CS120: Computer Networks

Lecture 28. Network Security 2

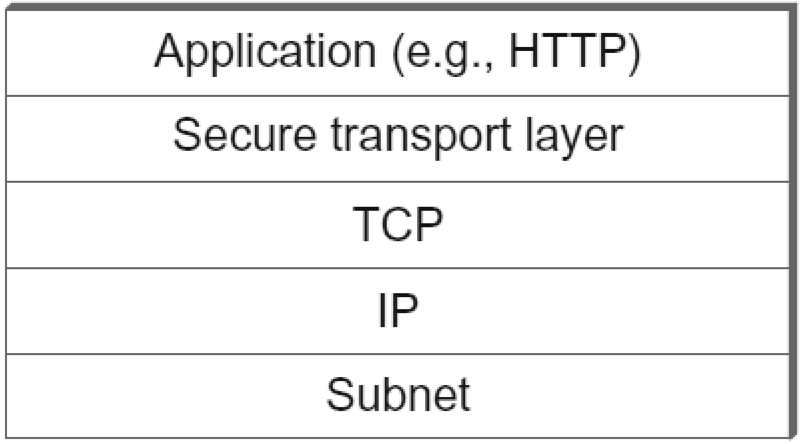
Zhice Yang

Example Systems

- TLS/SSL
- SSH
- Wi-Fi Security

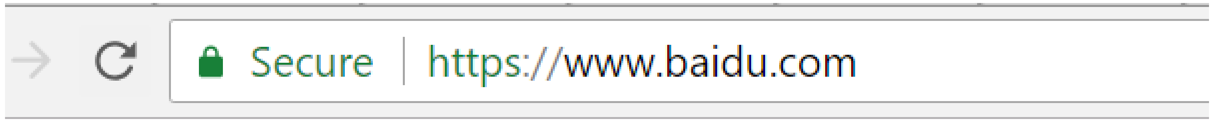
SSL: A Secure Transportation Layer Protocol

- SSL: Secure Sockets Layer
  - Deprecated [2015]
- TLS: Transport Layer Security
  - TLS 1.3: RFC 8846 [2018]
- Security for any application that uses TCP
  - HTTPS (HTTP over SSL)
  - Some VPN
- Be able to handle threats
  - Eavesdropping
    - Confidentiality
  - Manipulation
    - Integrity
  - Impersonation
    - Authentication



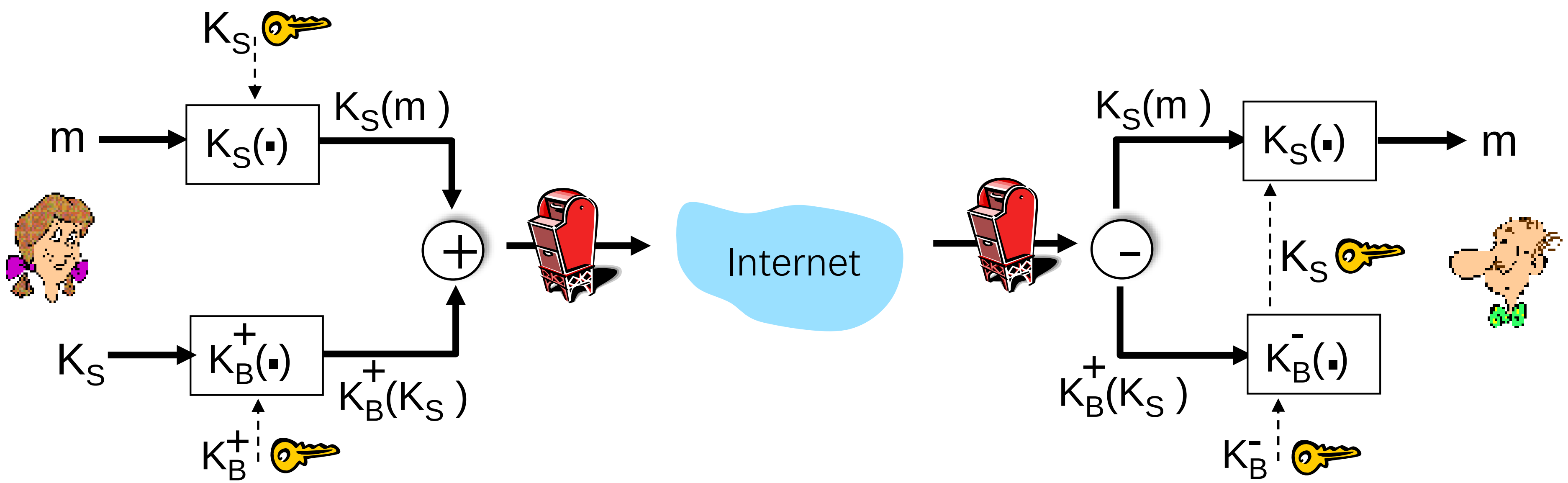
HTTPS

- Suppose a browser (client) wants to connect to a server who has a certificate from a trusted CA



Secure Message: Confidentiality

Alice wants to send *confidential* Message, m, to Bob.



Alice:

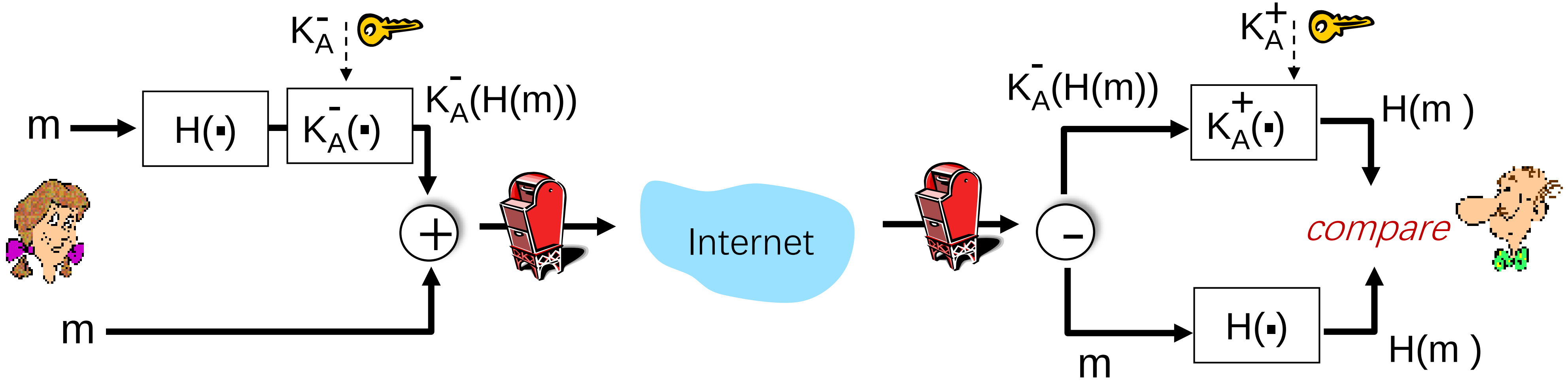
- generates random *symmetric* private key, K_S
- encrypts message with K_S (for efficiency)
- also encrypts K_S with Bob's public key
- sends both $K_S(m)$ and $K^+_B(K_S)$ to Bob

Bob:

- uses his private key to decrypt and recover K_S
- uses K_S to decrypt $K_S(m)$ to recover m

Secure Message: Integrity + Authentication

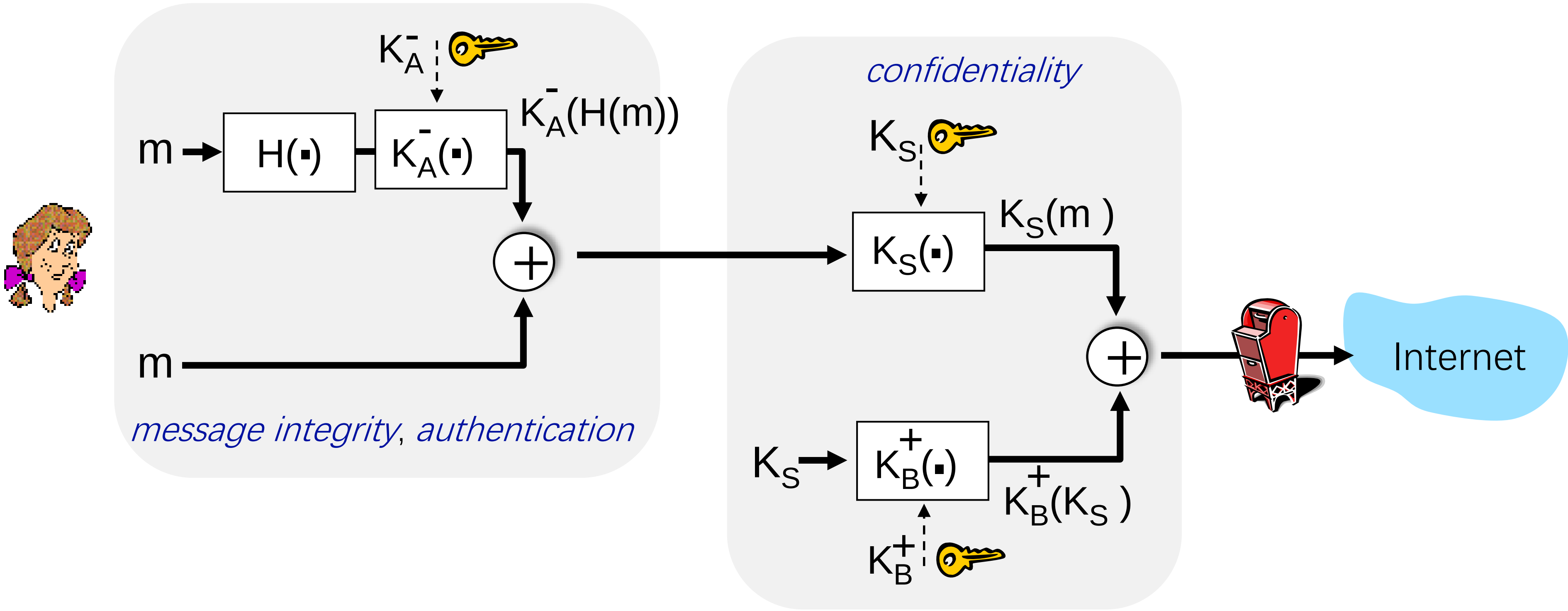
Alice wants to send m to Bob, with *message integrity*, *authentication*



