CS 547: Foundation of Computer Security

S. Tripathy
IIT Patna

Previous Classes

- Network Security Controls
  - Link Encryption & End to End Encryption
  - IP-Sec

Present class

- Security in Networks
    - TLS

Security at the Transport Layer

- SSL: Secure Sockets Layer & TLS: Transport layer Security
- Objective: To provide a secure transport connection between applications.
- Privacy
  - Anyone can see content
- Integrity
  - Someone might alter content
- Authentication
  - Not clear who you are talking with

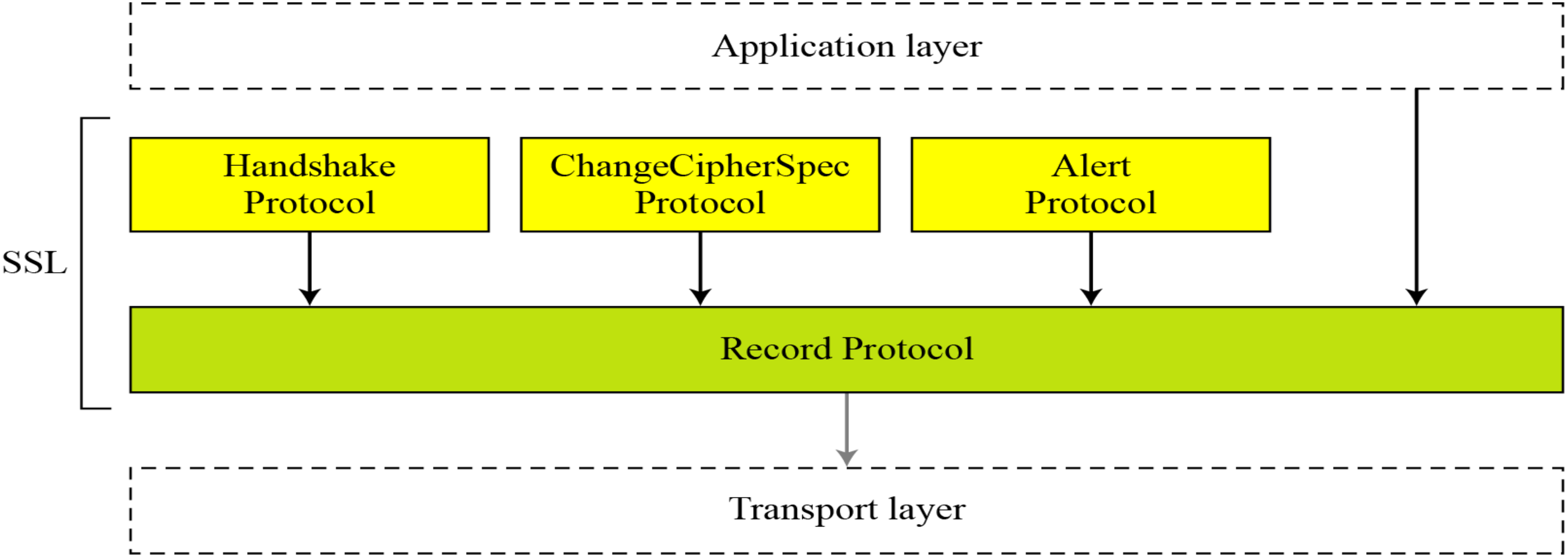
SSL & TLS: Overview

- Establish a session (Secure)
  - Agree on algorithms
  - Share secrets
  - Perform authentication
- Transfer application data (securely)
  - Ensure privacy and integrity

