

# Lecture 10. PKI and Applications

Hui Xu

xuh@fudan.edu.cn



# Recap

- We have learned several different cryptography approaches
  - Asymmetric encryption: RSA
  - Symmetric encryption
  - Hash
- Question: How to use them in practice?
  - Key distribution and management
  - Usage of cryptography algorithms
- In this lecture, we focus on the centralized trust model
  - *i.e.*, there is an authority that all participants can trust

# Practice 1

- Given  $p = 3$ ,  $q = 11$ ,  $e = 7$ ,
  - 1) calculate the private key
  - 2) use the private key to encrypt  $M=5$
  - 3) decrypt the previous encrypted data with the public key

## Practice 2

- Analyze the security of the following hash function where  $M = a_1, \dots, a_n$

$$Hash(M) = \left( \sum_{i=1}^t a_i^2 \right) \bmod n$$

# Outline

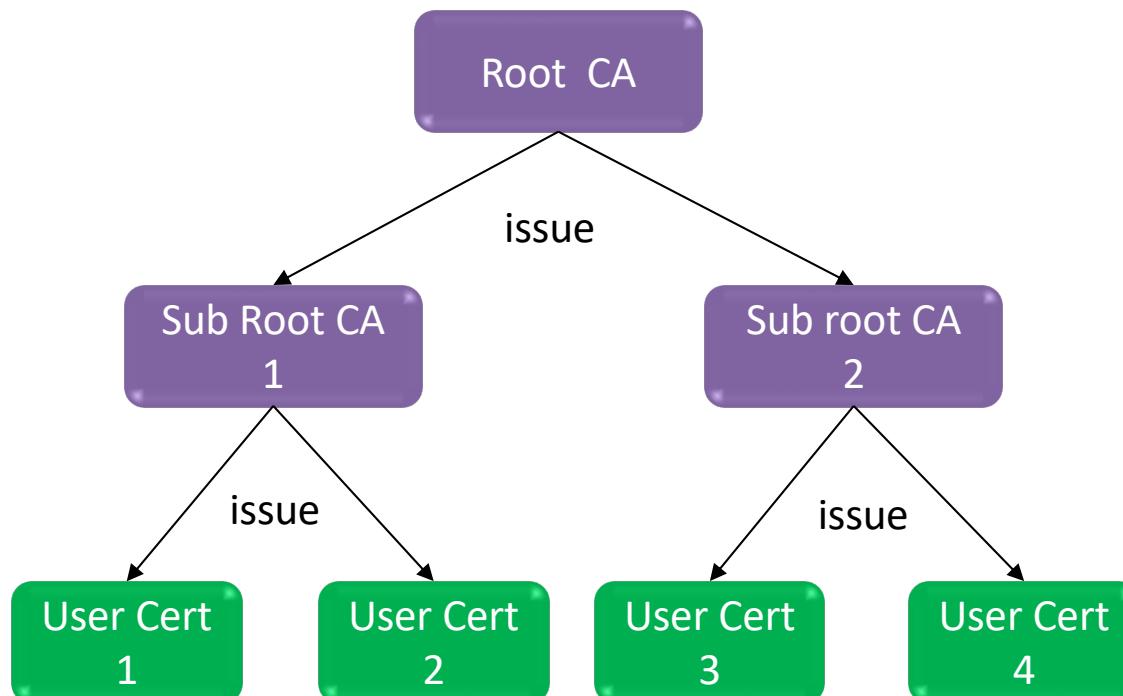
- ❖ 1. Public Key Infrastructure
- ❖ 2. Digital Signature and Envelope
- ❖ 3. Transport Layer Security
- ❖ 4. In-class Practice

# 1. Public Key Infrastructure

---

# Public Key Infrastructure

- A centralized trust framework for digital certificate management
- Certificate Authority (CA): Issues and verifies digital certificates.
- Digital Certificates: Certifies ownership of a public key, linking it to an entity.