- Alice digitally signs hash of her message with her private key, providing integrity and authentication
- sends both message (in the clear) and digital signature

Secure Message: ALL

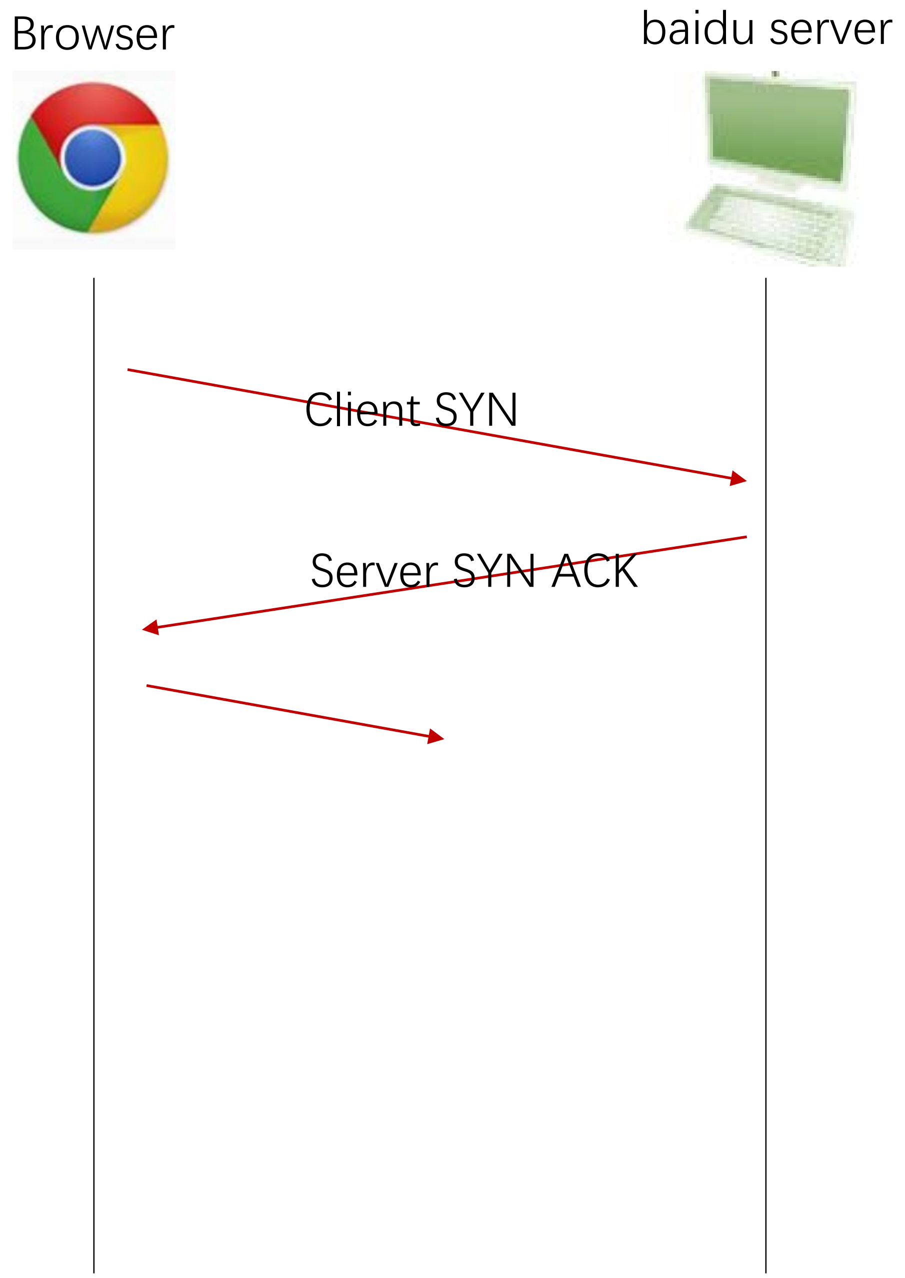
Alice sends m to Bob, with *confidentiality, message integrity, authentication*



Alice uses three keys: her private key, Bob's public key, new symmetric key

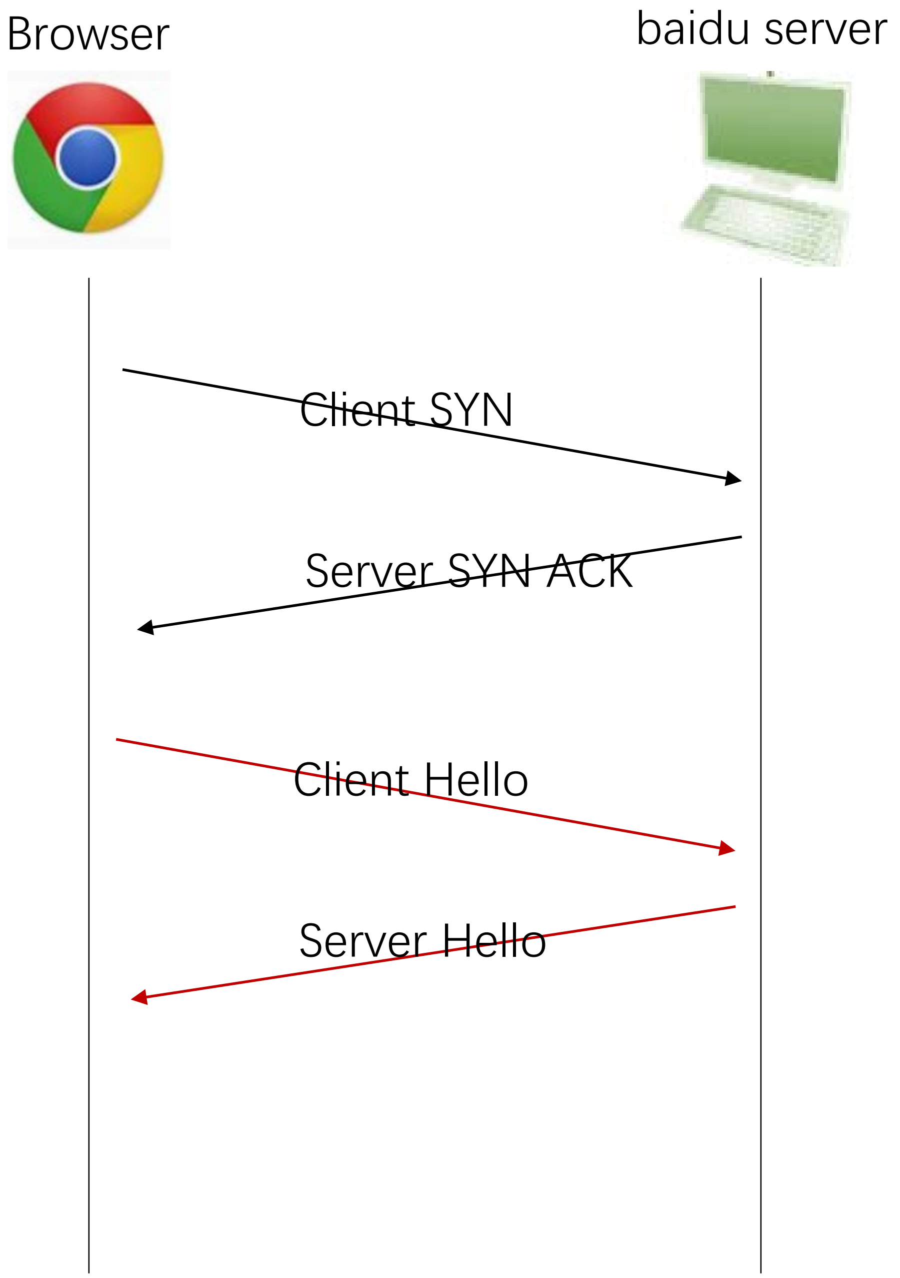
HTTPS via RSA

- Browser obtains the IP of the domain name www.baidu.com
- Browser connects to Baidu's HTTPS server (port 443) via TCP