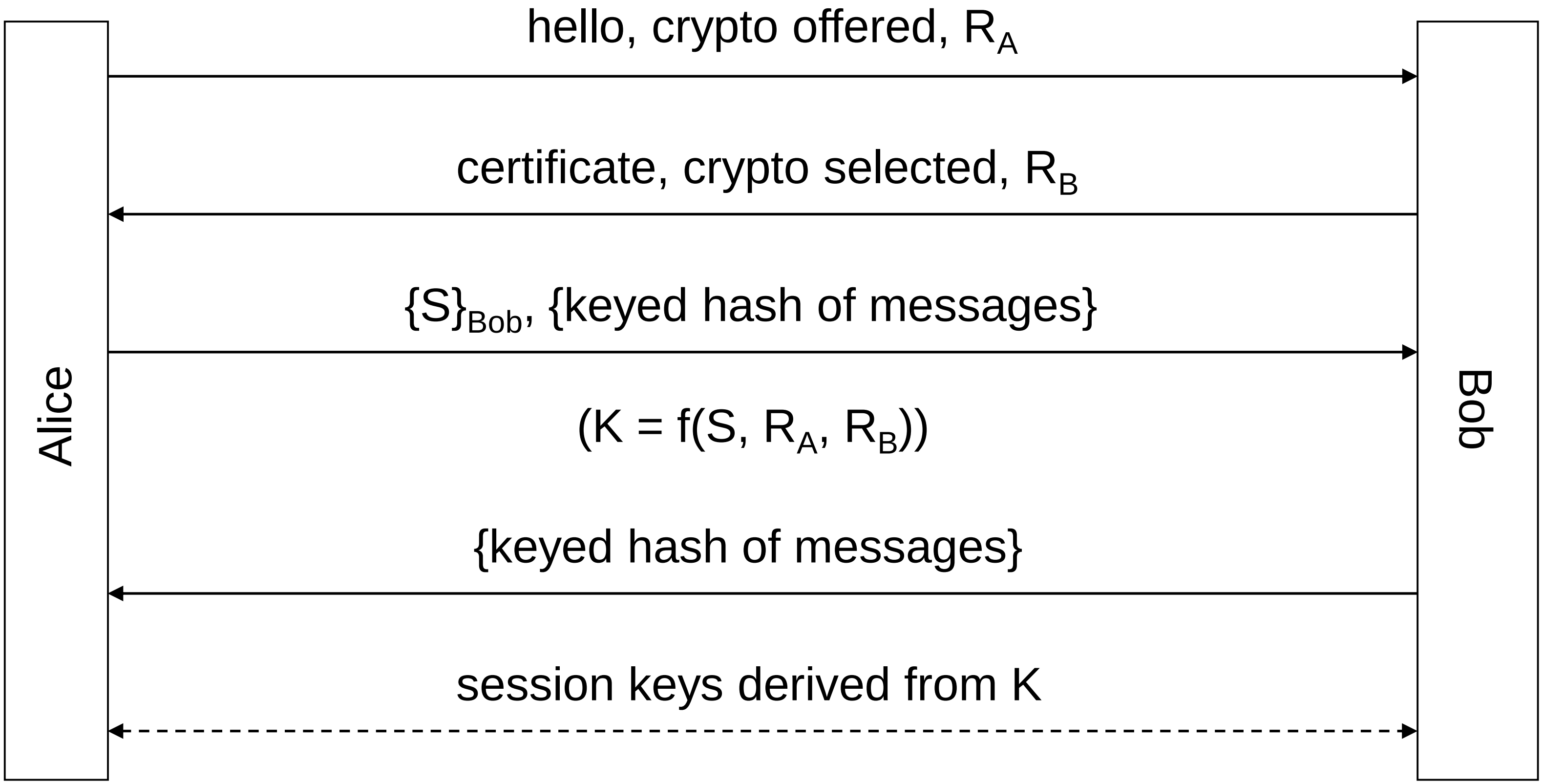
Components of SSL at

SSL defines Record Protocol to transfer application and SSL information

A session is established using a Handshake Protocol



Basic SSL/TLS Handshake Protocol



hello, crypto offered, R_A

certificate, crypto selected, R_B

$\{S\}_{Bob}$, {keyed hash of messages}

$(K = f(S, R_A, R_B))$

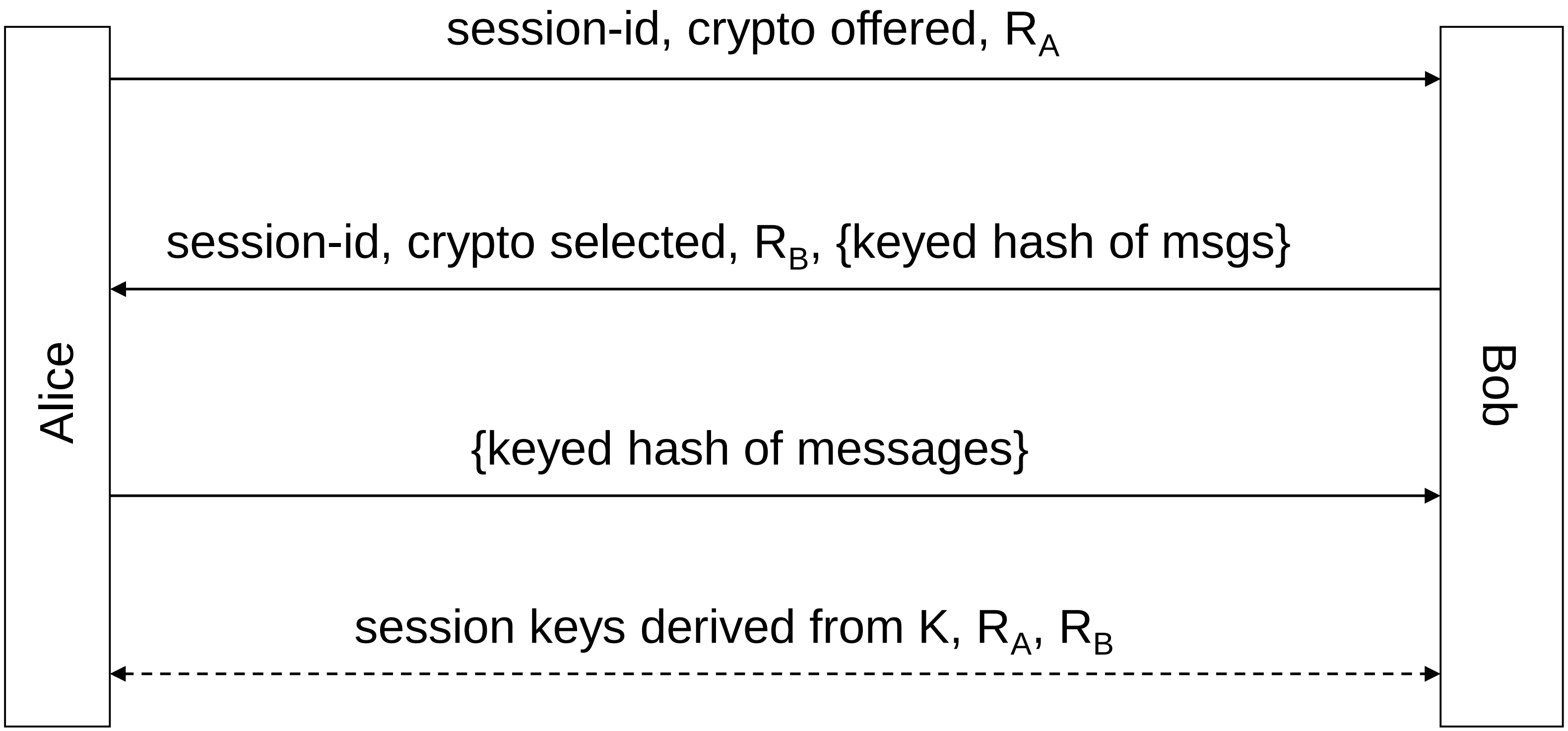
{keyed hash of messages}

session keys derived from K

SSL Session Establishment

- Client authentication: Bob can optionally send "certificate request" in message 2.
- Session vs. Connection: "Sessions" are relatively long-lived. Multiple "connections" (TCP) can be supported under the same SSL session.
- To start a connection, Alice can send an existing session ID.
- If Bob doesn't remember the session ID Alice sent, he responds with a different value.