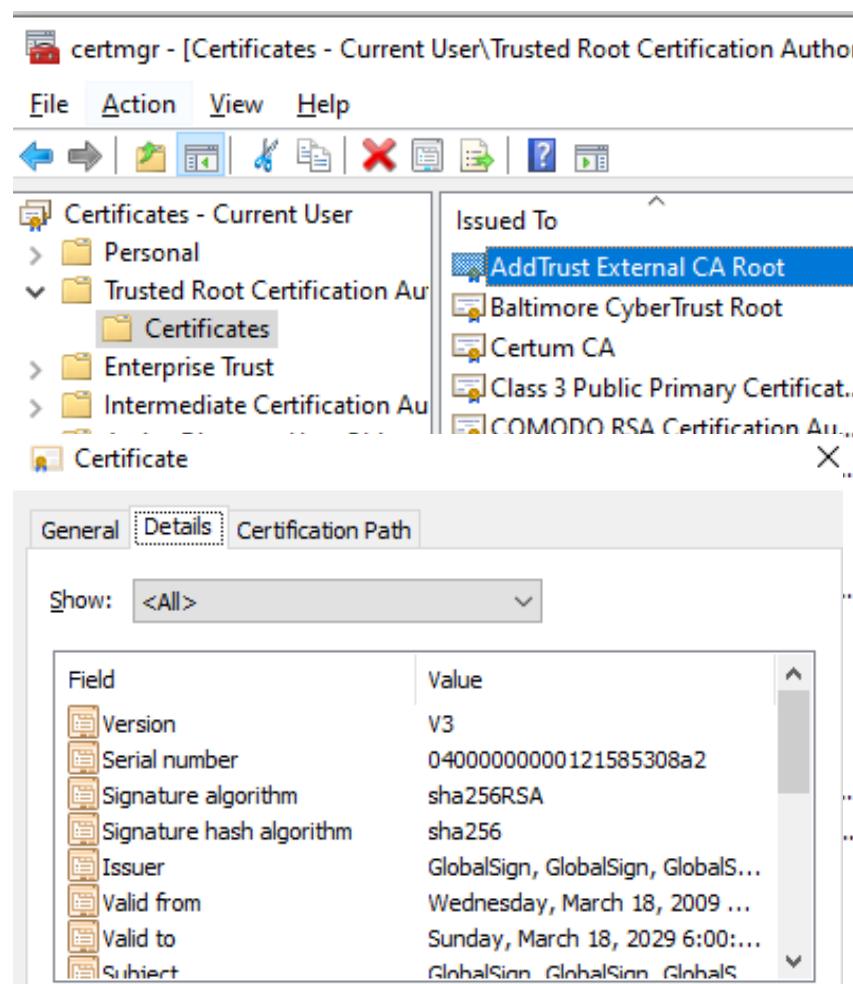


# Essential Fields of a Digital Cert

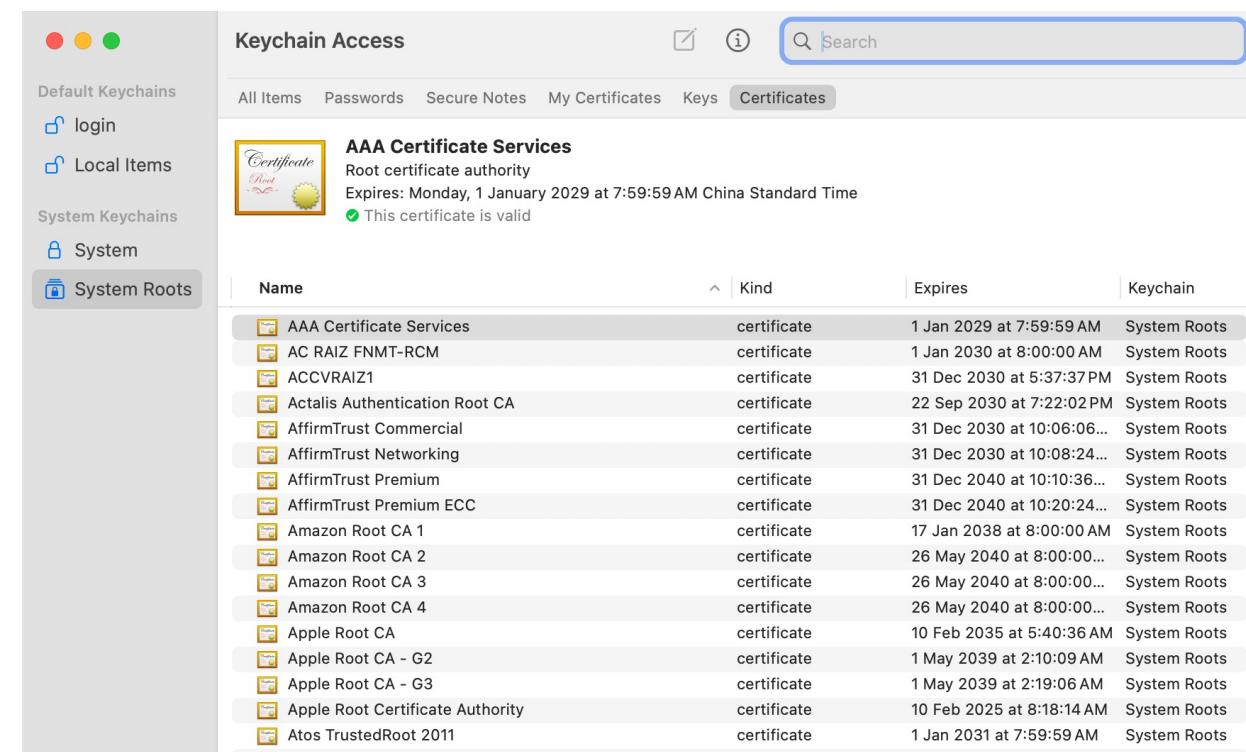
- **Version:** X.509 standard being used (commonly v3).
- **Serial Number:** a unique identifier assigned by the CA to distinguish each certificate it issues.
- **Subject:** The entity the certificate is issued to.
- **Issuer:** Identifies the CA that issued the certificate.
- **Validity Period:** The time frame for which the certificate is valid.
- **Signature:** Generated by the CA for authenticity check.

# View the Certs on your PC

Win + R: certmgr.msc



MacOS: Keychain Access



# Demonstration of Cert Issuing: User Cert

**User key generation** (assume using RSA as the public key algorithm):

$p=5, q=11, e=3$

=> public key: (3, 55), private key: 27

**User cert issuing:**

**Version:** x509.v3

**Serial Number:** 100202

**Subject:** CN = Alice, O = Fudan University, C = CN

**Issuer:** CN = RootCA, O = Fudan University, C = CN

**Validity:** 2024 - 0901 to 2027-07-31

**Public Key:** (3, 55)

**Sign(Hash(Ver || SN || Subject || Issuer || Validity || PubKey), PriKey<sub>rootCA</sub>)**

# Demonstration of Cert Issuing: Root Cert

**Root key generation** (assume using RSA as the public key algorithm):

$p=3, q=11, e=7$

=> public key: (7, 33), private key: 3

**Root cert issuing** (who signs the cert of the root CA):

**Version:** x509.v3

**Serial Number:** 100001

**Subject:** CN = RootCA, O = Fudan University, C = CN

**Issuer:** CN = RootCA, O = Fudan University, C = CN

**Validity:** 2000 - 0101 to 2099-12-31

**Public Key:** (7, 33)

**Sign(Hash(Ver || SN || Subject || Issuer || Validity || PubKey), PriKey<sub>rootCA</sub>)**

# Experiment: Generate Your Own Cert

CA initialization

Key Pair  Use site's private key  Use my own key  Generate new key  Import from key store

Key type RSA  Generate key only

Private key

```
-----BEGIN RSA PRIVATE KEY-----MIICWwlBAAKBgQC/omGYAUsoSVBA/MYe7LzHt6aaibLE+UBF1n1HckWSY90hpHMBp/u2C24s3G/sWloxt119rUo90VLBNjw7UWV01MHPjwRi3cVP/IS04Enq3eTfNX4QejZBly/MMHAh4BotO951vHJnAbEOcS2dIvo86HeA7GvnU2OqLFFsCiYgGQIDAQABAn9ea1mgwZ/4iolKGWjTQComAgzeSaW1hQX5scOb9Sy+jLqnmNBtD/nmvSdVmpXtRb6q3dBPMb4gS9T0iUgF0wJ2FO6db5I9ejMcJpdE8fO6ZlJrXypaF380+qzEZgP
```