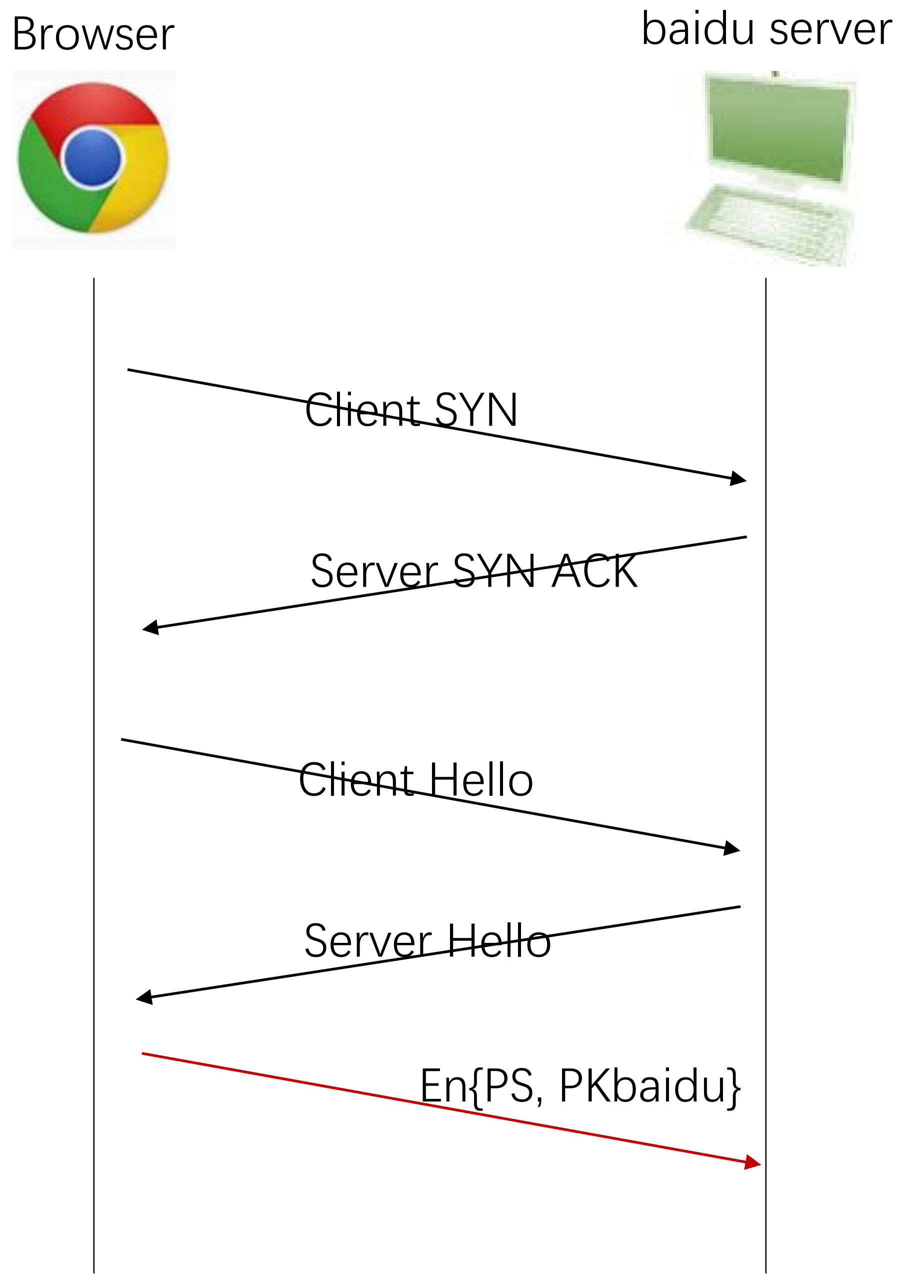
HTTPS via RSA

- Client Hello contains
  - 256-bit random number R_B
  - list of crypto algorithms it supports
- Server Hello contains
  - 256-bit random number R_S
  - Selects algorithms to use for this session
  - Server's certificate
- Browser validates server's cert
  - According to CAs



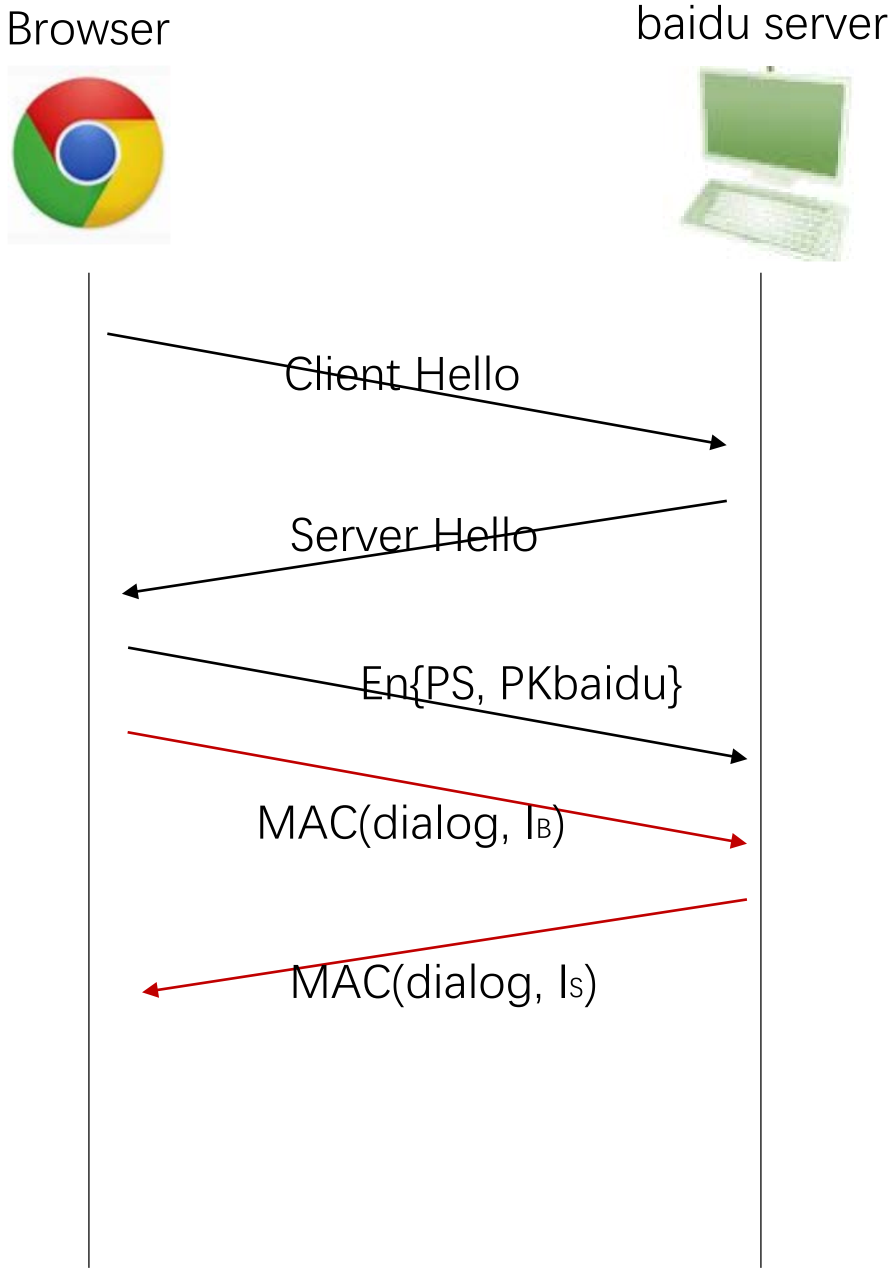
HTTPS via RSA

- Browser constructs “Premaster Secret” **PS**.
    - Uses R_B, R_S
- Browser sends **PS** encrypted using Baidu’s public RSA key: PKbaidu
- Using **PS**, R_B, and R_S, browser & server derive symmetric cipher keys (C_B, C_S) & MAC integrity keys (I_B, I_S)
    - One pair to use in each direction
    - Considered bad to use same key for more than one cryptographic function
        - I and C are different



