Unit 5
Network and Internet Security

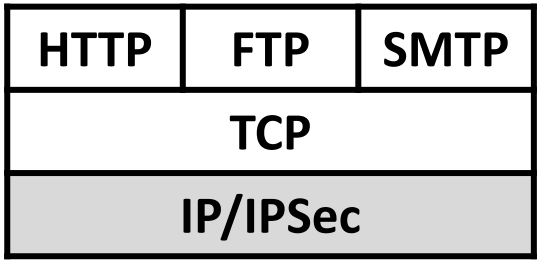
Outline

- Secure Socket Layer (SSL) architecture and working
- Transport Level Security (TLS)
- Secure Shell (SSH) protocol
- Pretty Good Privacy (PGP)
- S/MIME
- IP Security, IPSec
- IPSec Key Management

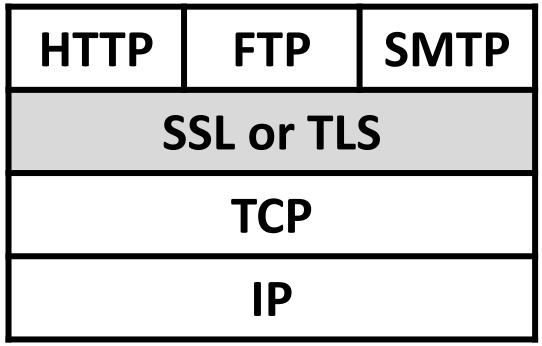
Web Security Issues

- Original Internet protocols do not have built-in security (IP, TCP, HTTP).
- Many threats arise for web and other Internet applications.
- Issues at: client, server and traffic between client and server.
- Cover: SSL/TLS, SSH, IPsec.

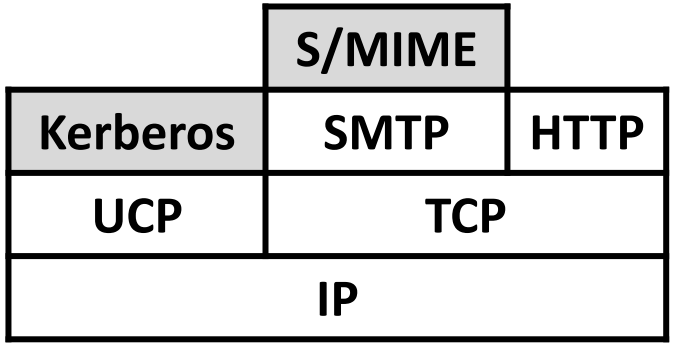
Relative Location of Security Facilities in the TCP/IP Protocol Stack