Validate & deduce public

Public key

```
-----BEGIN PUBLIC KEY-----MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/omGYAUsoSVBA/MYe7LzHt6aaibLE+UBF1n1HckWSY90hpHMbp/u2C24s3G/sWloxt119rUo90VLBNjw7UWV01MHPjwRi3cVP/IS04Enq3eTfNX4QejZBly/MMHAh4BotO951vHJnAbEOcS2dIvo86HeA7GvnU2OqLFFsCiYgGQIDAQAB
```

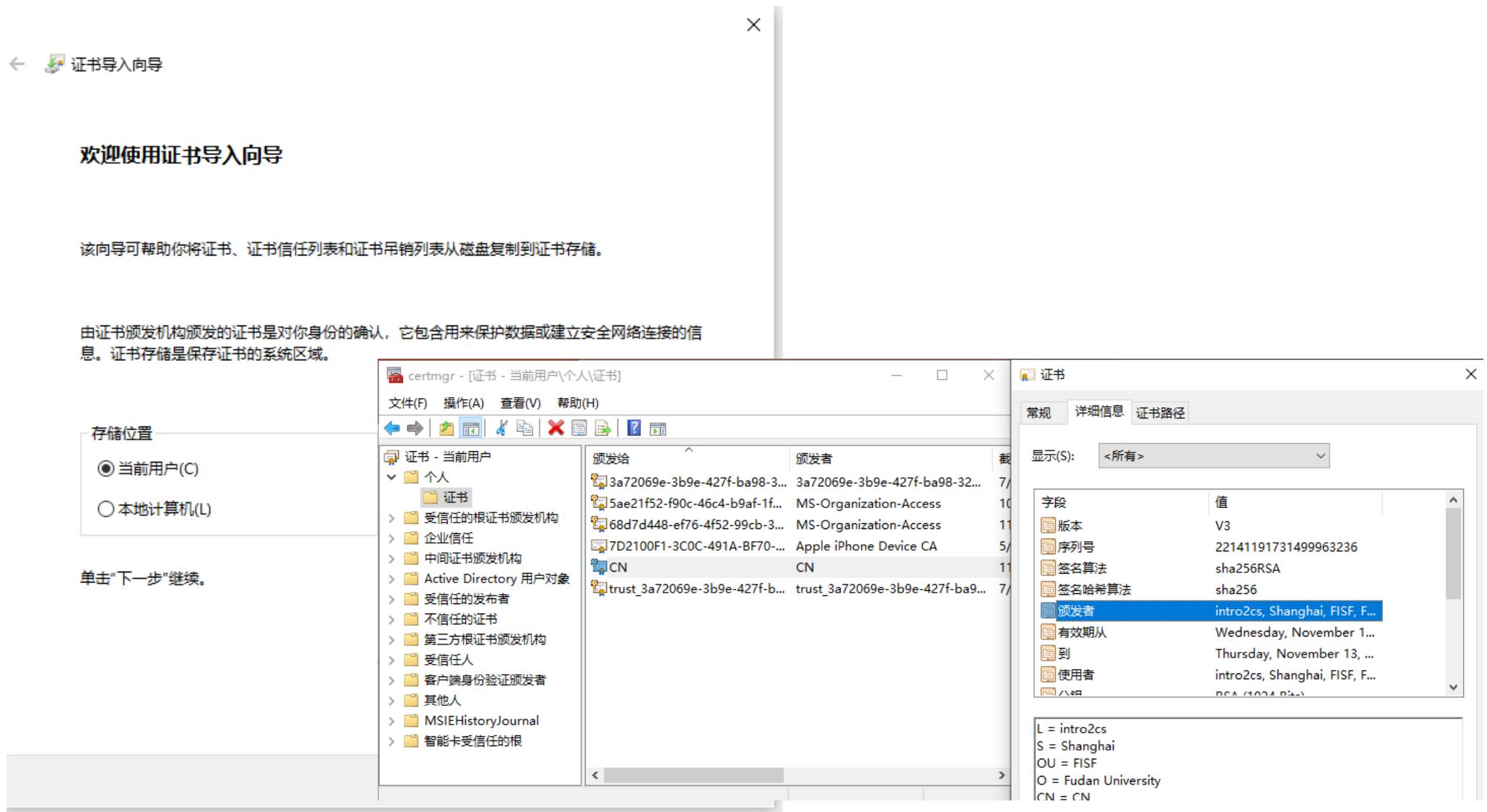
Certificate Attribute  Use site's template  Custom self-signed  Use signed certificate

Subject DN

CN CN	O Fudan University	OU FISF	L	ST Shanghai
C intro2cs	<input type="button" value=""/>			

Export to key store

# Experiment: Install The Cert



# Private Key Protection

- Software approach: Encrypt the private key with a password.
- Security chips:
  - Generate key pairs or import key pairs.
  - Perform encryption and decryption operations.
  - Protect the key from being exported.



# Cert Revocation

- Publish to a cert revocation list signed by the Root CA

AAA Certificate Services  
Signature 200 bytes. 00 00 10 02 10 9D E0 FF ...

---

**Extension** Key Usage ( 2.5.29.15 )  
**Critical** YES  
**Usage** Key Cert Sign, CRL Sign

**Extension** Basic Constraints ( 2.5.29.19 )  
**Critical** YES  
**Certificate Authority** YES

**Extension** Subject Key Identifier ( 2.5.29.14 )  
**Critical** NO  
**Key ID** A0 11 0A 23 3E 96 F1 07 EC E2 AF 29 EF 82 A5 7F D0 30 A4 B4

**Extension** CRL Distribution Points ( 2.5.29.31 )  
**Critical** NO  
**URI** <http://crl.comodoca.com/AAACertificateServices.crl>  
**URI** <http://crl.comodo.net/AAACertificateServices.crl>

