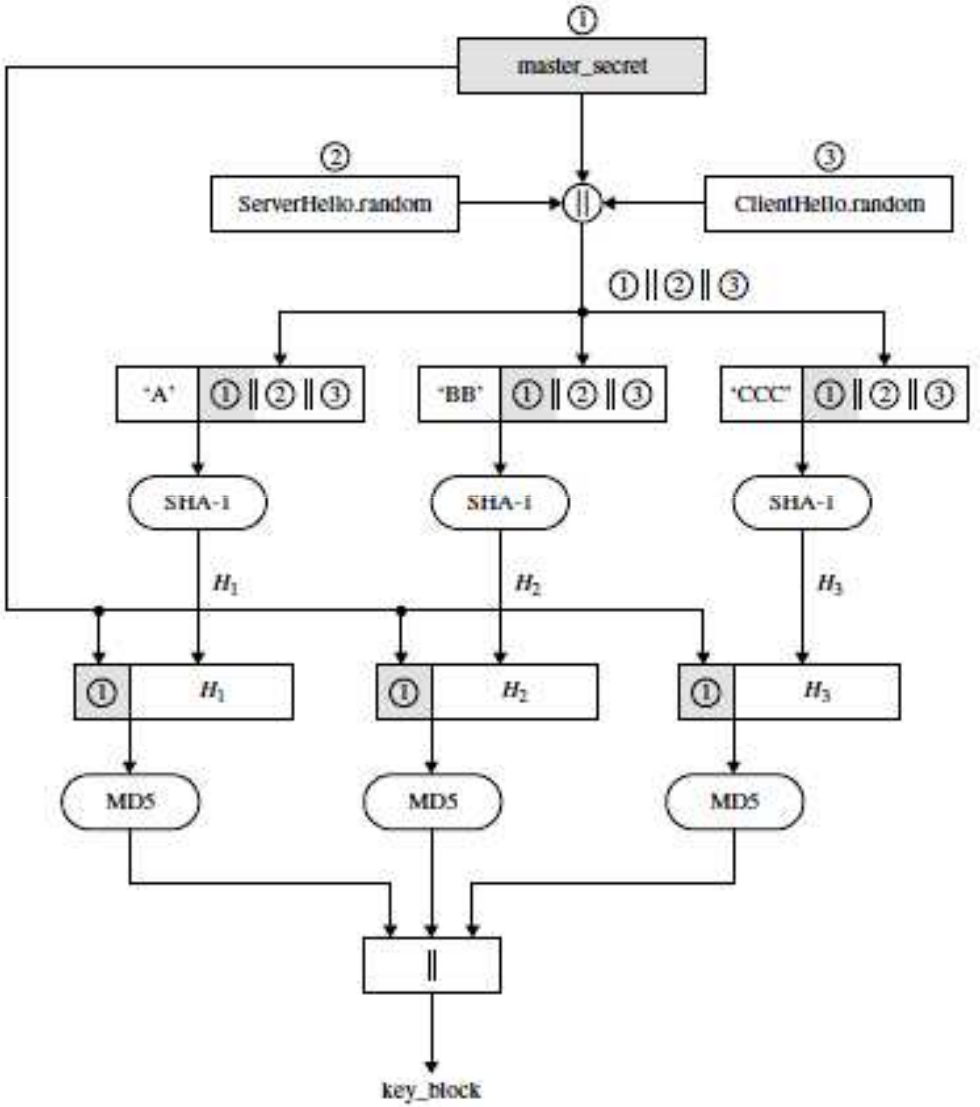

Figure 8.7 Generation of key block.