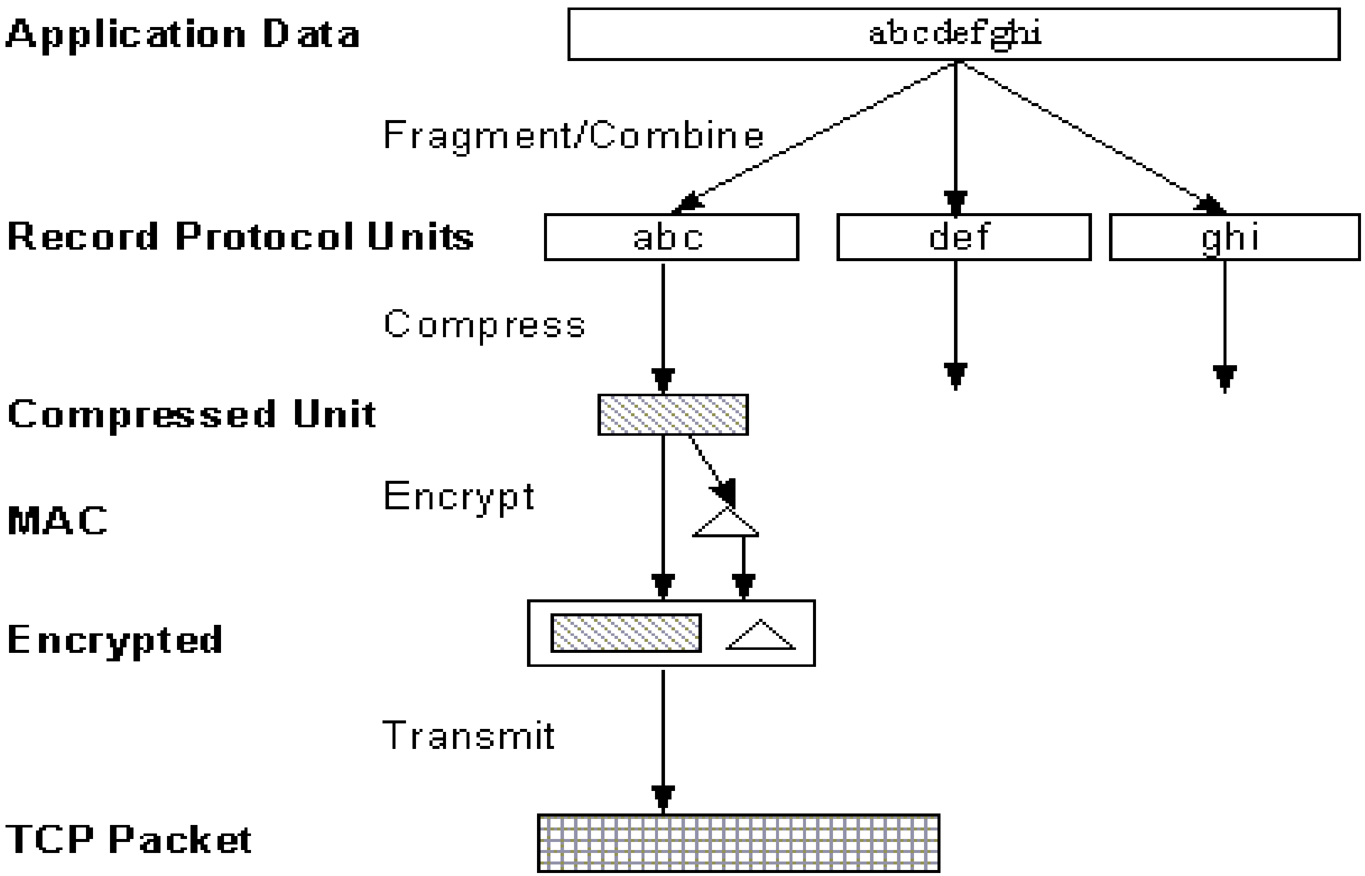
Session Resumption (“Connection”)


Alice
Bob
session-id, crypto offered, R_A
session-id, crypto selected, R_B, {keyed hash of msgs}
{keyed hash of messages}
session keys derived from K, R_A, R_B