---

**Fingerprints**

**SHA-256** D7 A7 A0 FB 5D 7E 27 31 D7 71 E9 48 4E BC DE F7 1D 5F 0C 3E  
0A 29 48 78 2B C8 3E E0 EA 69 9E F4

**SHA-1** D1 EB 23 A4 6D 17 D6 8F D9 25 64 C2 F1 F1 60 17 64 D8 E3 49

## 2. Digital Signature and Envelope

---

# Security Goal: CIAN

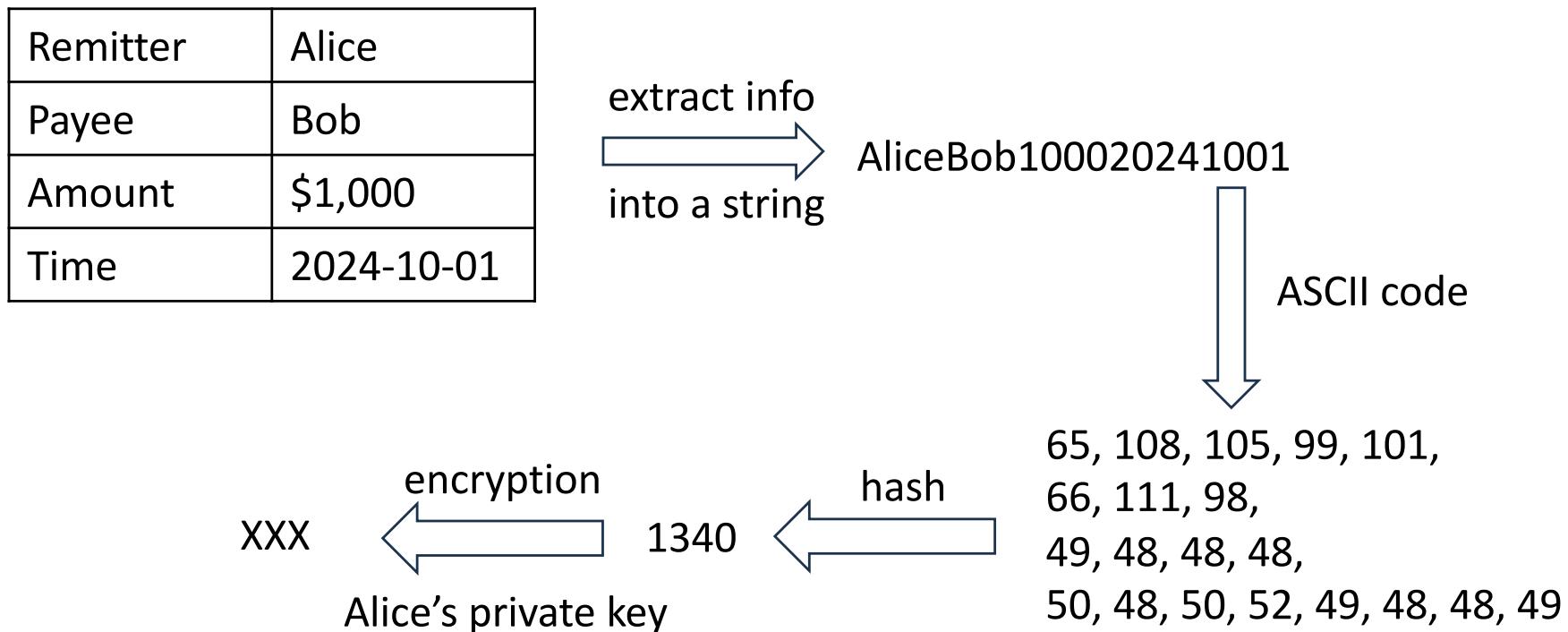
- **Confidentiality (C):** Ensuring that sensitive information is only accessible to authorized individuals or systems.
- **Integrity (I):** Guaranteeing that data remains accurate, unaltered, and trustworthy throughout its lifecycle
- **Availability (A):** Ensuring that information and resources are available to authorized users when needed.
- **Non-repudiation (N):** Providing proof of the origin and integrity of data, ensuring that actions or communications cannot later be denied by the entity that performed them.

# Digital Signature

- A digital signature is a cryptographic method used to validate the authenticity and integrity of a digital message, software, or document.
- **Key Characteristics:**
  - Authentication: Confirms the identity of the sender.
  - Integrity: Ensures the message hasn't been tampered with.
  - Non-Repudiation: Prevents the sender from denying they sent the message.
- **Applications:** Used widely in e-signatures, financial transactions, contract management, and secure email communication.

# How It Works? Sign

- **Hashing:** The document is hashed into a fixed-length string.
- **Encryption:** The hash is encrypted with the sender's private key.



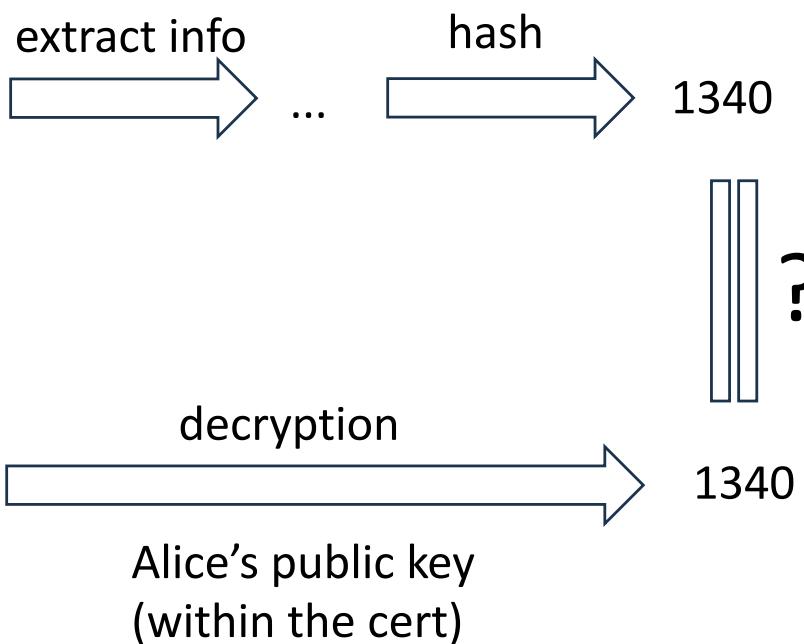
# How It Works? Verification

- The recipient uses the sender's public key to verify the signature.
- The recipient uses the root certificate to verify the sender's certificate.

Remitter	Alice
Payee	Bob
Amount	\$1,000
Time	2024-10-01

Received from Alice

Signature: XXX  
(Received from Alice)



# Question

- What is the benefit of hashing before RSA for digital signature? Is it necessary?
- Can you design a login mechanism based on digital signature?