(a) Network Level



(b) Transport Level



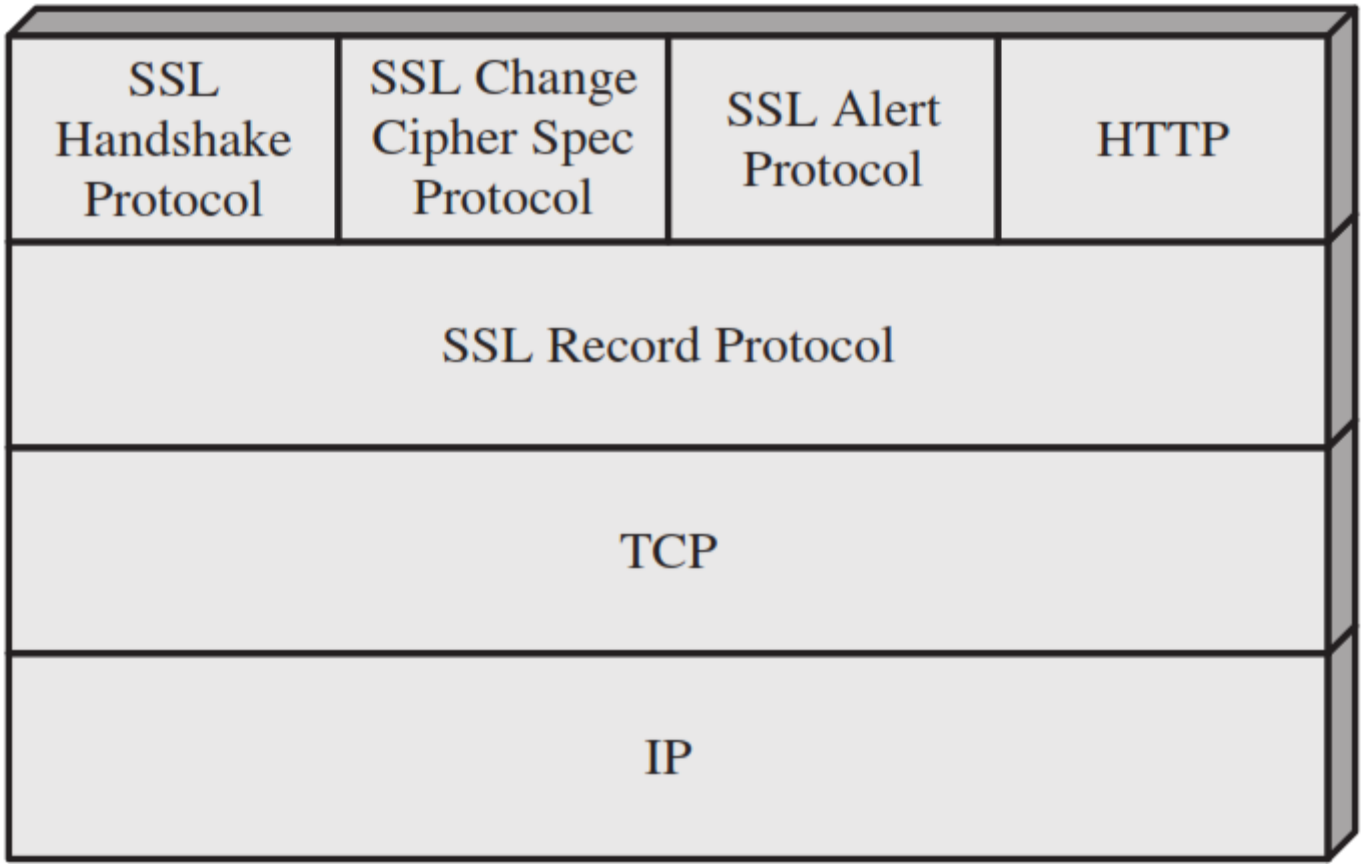
(c) Application Level

- **IPsec:**
  - Security for IP datagrams.
  - General solution for all Internet traffic.
  - Implemented in OS.
- **SSL/TLS:**
  - Security for TCP segments.
  - General solution for all TCP-based applications.
  - Implemented in libraries/applications (e.g. OpenSSL).
- **Application-specific:**
  - Security for application messages.
  - Specific to each applications.
  - Implemented in single application.

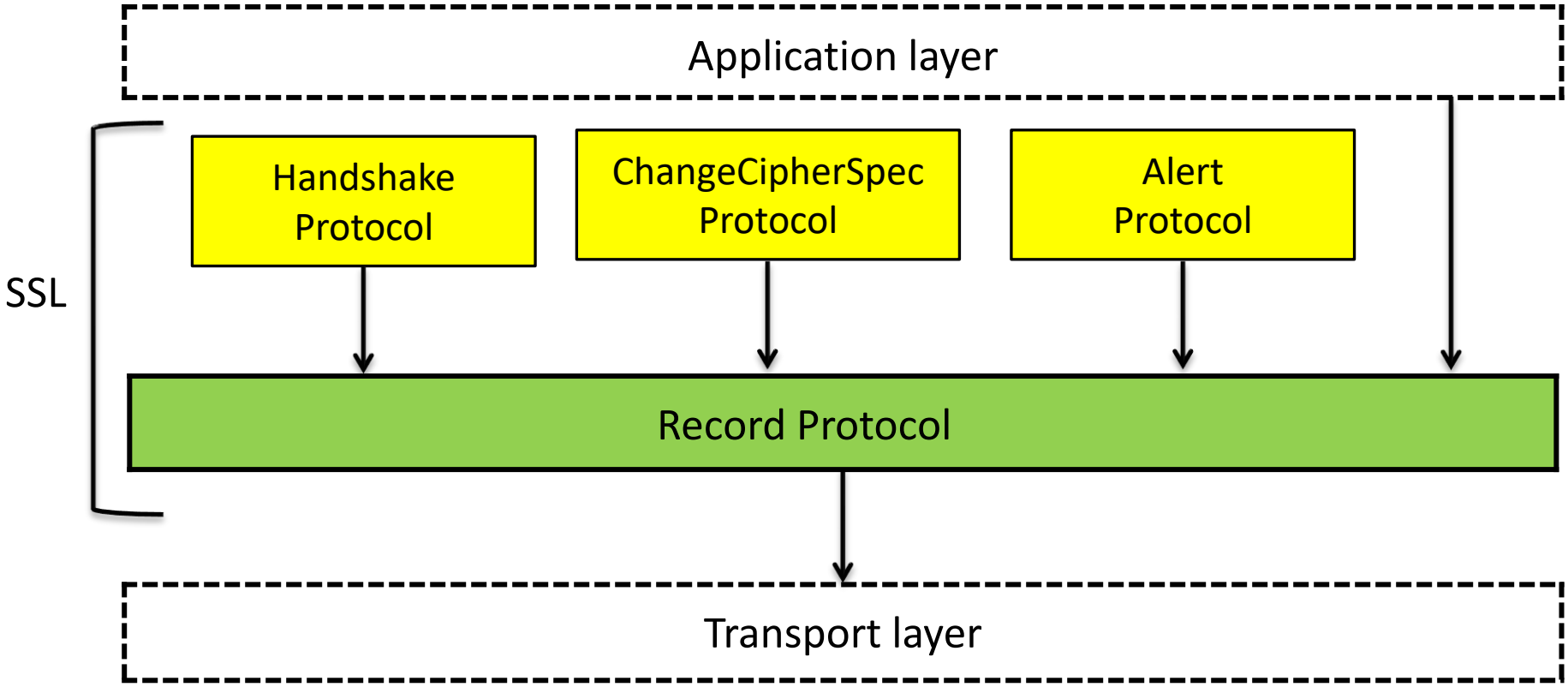
Secure Socket Layer (SSL)

- Secure Socket Layer (SSL) provides security services between TCP and applications that use TCP. The Internet standard version is called Transport Layer Service (TLS).
- SSL/TLS provides confidentiality using symmetric encryption and message integrity using a message authentication code.
- SSL/TLS includes protocol mechanisms to enable two TCP users to determine the security mechanisms and services they will use.
- SSL is designed to make use of TCP to provide a reliable end-to-end secure service.