HTTPS via RSA

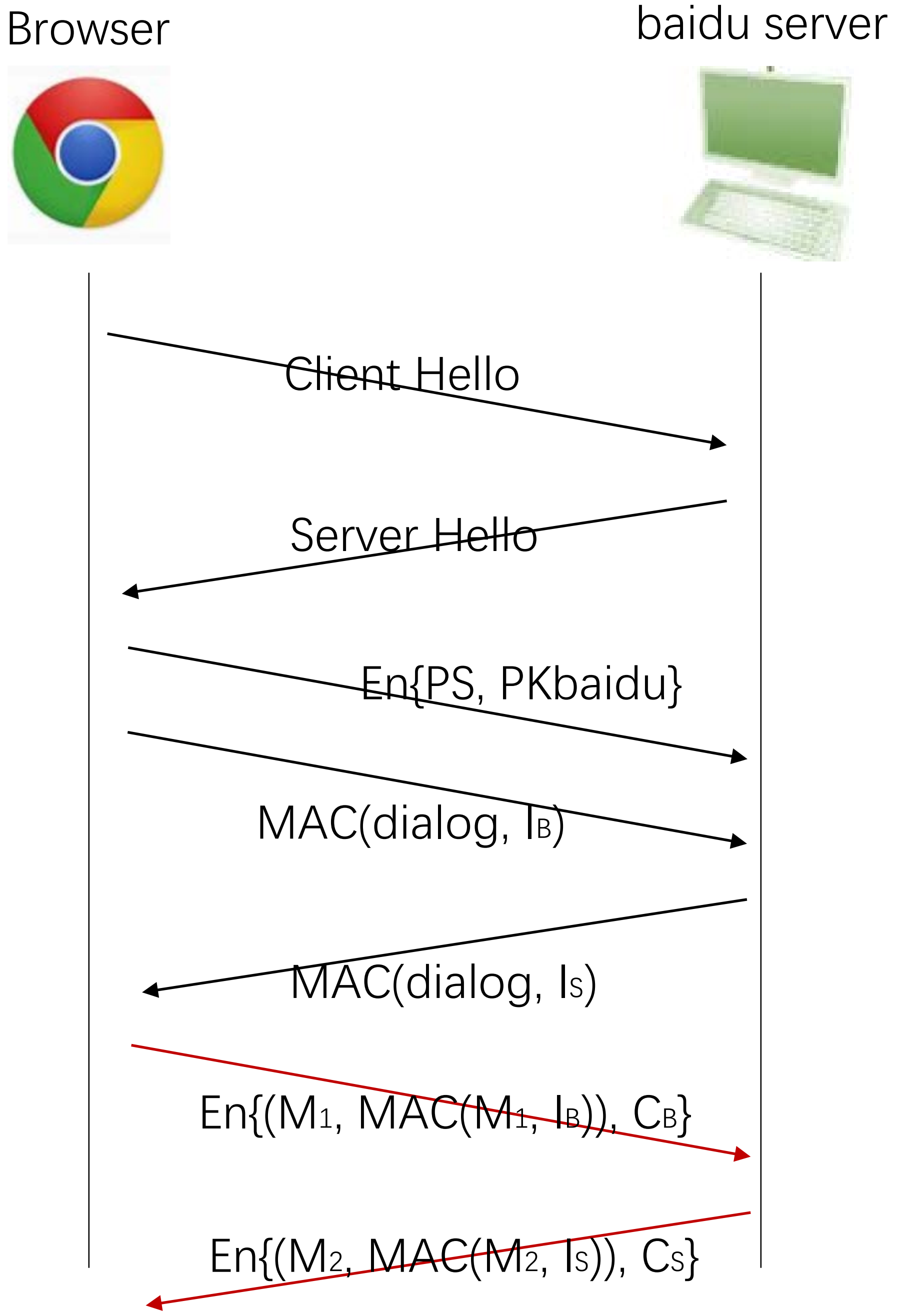
- Browser & server exchange MACs computed over entire dialog so far
  - Verify that (C_B, C_S) (I_B, I_S) are calculated correctly
- If good MAC, Browser displays 🔒 Secure



HTTPS via RSA

- Browser & server exchange MACs computed over entire dialog so far
- If good MAC, Browser displays 

- All subsequent communication encrypted with symmetric cipher (AES, 3DES, etc.)

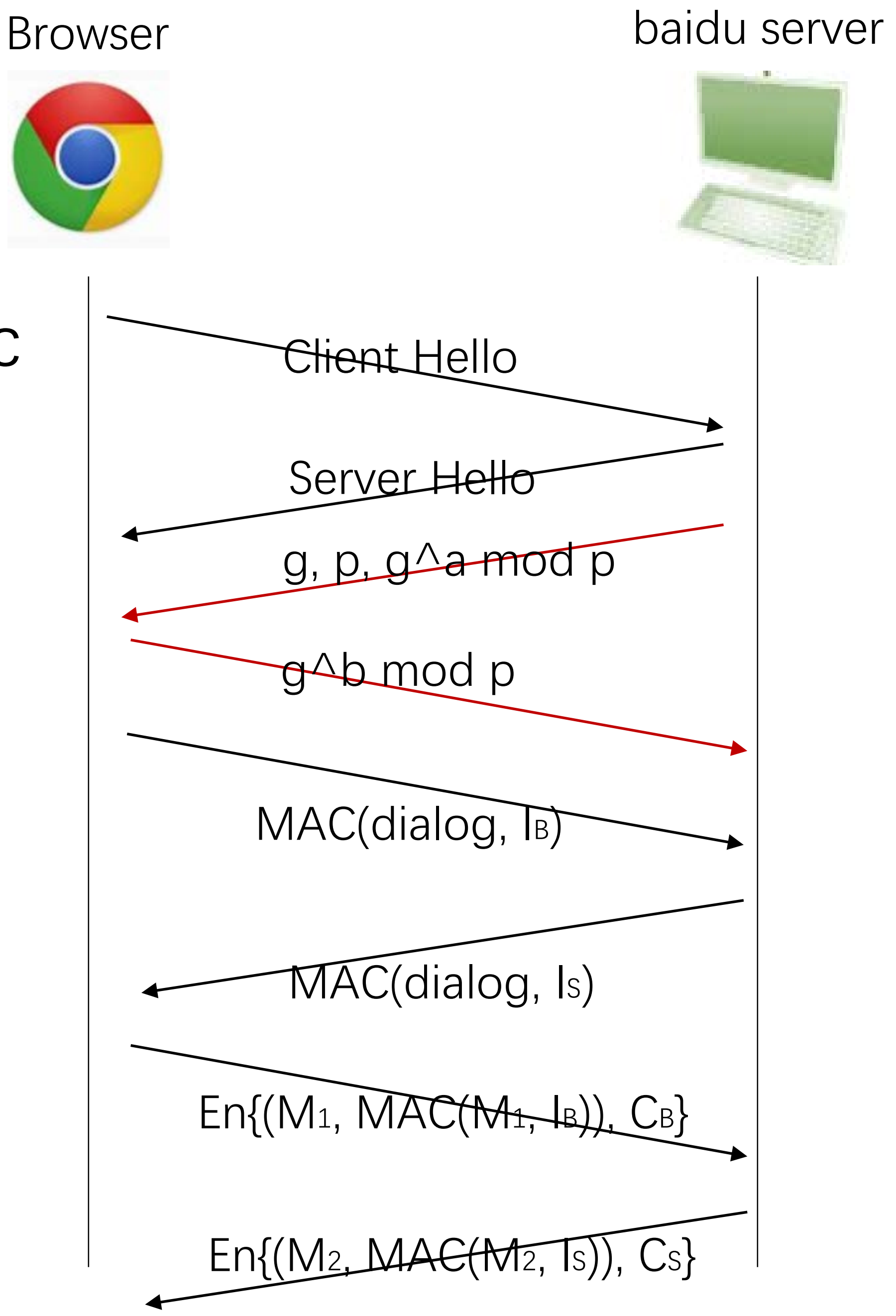


HTTPS via Diffie-Hellman Key Exchange

- Forward Secrecy
  - Attacker can log all the traffic (some day the private key of server might be compromised)
    - PKbaidu is known to the attacker in future
  - The attacker should not be able to read past conversations
  - In RSA, **PS** is encrypted by Pkbaidu. **R_B** and **R_S** are not encrypted
    - Attacker can calculate session keys (C_B, C_S) (I_B, I_S)
- Solution
  - Diffie-Hellman Key exchange

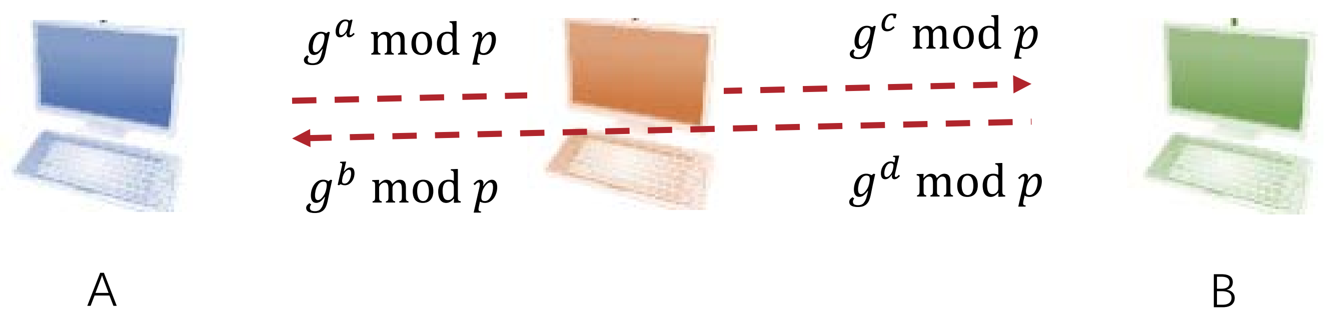
HTTPS via DH

- Server generates random **a**, sends public parameters and g^a mod p
- Browser generates random **b**, computes **PS** = g^ab mod p, sends g^b mod p to server
- Server also computes **PS** = g^ab mod p