# Experiment: Sign an XML file

Initialize signer private key and certificate

Key pair  Use site's private key  Use my own key  Import from key store

Browse key store 浏览... data.p12

Alias

Key store data Password key store .....  
Password entry

Signature algorithm SHA-256 with RSA ▾

Examine key store

XML signature property

XML data 浏览... 未选择文件。  
<xml>to be signed</xml> <xml>to be signed</xml>

Signature Scheme XMLSig Version 2.0

Signature type  Enveloped  Enveloping  Detached

Canonicalization Algorithm Canonical XML 1.0

Namespace Input prefix namespace. May be empty Input URI namespace. May be empty

Subject name  Add X509 subject name

Node to sign  Choose from list Choose nodes to sign. Sign whole document as default

Sign

The screenshot shows the 'Initialize signer private key and certificate' section with 'Import from key store' selected. It displays fields for 'Browse key store' (data.p12), 'Alias' (empty), 'Key store data' (Password key store, password masked), and 'Signature algorithm' (SHA-256 with RSA). The 'XML signature property' section contains 'XML data' with the XML code '<xml>to be signed</xml>' and its copy. Configuration for the signature includes 'Signature Scheme' (XMLSig Version 2.0), 'Signature type' (Enveloped), 'Canonicalization Algorithm' (Canonical XML 1.0), and two 'Namespace' input fields. At the bottom, there are options for 'Subject name' (checkbox) and 'Node to sign' (checkbox, 'Choose from list'). A large blue 'Sign' button is at the bottom.