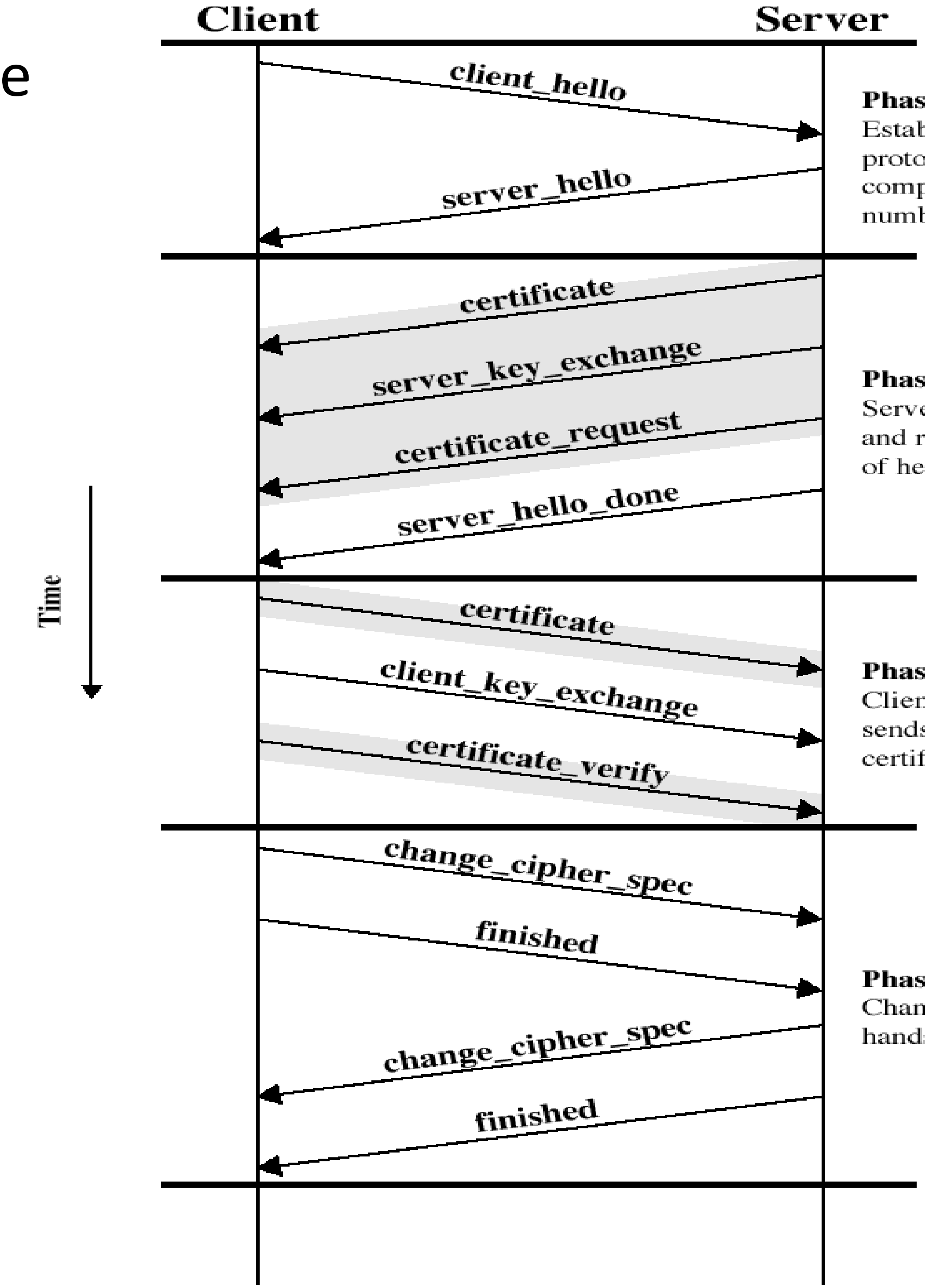
Key Computation

- "pre-master key": S
- "master key": $K = f(S, R_A, R_B)$
- For each connection, 6 keys are generated from K and the nonces. (3 keys for each direction: encryption, authentication/integrity, IV)

SSL Record Protocol



Handshake Protocol



Phase 1
Establish security capabilities, including protocol version, session ID, cipher suite, compression method, and initial random numbers.

Phase 2
Server may send certificate, key exchange, and request certificate. Server signals end of hello message phase.

Phase 3
Client sends certificate if requested. Client sends key exchange. Client may send certificate verification.

Phase 4
Change cipher suite and finish handshake protocol.