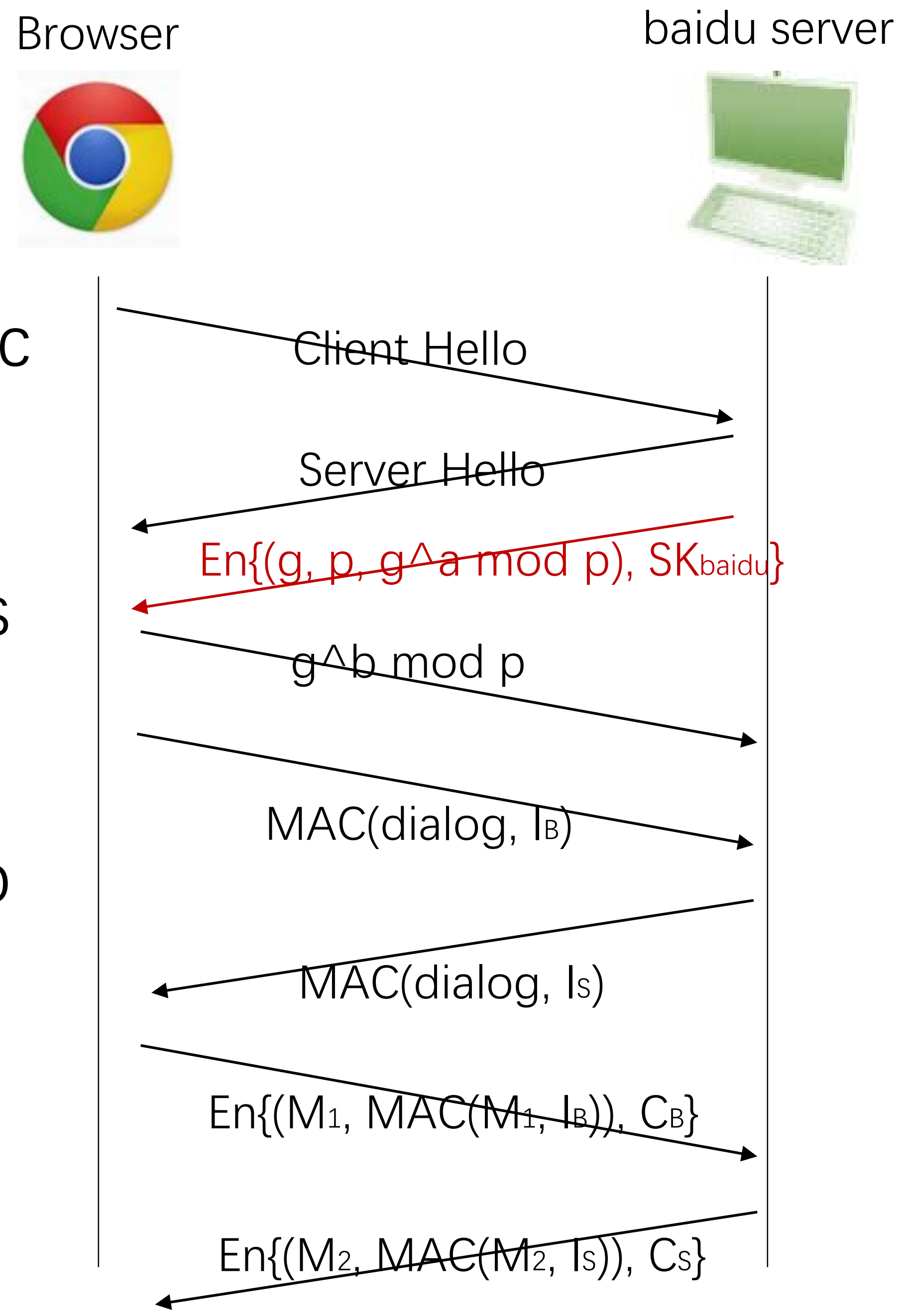
Diffie-Hellman Key Exchange

- Man in the middle attack
  - A cannot authenticate he is talking with B
- Diffie-Hellman Key Exchange is not secure without authentication



HTTPS via DH

- Server generates random **a**, sends public parameters and g^a mod p
  - Signed with servers' private key **SKbaidu**
- Browser generates random b, computes **PS** = g^ab mod p, sends g^b mod p to server
- Server also computes **PS** = g^ab mod p
- Attacker is not able to calculate PS, because **a** and b are not transmitted !

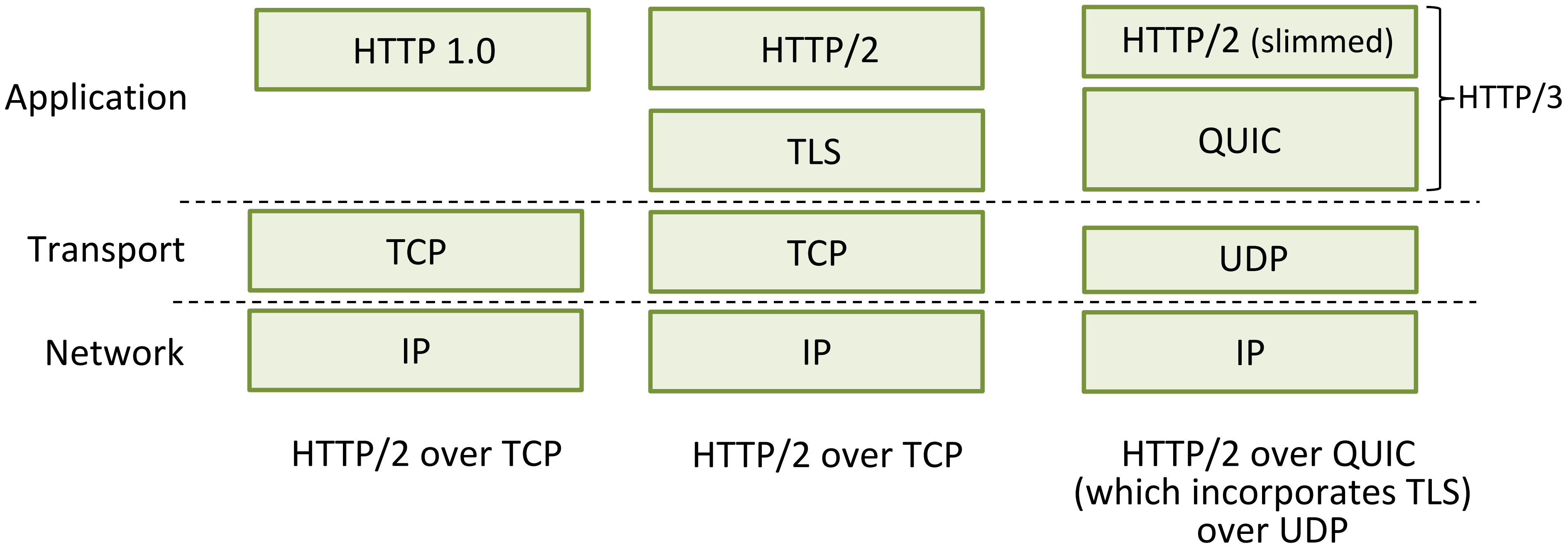


RSA and Diffie-Hellman Key Exchange are normally combined to improve security

Possible Attacks

- Re-ordering: man-in middle intercepts TCP segments and reorders (manipulating sequence #s in unencrypted TCP header)
  - record TLS sequence numbers in MAC
- Replay: attacker replays recorded sessions
  - use nonce
- Truncation attack: attacker forges TCP connection close segment
  - record types in MAC