Secure Socket Layer (SSL) Architecture



Four SSL Protocols

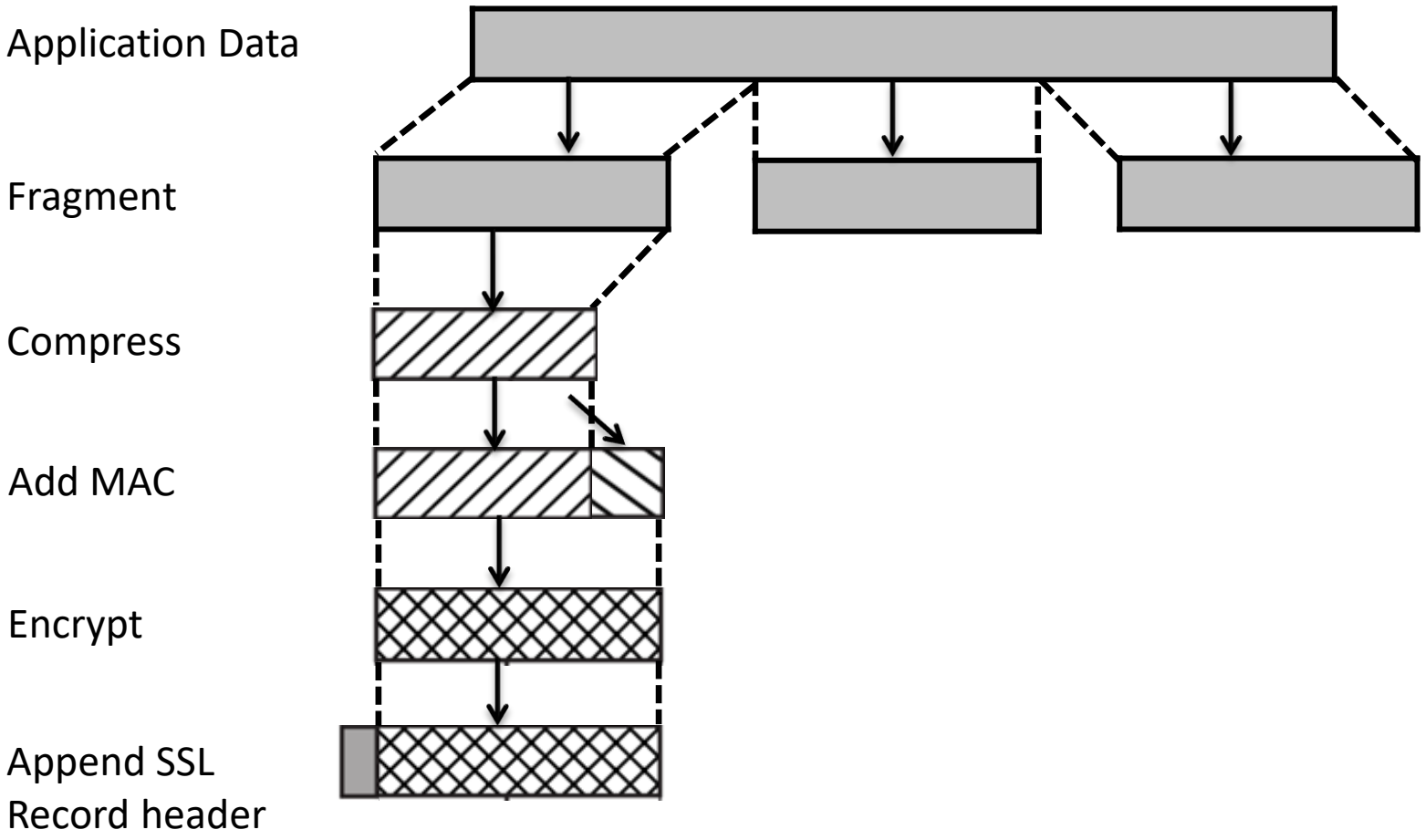


- **Record:** Provides confidentiality and message integrity.
- **Handshake:** Authenticate entities, negotiate parameter values.
- **Change Cipher:** Change cipher for use in connection.
- **Alert:** Alert peer entity of status/warning/error.

SSL Record Protocol

- It provides two services for SSL connections.
- **Confidentiality:** The Handshake Protocol defines a shared secret key that is used for conventional encryption of SSL payloads.
- **Message Integrity:** The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC).

SSL Record Protocol



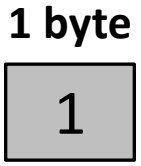
- Transmits the result in a TCP segment.
- Maximum fragment size is 16384 Bytes.

SSL Record Protocol – Cont…

- The Record Protocol takes an application message to be transmitted, fragments the data into manageable blocks, optionally compresses the data, applies a MAC, encrypts, adds a header, and transmits the resulting unit in a TCP segment.
- Received data are decrypted, verified, decompressed, and reassembled before being delivered to higher-level users.