# Experiment: Verify the Signed XML file

XML File

Signature type  Attached signature  Detached signature

XML signed data  data(2).txt

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?><xml>to be  
signed<Signature xmlns="http://www.w3.org/2000/09/  
xmldsig#"><SignedInfo><CanonicalizationMethod Algorithm="http://www.w3.org/  
TR/2001/REC-xml-c14n-20010315"/><SignatureMethod Algorithm="http://  
www.w3.org/2001/04/xmldsig-more#rsa-sha256"/><Reference  
URI=""><Transforms><Transform Algorithm="http://www.w3.org/2000/09/
```

Signature Scheme

Public key  Get from document  Get from certificate  Get from file

XML validation result

Signature #1

Integrity Document has not been modified since signing

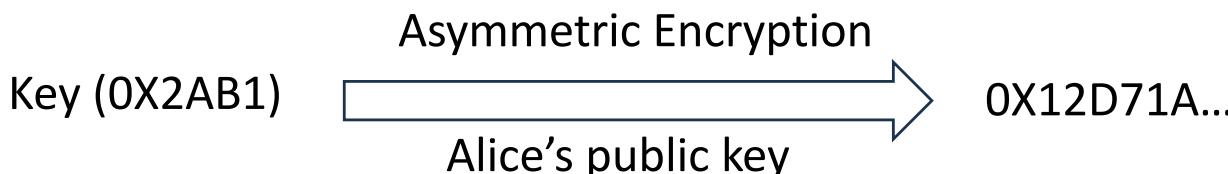
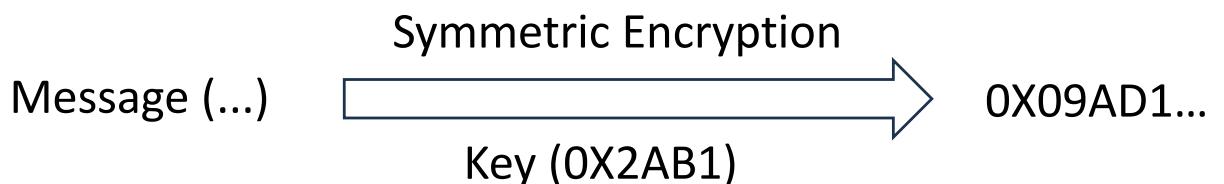
Certificates DN: L=intro2cs,ST=Shanghai,OU=FISF,O=Fudan University,CN=CN

# Digital Envelope

- A digital envelope is a secure method for transmitting sensitive data by combining encryption techniques to ensure both confidentiality and integrity of the message.
- **Benefits:**
  - Confidentiality: Ensures only the intended recipient can read the message.
  - Efficiency: Combines fast symmetric encryption with secure asymmetric encryption.
  - Scalability: Effective for transmitting large files securely.
- **Applications:** Used in email encryption, secure data exchange, and digital communication protocols.

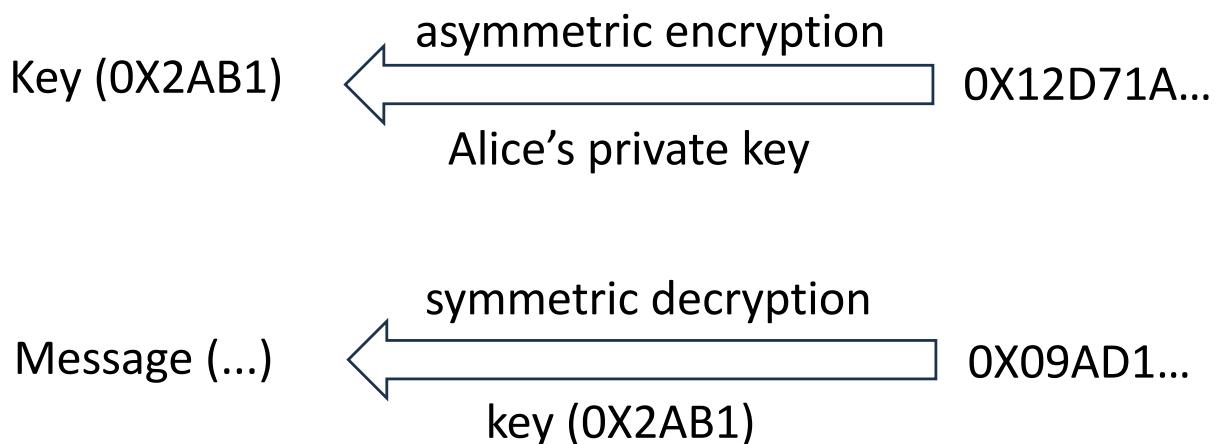
# How It Works? Encryption

- **Symmetric Key Encryption:** The message is encrypted with a randomly generated symmetric key (e.g., AES).
- **Asymmetric Key Encryption:** The symmetric key is then encrypted using the recipient's public key.
- **Transmission:** The encrypted message and the encrypted symmetric key (the "digital envelope") are sent to the recipient.



# How It Works? Decryption

- **Decryption by Recipient:** The recipient decrypts the symmetric key using their private key.
- The decrypted symmetric key is used to decrypt the original message.



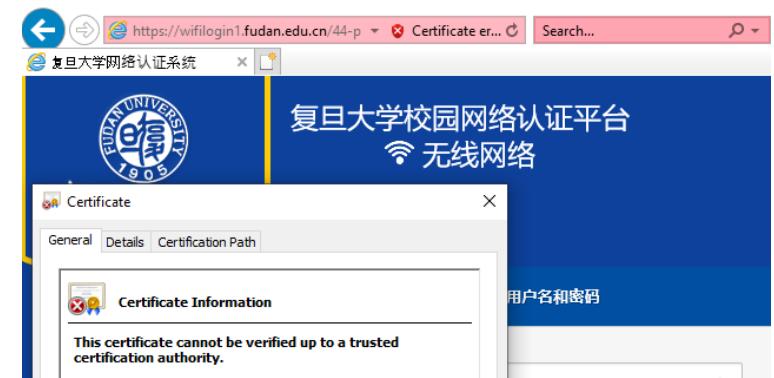
## 3. Transport Layer Security

---

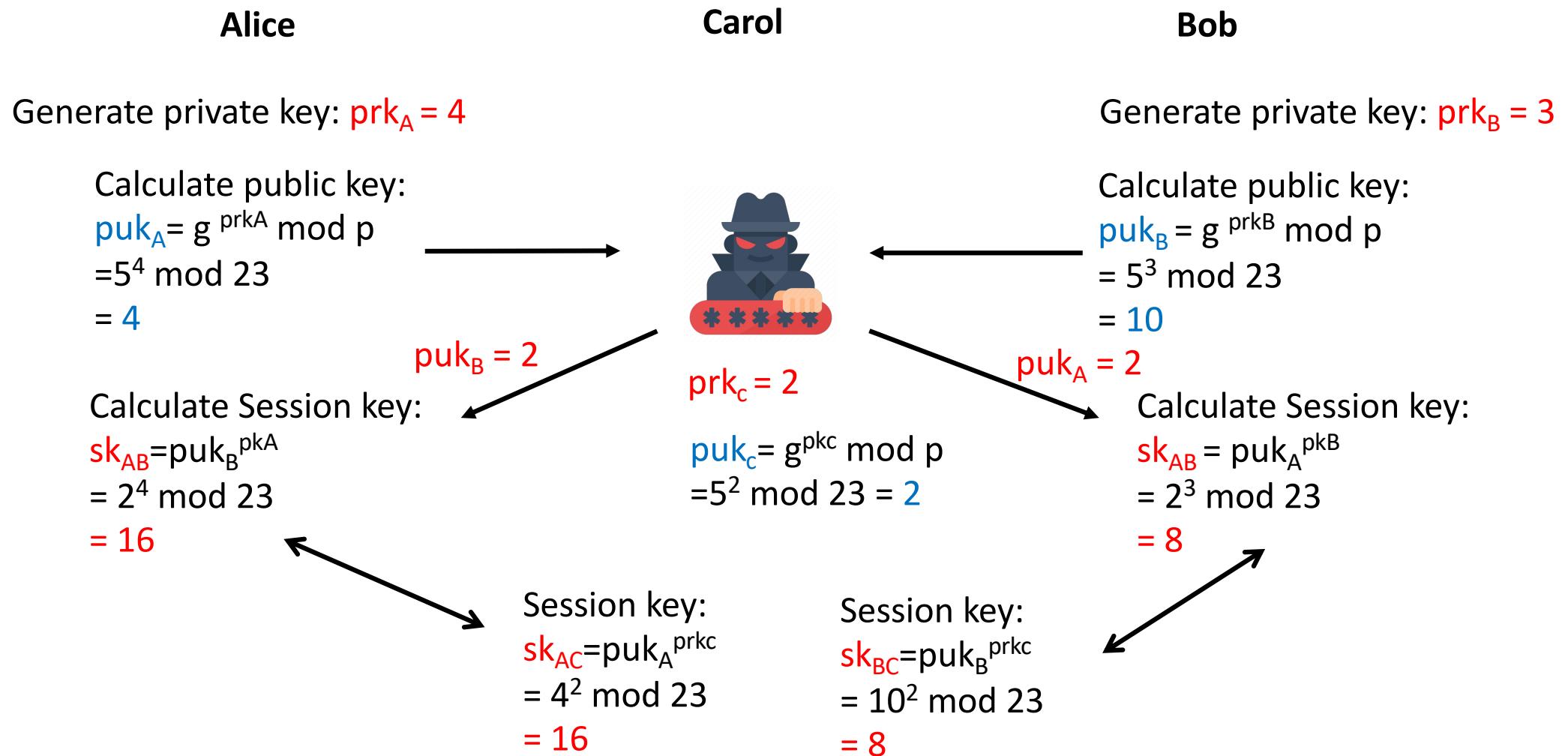
Previously known as SSL (secure socket layer)

# TLS/HTTPS

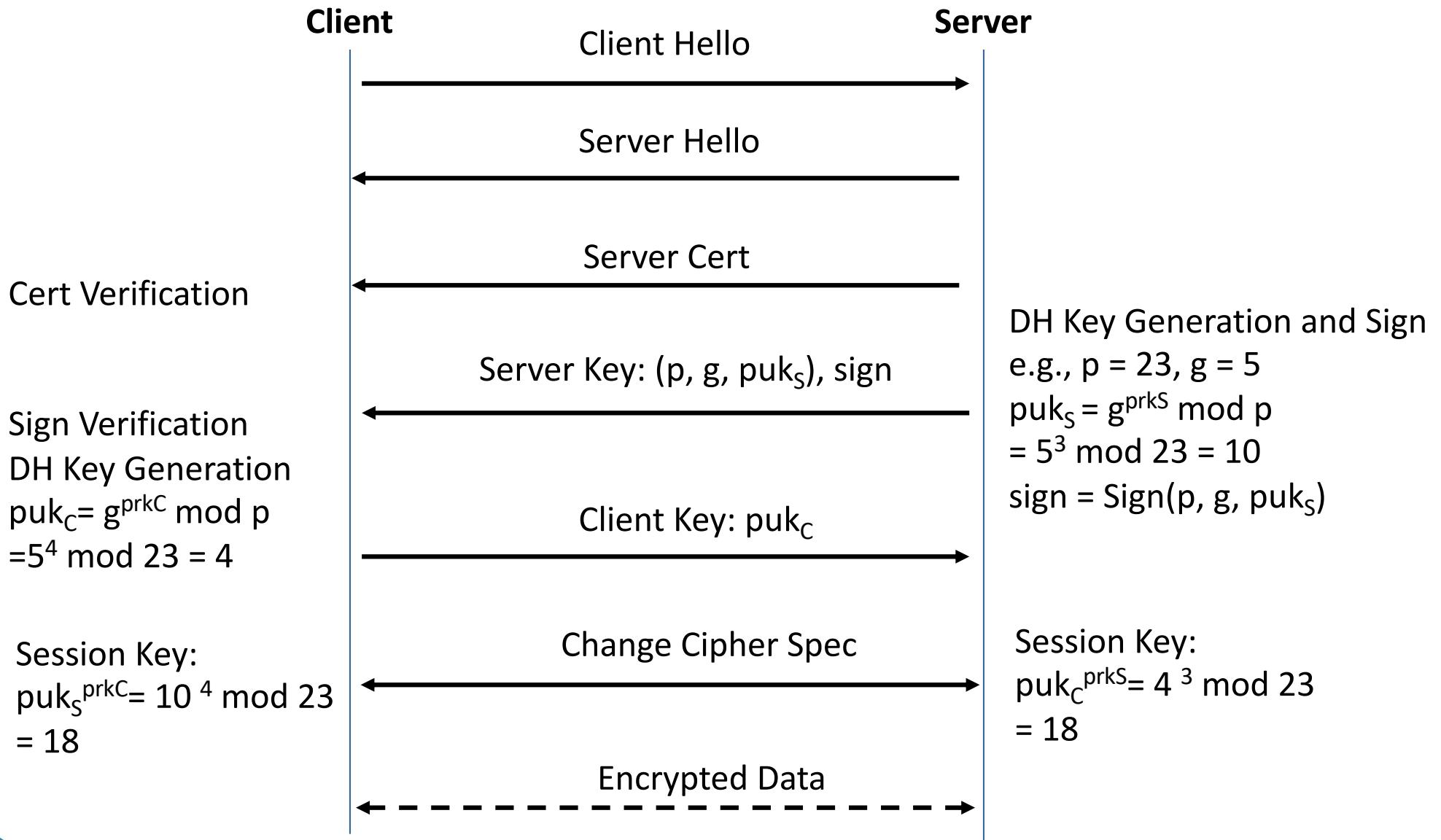
- TLS is a protocol designed to secure data transmitted over networks.
  - Useful for network traffic encryption.
  - Generally based on digital certificates.
- HTTPS: HTTP over TLS
  - The website is configured with digital certificates.
  - Useful to prevent phishing attacks (forgery websites).