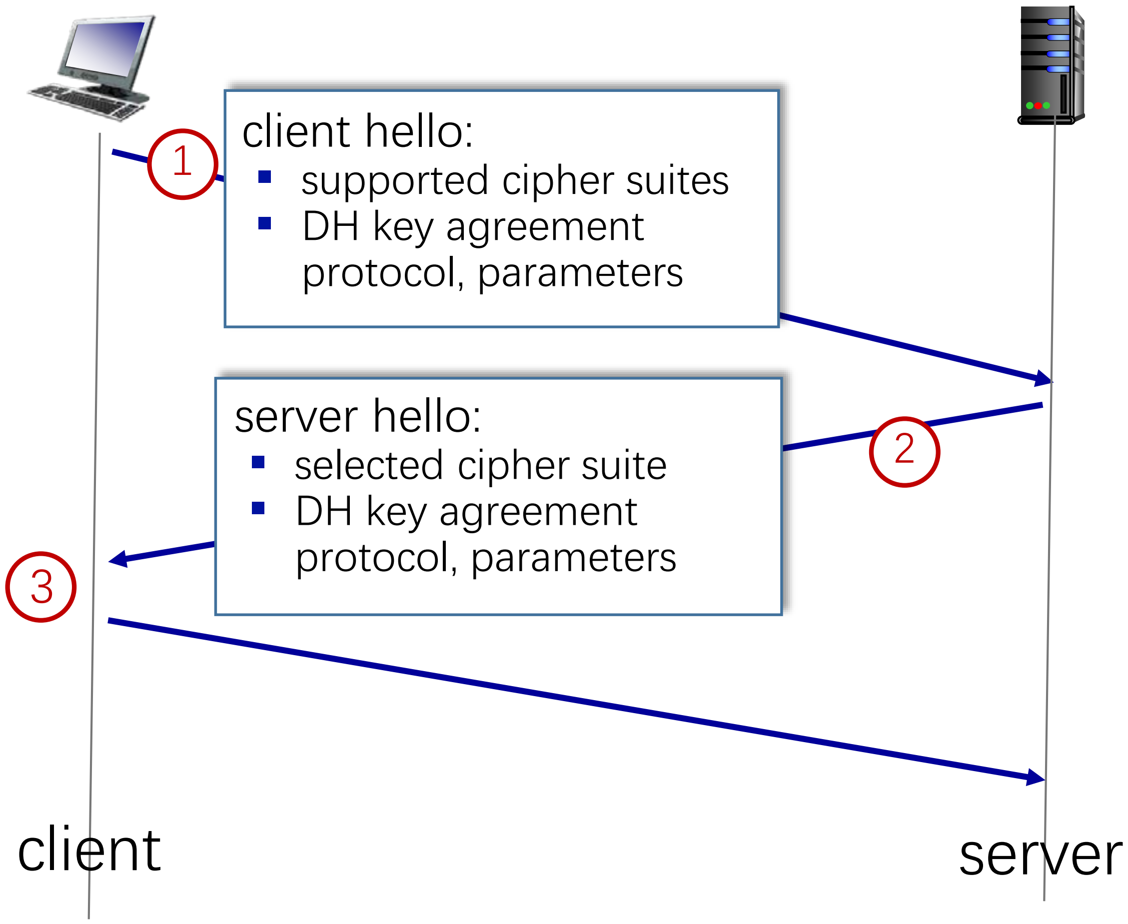
An HTTP view of TLS:



TLS: 1.3

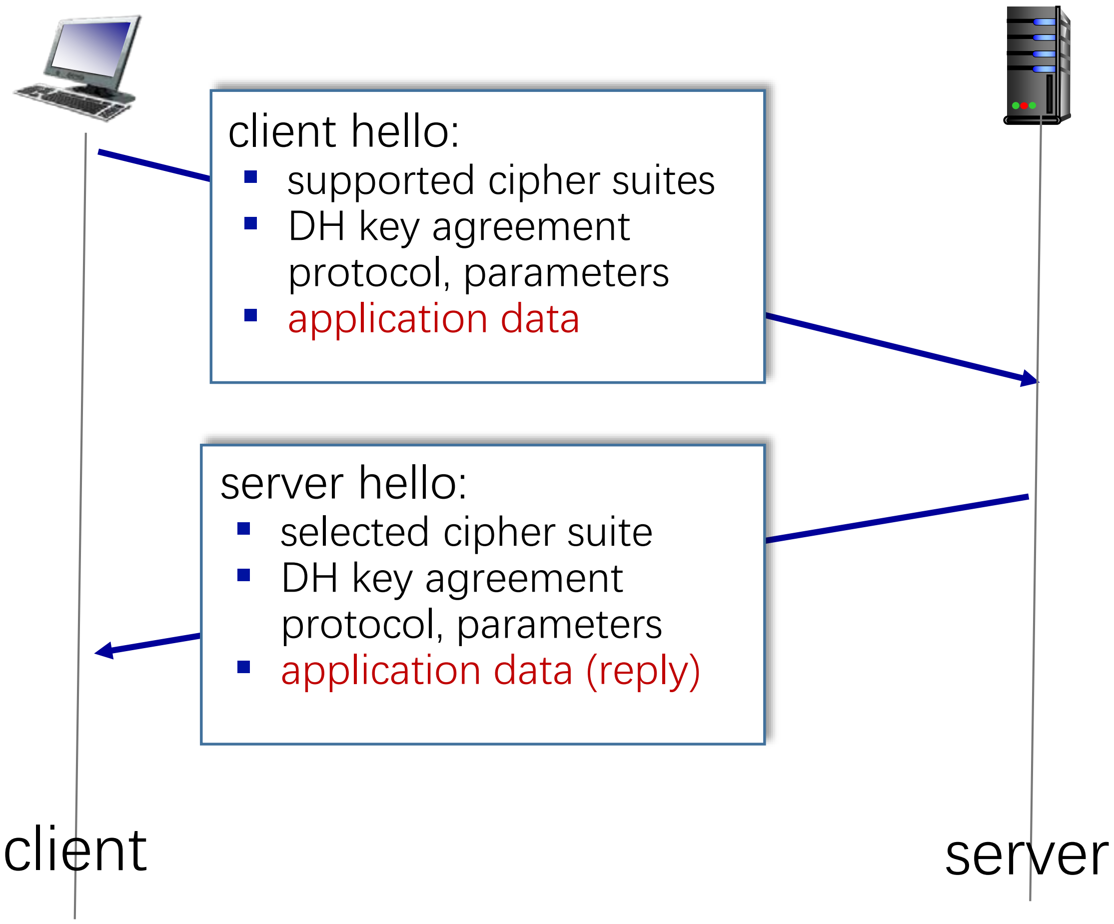
- TLS: 1.3 (2018)
  - only 5 cipher choices, rather than 37 choices (TLS 1.2)
  - requires Diffie-Hellman (DH) for key exchange, rather than DH or RSA
  - combined encryption and authentication algorithm ("authenticated encryption") for data rather than serial encryption, authentication
  - HMAC uses SHA (256 or 284) cryptographic hash function

TLS 1.3 Handshake: 1 RTT



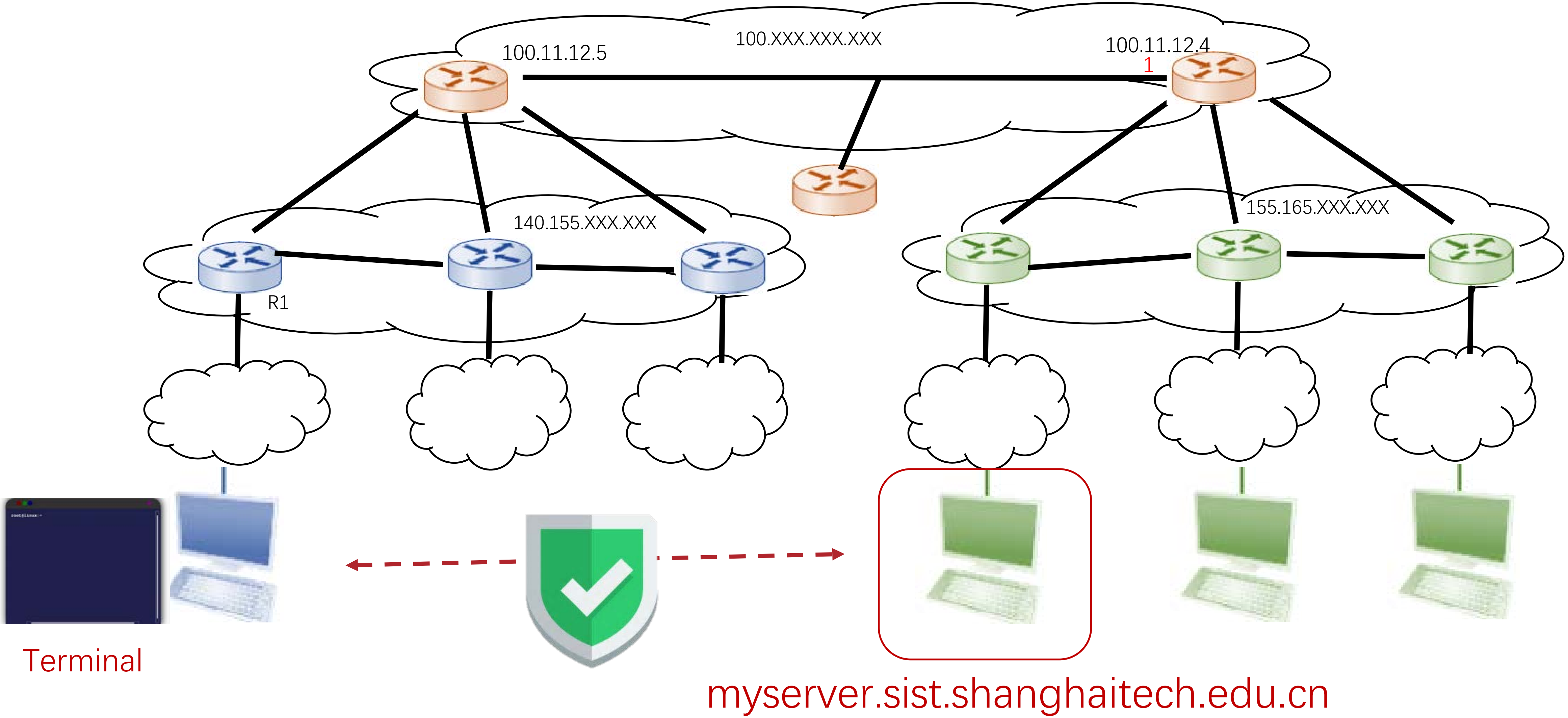
1. client TLS hello msg:
   - *guesses* key agreement protocol, parameters
   - indicates cipher suites it supports
2. server TLS hello msg chooses
   - key agreement protocol, parameters
   - cipher suite
   - server-signed certificate
3. client:
   - checks server certificate
   - generates key
   - can now make application request (e.g.., HTTPS GET)