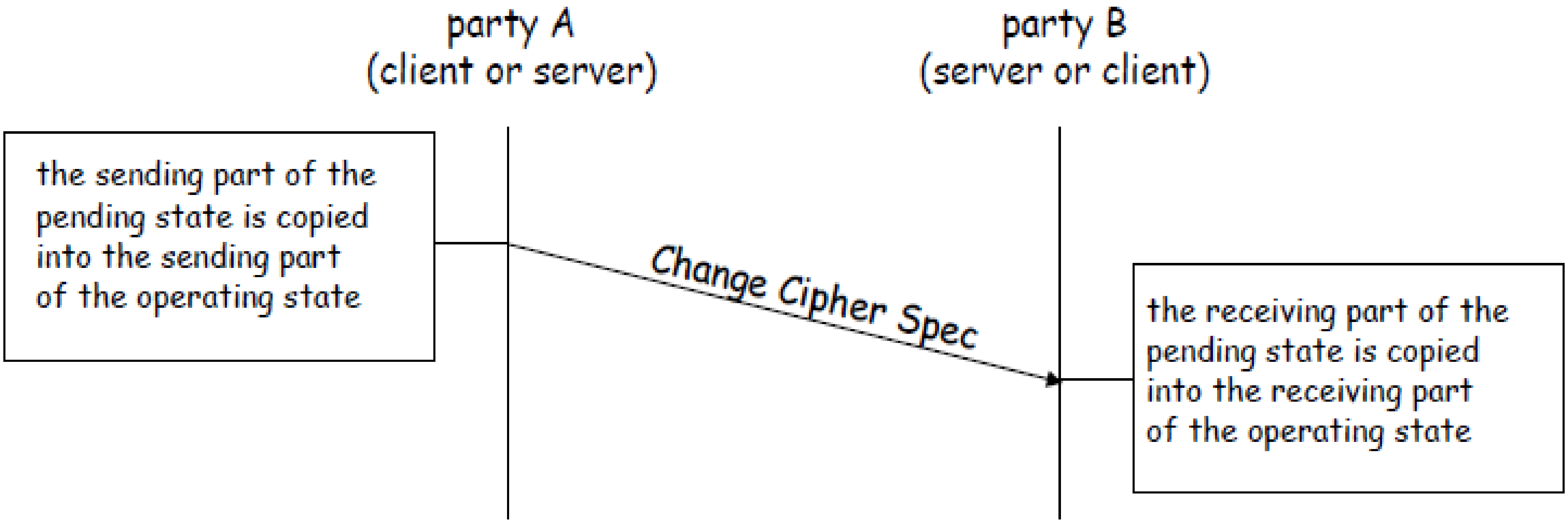
Note: Shaded transfers are optional or situation-dependent messages that are not always sent.

Change cipher Spec

Changing State & moving parameters

- operating state

- pending state
- operating state ← pending state
  - at the transmission and reception of a Change Cipher Spec message



party A
(client or server)