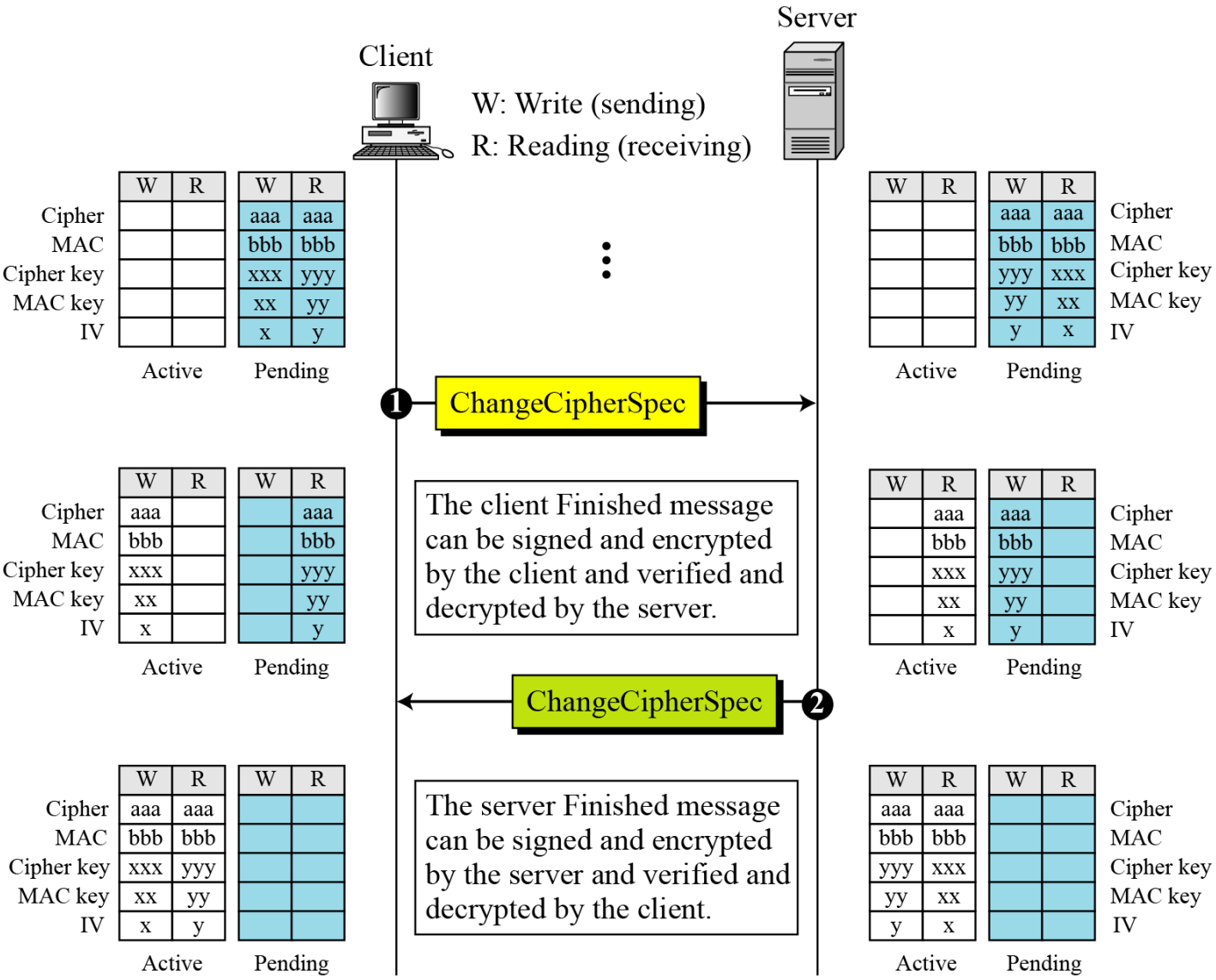
Change Cipher Spec Protocol

- The Change Cipher Spec Protocol is one of the three SSL-specific protocols that use the SSL Record Protocol, and it is the simplest one.
- This protocol consists of a single message which consists of a single byte with the value 1.
- The sole purpose of this message is to cause the pending state to be copied into the current state, which updates the cipher suite to be used on this connection.



Change Cipher Spec Protocol

Change Cipher Spec Protocol – Cont…



Alert Protocol

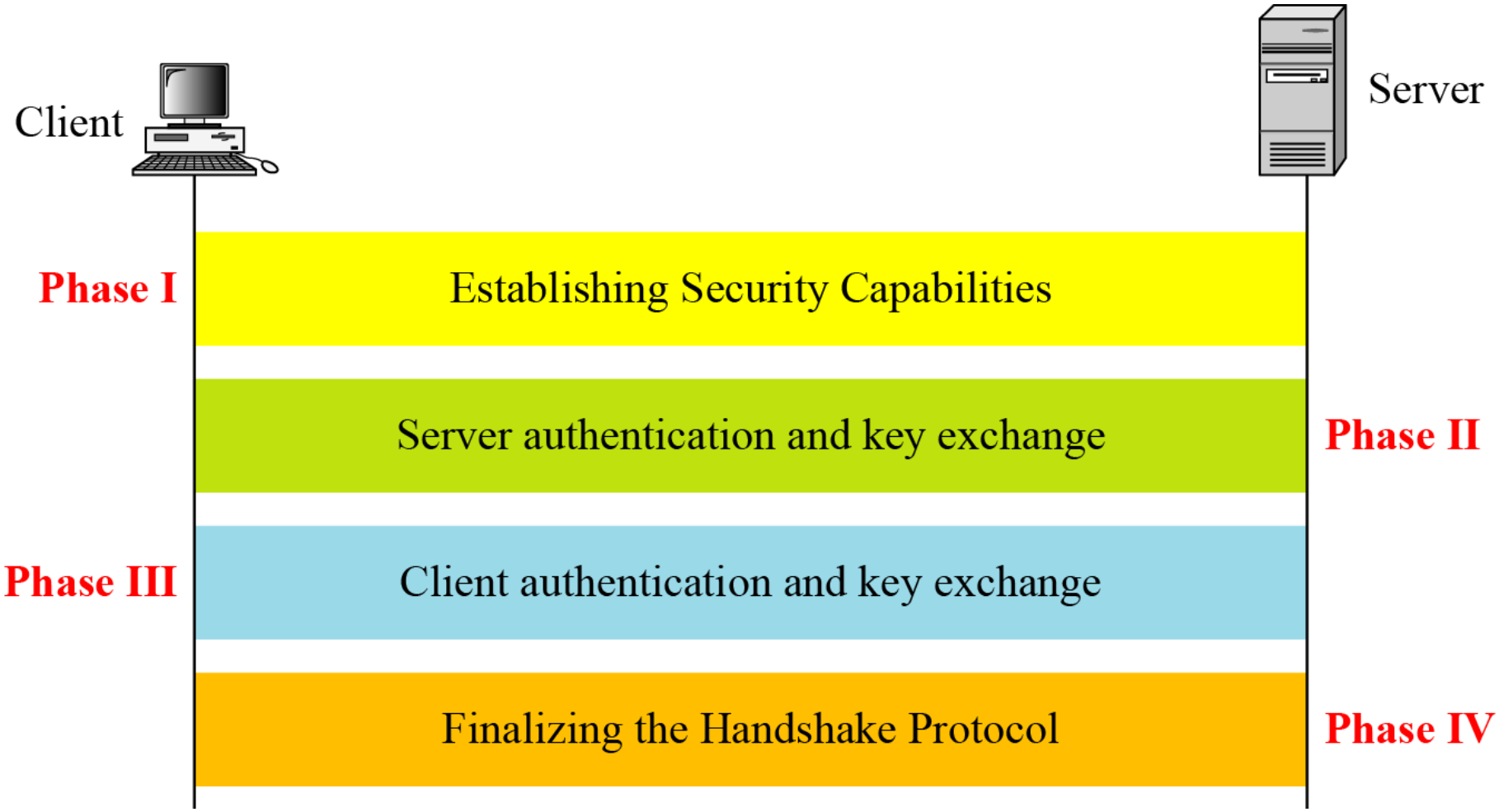
- The Alert Protocol is used to convey SSL-related alerts to the peer entity. As with other applications that use SSL, alert messages are compressed and encrypted, as specified by the current state.