TLS 1.3 Handshake: 0 RTT



- initial hello message contains encrypted application data!
  - "resuming" earlier connection between client and server
  - application data encrypted using "resumption master secret" from earlier connection
- vulnerable to replay attacks!
  - maybe OK for get HTTP GET or client requests not modifying server state

The Secure Shell (SSH)

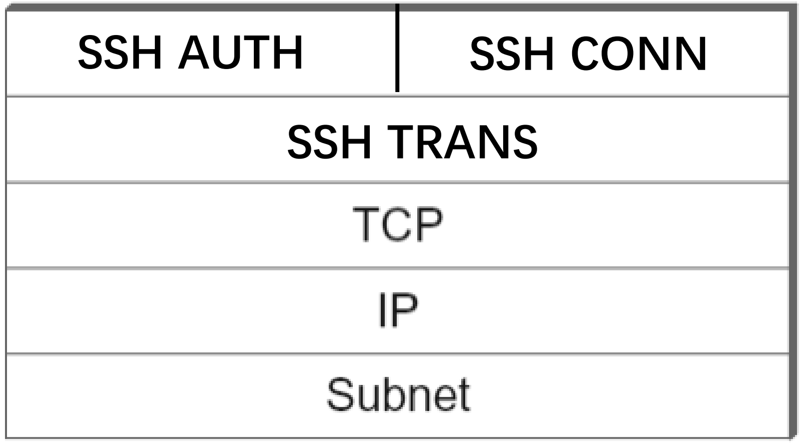


The Secure Shell (SSH)

- Developed by Tatu Ylönen, Helsinki University of Technology, Finland in 1995
- A Secure Version of Telnet
  - Message confidentiality
  - Message integrity
  - Client/server authentication

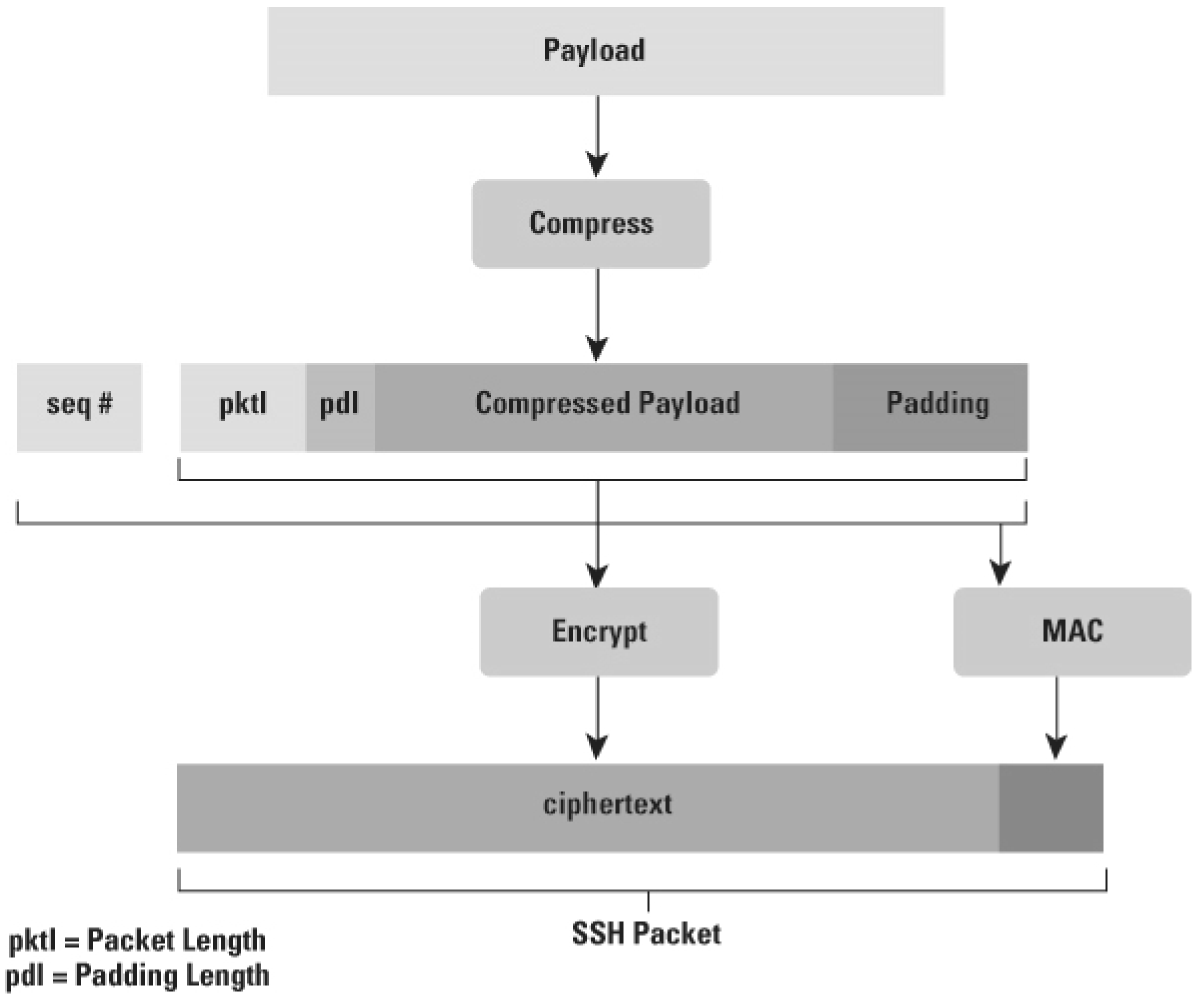
SSH v2 Protocols

- SSH Transportation Layer Protocol
  - Establish secure channel between client and server
  - Client authorizes server
- SSH User Authentication Protocol
  - Server authorizes client
- SSH Connection Protocol
  - Tunnel over secure channel



SSH-TRANS

- Protocol Steps
  - Establish TCP Connection
  - Exchange SSH Parameters
    - Distribution of server's public key
      - Manually through offline channel
      - Trust the first time
  - Key Exchange
  - Messages



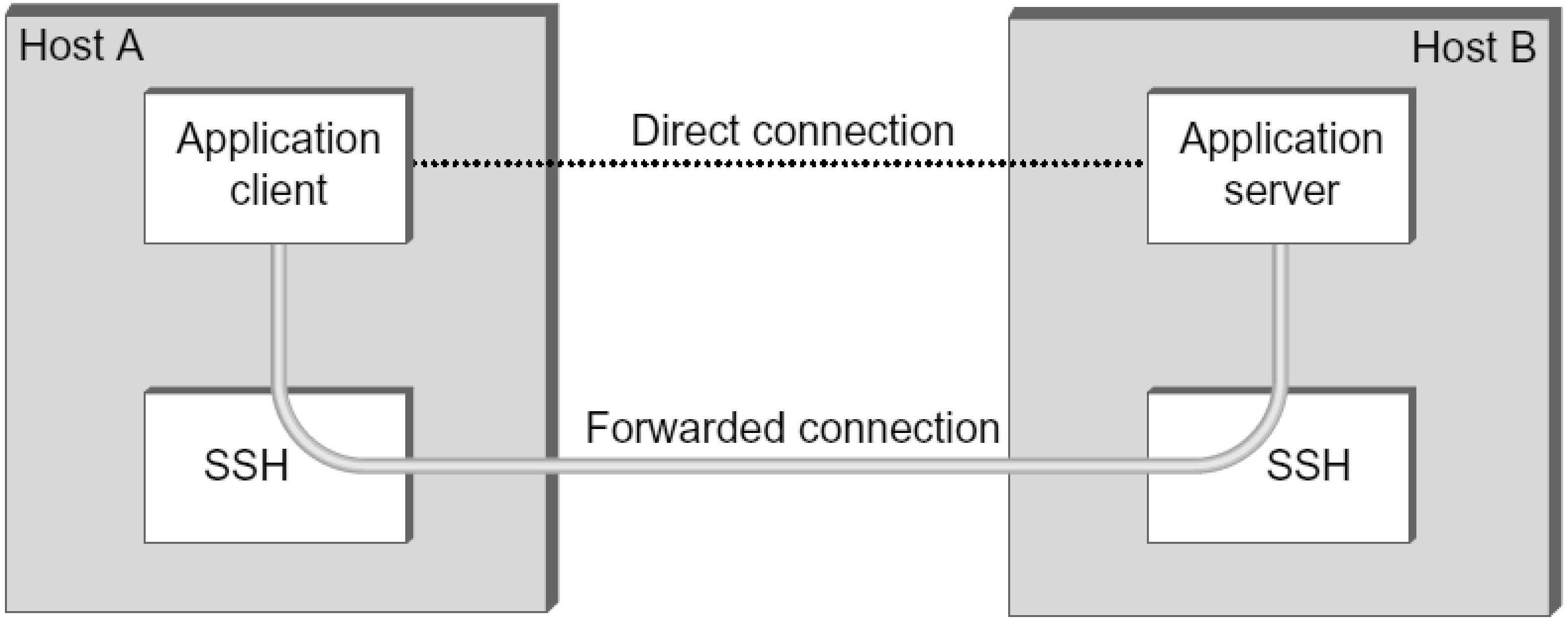
https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-46/124-ssh.html