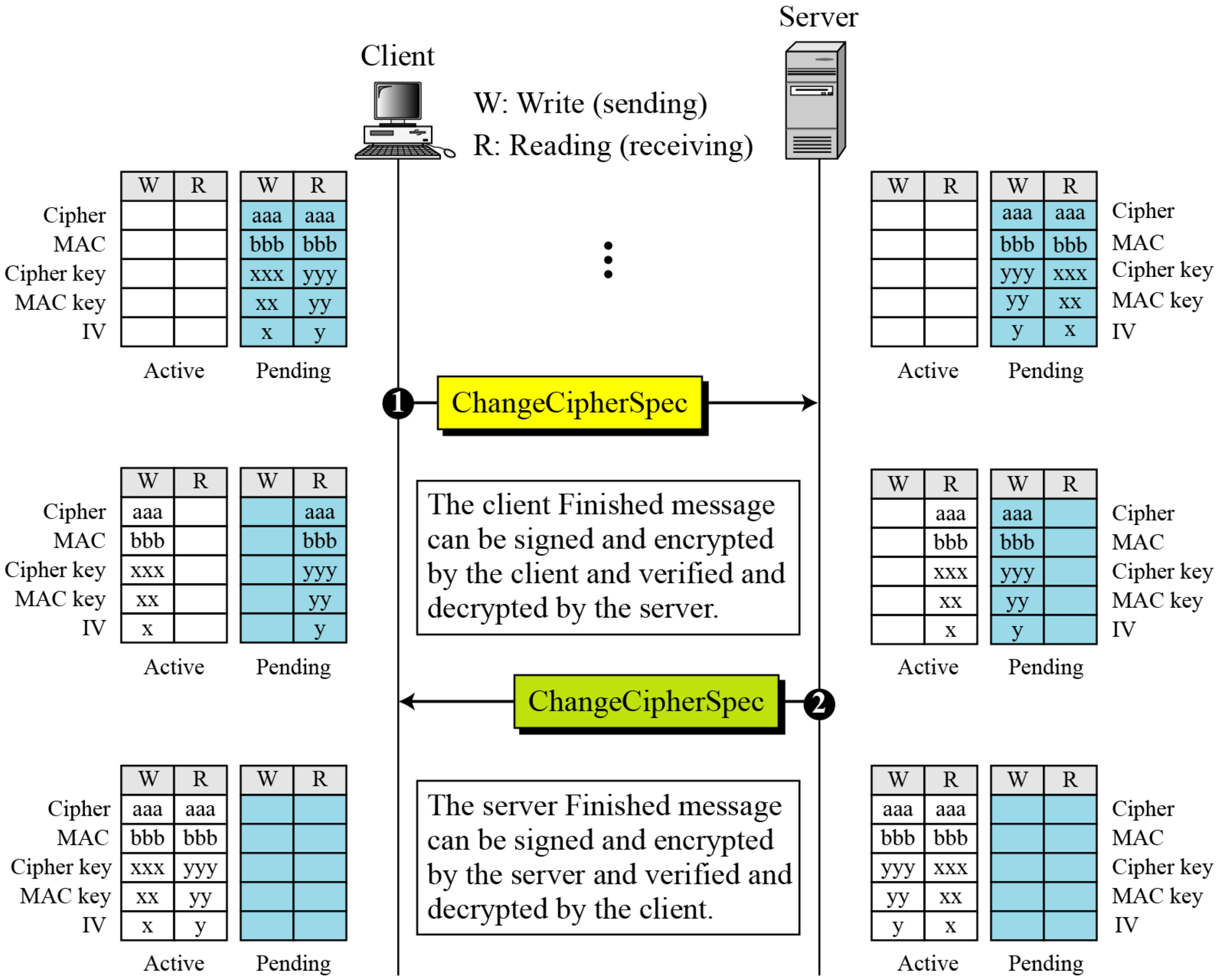
party B
(server or client)

the sending part of the pending state is copied into the sending part of the operating state

Change Cipher Spec

the receiving part of the pending state is copied into the receiving part of the operating state

Movement of parameters
From Pending state to active state



Client

	Active		Pending	
	W	R	W	R
Cipher			aaa	aaa
MAC			bbb	bbb
Cipher key			xxx	yyy
MAC key			xx	yy
IV			x	y

Server

	Active		Pending	
	W	R	W	R
Cipher			aaa	aaa
MAC			bbb	bbb
Cipher key			yyy	xxx
MAC key			yy	xx
IV			y	x

Client

	Active		Pending	
	W	R	W	R
Cipher	aaa			aaa
MAC	bbb			bbb
Cipher key	xxx			yyy
MAC key	xx			yy
IV	x			y

The client Finished message can be signed and encrypted by the client and verified and decrypted by the server.

Server

	Active		Pending	
	W	R	W	R
Cipher		aaa	aaa	
MAC		bbb	bbb	
Cipher key		xxx	yyy	
MAC key		xx	yy	
IV		x	y	

Client

	Active		Pending	
	W	R	W	R
Cipher	aaa	aaa		
MAC	bbb	bbb		
Cipher key	xxx	yyy		
MAC key	xx	yy		
IV	x	y		

The server Finished message can be signed and encrypted by the server and verified and decrypted by the client.

Server

	Active		Pending	
	W	R	W	R
Cipher	aaa	aaa		
MAC	bbb	bbb		
Cipher key	yyy	xxx		
MAC key	yy	xx		
IV	y	x		

Summary

- OpenSSL is an Open Source toolkit implementing SSL/TLS & Cryptography
- It has a command-line interface & an application programming interface
- There are a lot of tools using OpenSSL's libraries to secure data or establish secure connections

Thanks

- All the Best for Exam