Value	*Description*	*Meaning*
0	*CloseNotify*	Sender will not send any more messages.
10	*UnexpectedMessage*	An inappropriate message received.
20	*BadRecordMAC*	An incorrect MAC received.
30	*DecompressionFailure*	Unable to decompress appropriately.
40	*HandshakeFailure*	Sender unable to finalize the handshake.
41	*NoCertificate*	Client has no certificate to send.
42	*BadCertificate*	Received certificate corrupted.
43	*UnsupportedCertificate*	Type of received certificate is not supported.
44	*CertificateRevoked*	Signer has revoked the certificate.
45	*CertificateExpired*	Certificate expired.
46	*CertificateUnknown*	Certificate unknown.
47	*IllegalParameter*	An out-of-range or inconsistent field.

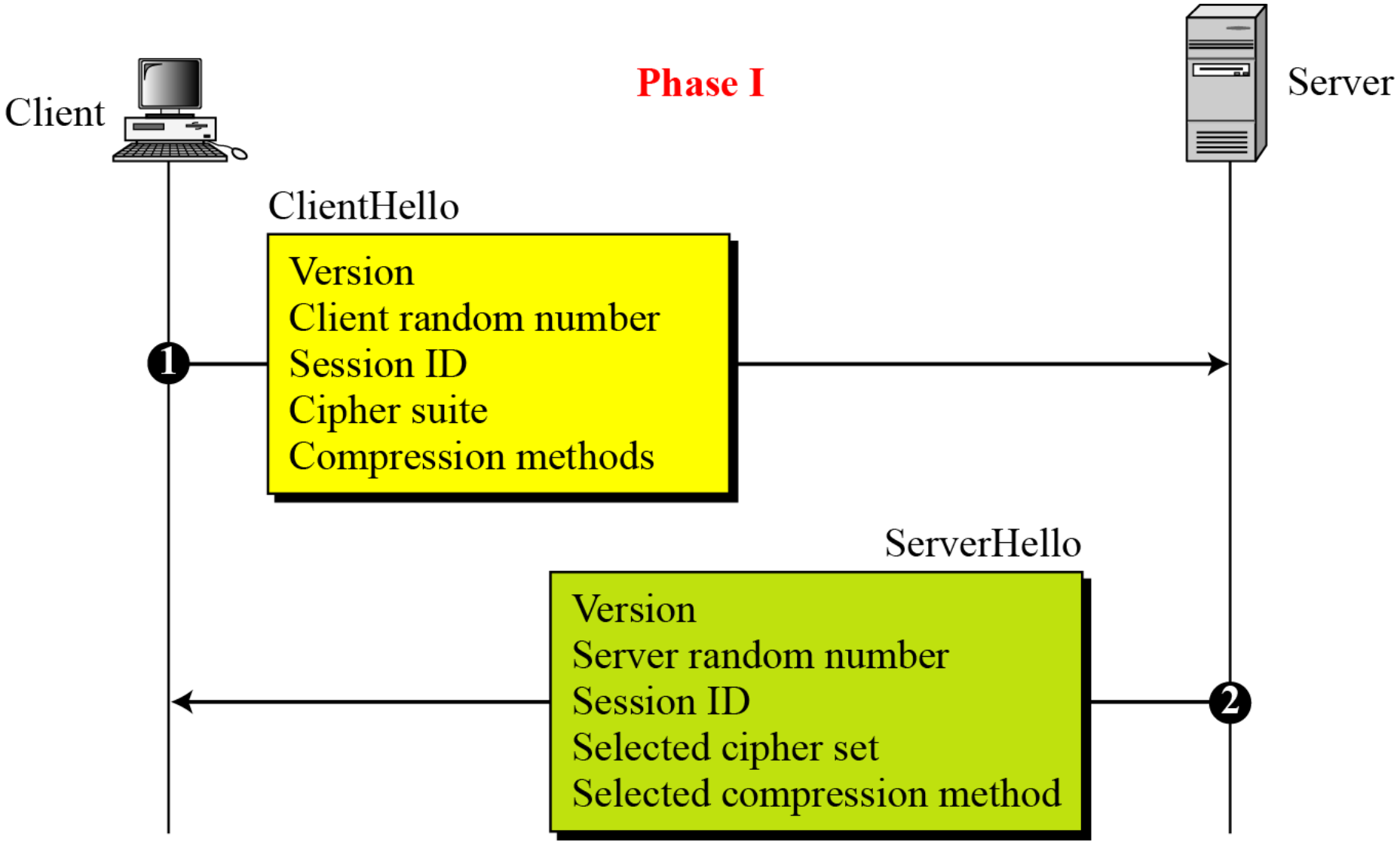
SSL Handshake Protocol

- Allow client and server to authenticate each other.
- Negotiate encryption and MAC algorithms, exchange keys.
  - **Key Exchange:** RSA, Diffie-Hellman
  - **MAC:** HMAC using SHA or MD5
  - **Encryption:** RC4, RC2, DES, 3DES, IDEA, AES
- Multiple phases:
  1. Establish security capabilities
  2. Server authentication and key exchange
  3. Client authentication and key exchange
  4. Finish setting up connection