SSH AUTH

- Server Authorizes Client
  - User Name + Password
  - RSA
  - Host-based Authentication

SSH CONN

- Examples
  - SFTP
  - SSH Tunnel



SSL v.s. SSH

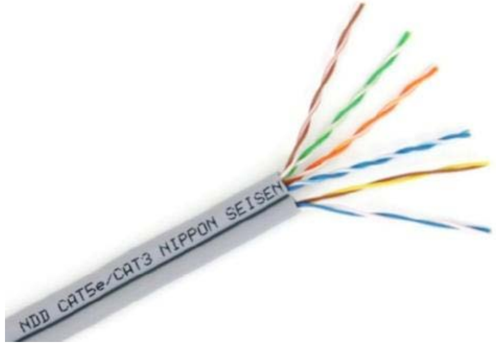
- Applications: Quite Different
  - SSL: browsers
  - SSH: remote consoles
- Techniques: Very Similar
  - Data integrity
    - HMAC (MD5, SHA-1)
  - Confidentiality
    - Symmetric-key ciphers: 3DES, AES, etc.
  - Session Key Establishment
    - RSA, DH, RSA+DH, etc.

Example Systems

- TLS/SSL
- SSH
- ➢ Wi-Fi Security

Wi-Fi Security

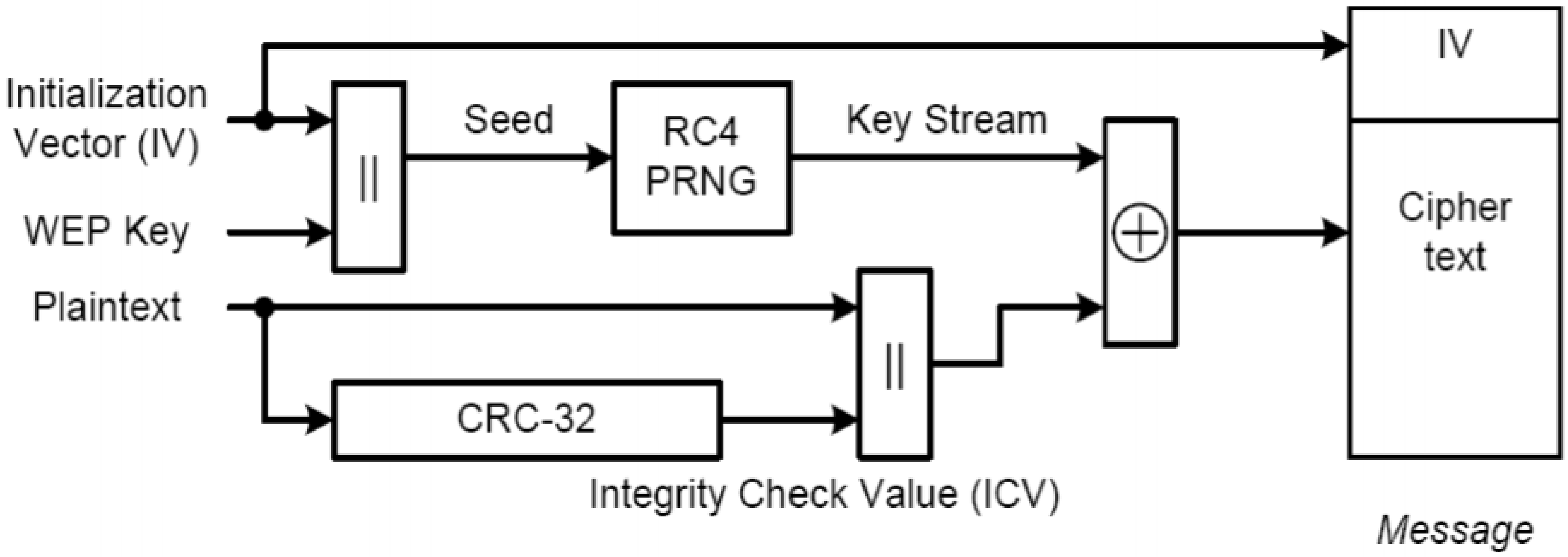
- Why ?
  - The broadcast nature of the wireless medium



Wi-Fi Security

- Authentication Method
  - Wired Equivalent Privacy (WEP)
    - Not secure
  - Wi-Fi Protected Access (WAP)

Wired Equivalent Privacy (WEP)

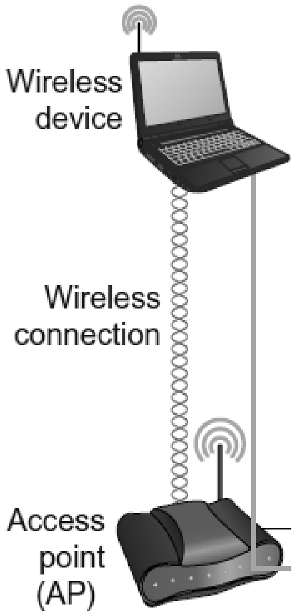


WEP Weakness

- Fluhrer-Mantin-Shamir (FMS) Attack
  - 24 bit IV, reuse very soon
  - Leverage the first two bytes of the plaintext
    - 0xAA
  - Collecting multiple messages to exploit the leakage

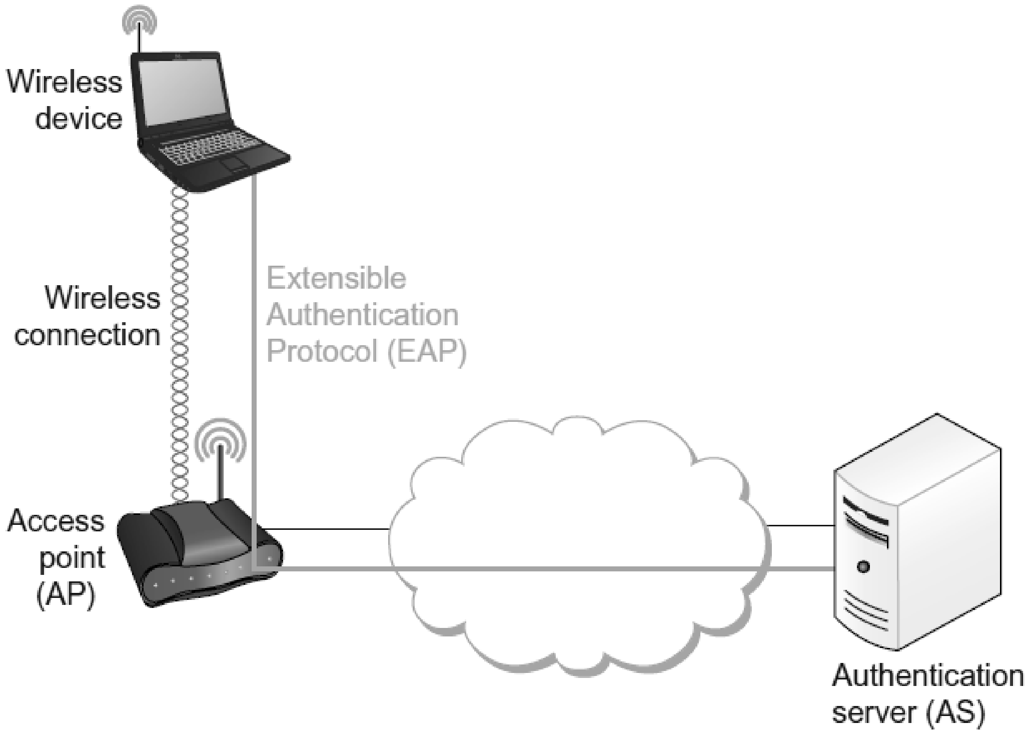
Authentication Directly

- Personal Mode



Authentication through EAP

- Enterprise Mode



Reference

- Textbook 8.4
- Some slides are adapted from http://www-net.cs.umass.edu/kurose_ross/ppt.htm by Kurose Ross
- http://inst.eecs.berkeley.edu/~cs161/sp18/