Handshake Protocol



Handshake Protocol – Phase I

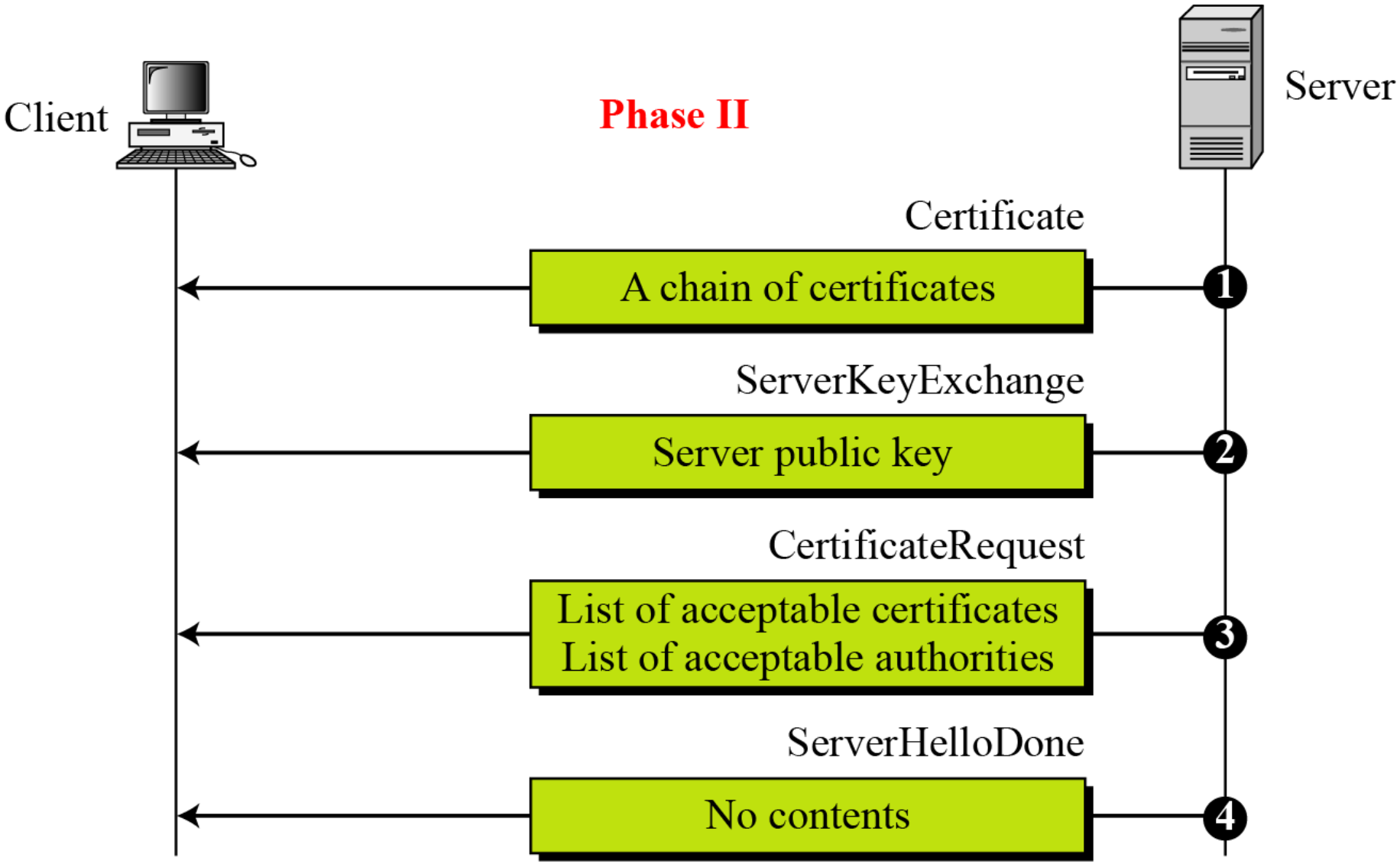


Handshake Protocol – Phase I

After Phase I, the client and server knows the following:

- The version of SSL.
- The algorithms for key exchange, message authentication, and encryption.
- The compression method.
- The two random numbers for key generation.

Handshake Protocol – Phase II

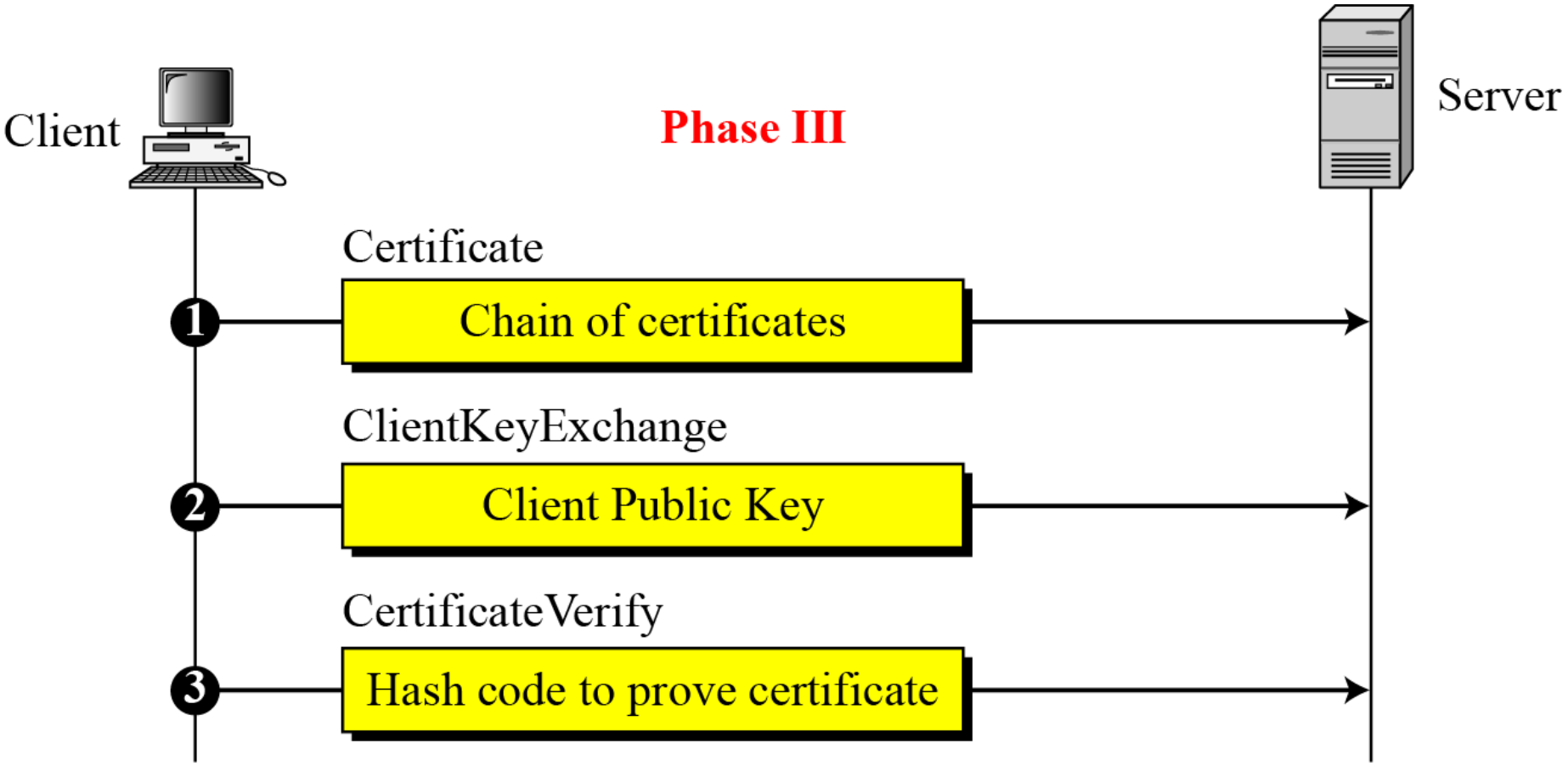


Handshake Protocol – Phase II

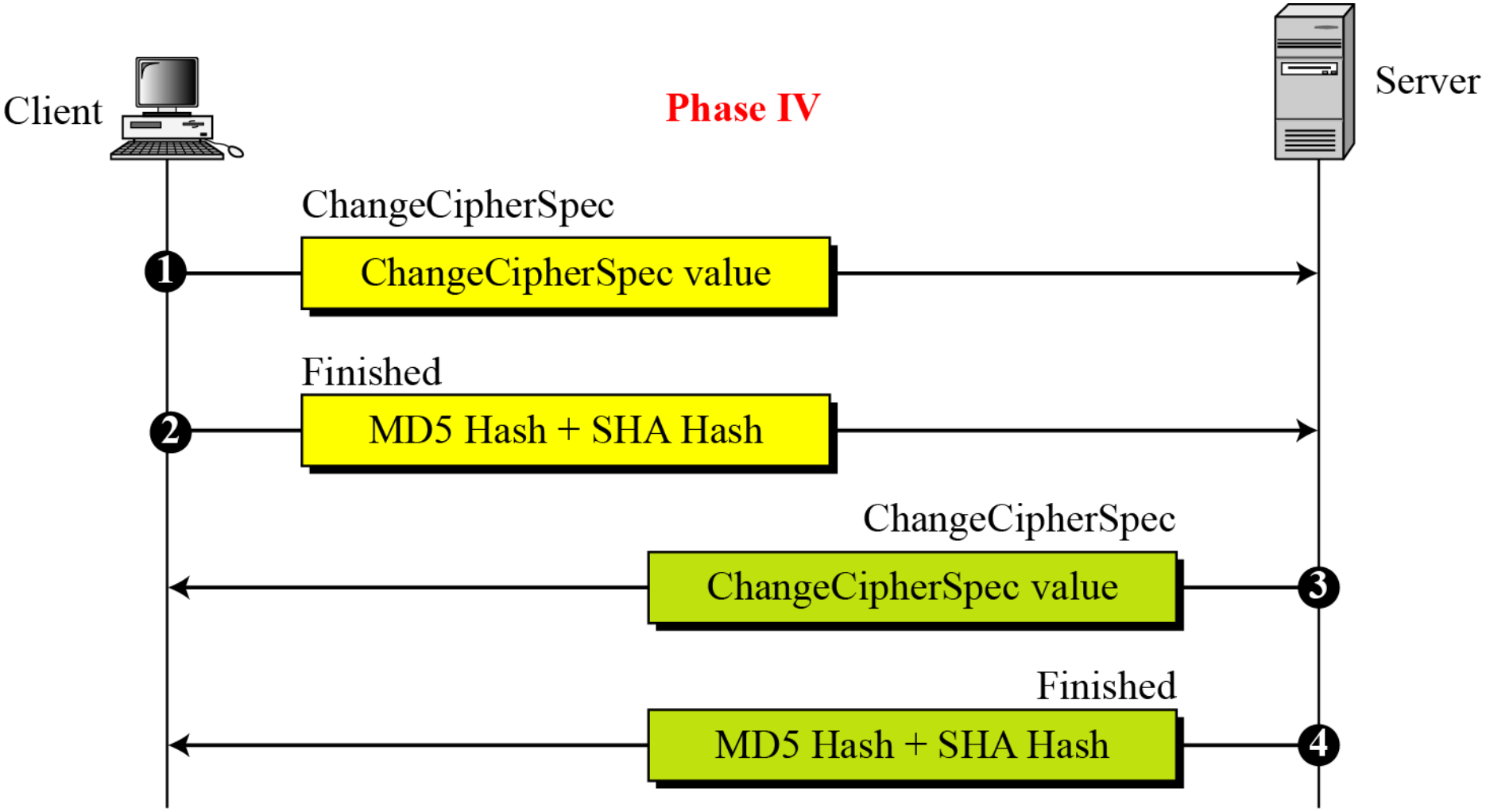
After Phase II

- The server is authenticated to the client.
- The client knows the public key of the server if required.

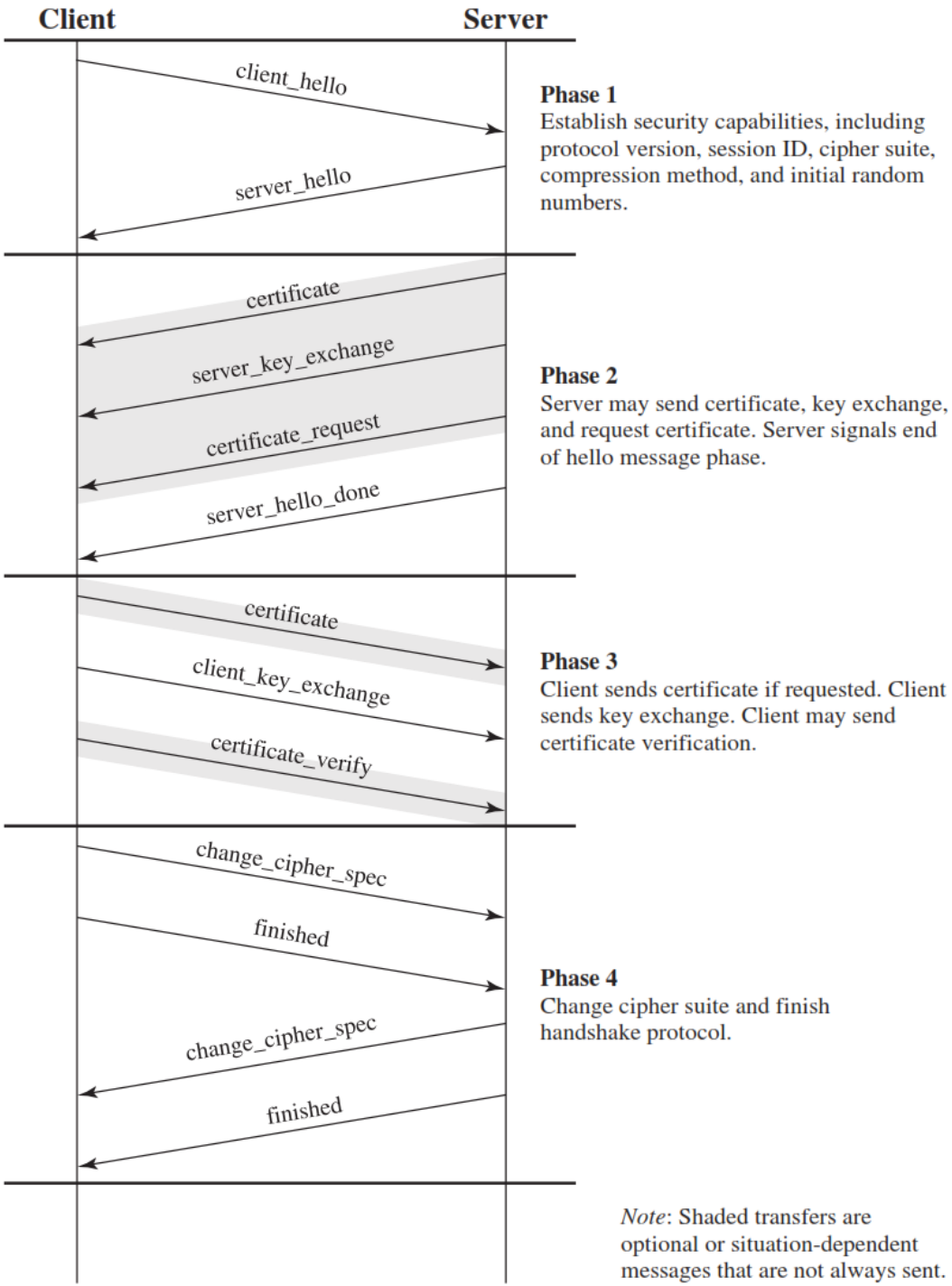
Handshake Protocol – Phase III



Handshake Protocol – Phase IV



SSL Handshake Protocol Phases



HTTPS (HTTP over SSL)

- HTTPS (HTTP over SSL) refers to the combination of HTTP and SSL to implement secure communication between a Web browser and a Web server.
- When HTTPS is used, the following elements of the communication are encrypted:
  1. URL of the requested document.
  2. Contents of the document.
  3. Contents of browser forms (filled in by browser user).
  4. Cookies sent from browser to server and from server to browser.
  5. Contents of HTTP header.

SSH (Secure Shell)

- Secure Shell (SSH) is a protocol for secure network communications designed to be relatively simple and inexpensive to implement.
- The initial version, SSH1 was focused on providing a secure remote logon facility to replace TELNET and other remote logon schemes that provided no security.

SSH (Secure Shell) – Cont…