    - For example, a fake website that looks exactly the same as the target web page.
    - Attackers can steal your account and password if you enter your credentials.



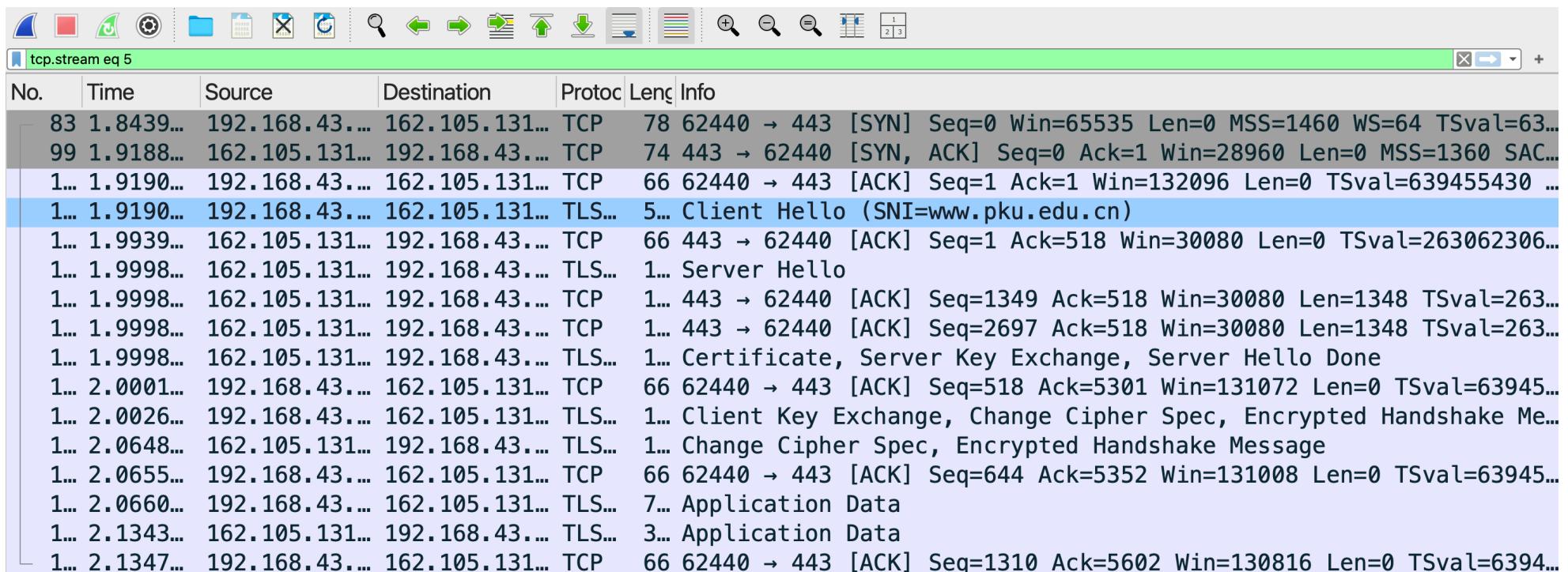
# Recap: MITM Attack for Diffie-Hellman Key Exchange



# Mechanism (Simplified 1-Way TLS)



# Experiment: TLS



The screenshot shows a Wireshark capture of a TLS handshake. The packet list is filtered to show only stream 5. The columns in the table are: No., Time, Source, Destination, Protocol, Length, and Info. The Info column provides detailed information about each packet, such as sequence numbers, acknowledgments, window sizes, and message types like SYN, ACK, and Client Hello.

No.	Time	Source	Destination	Protocol	Length	Info
83	1.8439...	192.168.43...	162.105.131...	TCP	78	62440 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=63...
99	1.9188...	162.105.131...	192.168.43...	TCP	74	443 → 62440 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1360 SAC...
1...	1.9190...	192.168.43...	162.105.131...	TCP	66	62440 → 443 [ACK] Seq=1 Ack=1 Win=132096 Len=0 TSval=639455430 ...
1...	1.9190...	192.168.43...	162.105.131...	TLS...	5...	Client Hello (SNI=www.pku.edu.cn)
1...	1.9939...	162.105.131...	192.168.43...	TCP	66	443 → 62440 [ACK] Seq=1 Ack=518 Win=30080 Len=0 TSval=263062306...
1...	1.9998...	162.105.131...	192.168.43...	TLS...	1...	Server Hello
1...	1.9998...	162.105.131...	192.168.43...	TCP	1...	443 → 62440 [ACK] Seq=1349 Ack=518 Win=30080 Len=1348 TSval=263...
1...	1.9998...	162.105.131...	192.168.43...	TCP	1...	443 → 62440 [ACK] Seq=2697 Ack=518 Win=30080 Len=1348 TSval=263...
1...	1.9998...	162.105.131...	192.168.43...	TLS...	1...	Certificate, Server Key Exchange, Server Hello Done
1...	2.0001...	192.168.43...	162.105.131...	TCP	66	62440 → 443 [ACK] Seq=518 Ack=5301 Win=131072 Len=0 TSval=63945...
1...	2.0026...	192.168.43...	162.105.131...	TLS...	1...	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Me...
1...	2.0648...	162.105.131...	192.168.43...	TLS...	1...	Change Cipher Spec, Encrypted Handshake Message
1...	2.0655...	192.168.43...	162.105.131...	TCP	66	62440 → 443 [ACK] Seq=644 Ack=5352 Win=131008 Len=0 TSval=63945...
1...	2.0660...	192.168.43...	162.105.131...	TLS...	7...	Application Data
1...	2.1343...	162.105.131...	192.168.43...	TLS...	3...	Application Data
1...	2.1347...	192.168.43...	162.105.131...	TCP	66	62440 → 443 [ACK] Seq=1310 Ack=5602 Win=130816 Len=0 TSval=6394...

# TCP Handshake: SYN

Screenshot of Wireshark showing a TCP handshake between two hosts. The timeline shows the sequence of packets:

- Packet 83: SYN (Seq=0, Win=65535, Len=0, MSS=1460, TSval=1.8439ms)
- Packet 99: SYN, ACK (Seq=0, Ack=1, Win=28960, Len=0, MSS=1360, TSval=1.9188ms)
- Packet 100: ACK (Seq=1, Ack=1, Win=132096, Len=0, TSval=1.9190ms)
- Packet 101: Client Hello (SNI=www.pku.edu.cn)
- Packet 102: ACK (Seq=1, Ack=518, Win=30080, Len=0, TSval=1.9939ms)
- Packet 103: Server Hello
- Packet 104: ACK (Seq=1349, Ack=518, Win=30080, Len=1348, TSval=1.9998ms)
- Packet 105: ACK (Seq=2697, Ack=518, Win=30080, Len=1348, TSval=1.9998ms)

The details pane for the first SYN packet (Frame 83) shows the following information:

- Source Port: 62440
- Destination Port: 443
- [Stream index: 5]
- [Stream Packet Number: 1]
- [Conversation completeness: Incomplete, DATA (15)]
- [TCP Segment Len: 0]
- Sequence Number: 0 (relative sequence number)
- Sequence Number (raw): 2206069321
- [Next Sequence Number: 1 (relative sequence number)]
- Acknowledgment Number: 0
- Acknowledgment number (raw): 0
- 1011 .... = Header Length: 44 bytes (11)
- Flags: 0x002 (SYN)
- Window: 65535
- [Calculated window size: 65535]

The bytes pane for the same packet shows the raw hex and ASCII data:

0000	ae 80 ca 77 57 7d
0010	00 40 00 00 40 00
0020	83 a0 f3 e8 01 bb
0030	ff ff 42 80 00 00
0040	08 0a 26 1d 50 7a

# TCP Handshake: SYN-ACK

tcp.stream eq 5

No.	Time	Source	Destination	Protocol	Length	Info
83	1.8439...	192.168.43...	162.105.131...	TCP	78	62440 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=
99	1.9188...	162.105.131...	192.168.43...	TCP	74	443 → 62440 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1360 S
	1.9190...	192.168.43...	162.105.131...	TCP	66	62440 → 443 [ACK] Seq=1 Ack=1 Win=132096 Len=0 TSval=63945543
	1.9190...	192.168.43...	162.105.131...	TLS...	5...	Client Hello (SNI=www.pku.edu.cn)
	1.9939...	162.105.131...	192.168.43...	TCP	66	443 → 62440 [ACK] Seq=1 Ack=518 Win=30080 Len=0 TSval=2630623
	1.9998...	162.105.131...	192.168.43...	TLS...	1...	Server Hello
	1.9998...	162.105.131...	192.168.43...	TCP	1...	443 → 62440 [ACK] Seq=1349 Ack=518 Win=30080 Len=1348 TSval=2
	1.9998...	162.105.131...	192.168.43...	TCP	1...	443 → 62440 [ACK] Seq=2697 Ack=518 Win=30080 Len=1348 TSval=2

> Frame 99: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface en0,  
> Ethernet II, Src: ae:80:ca:77:57:7d (ae:80:ca:77:57:7d), Dst: Apple\_74:12:a4 (9c:3e:53  
> Internet Protocol Version 4, Src: 162.105.131.160, Dst: 192.168.43.199  
> Transmission Control Protocol, Src Port: 443, Dst Port: 62440, Seq: 0, Ack: 1, Len: 0  
Source Port: 443  
Destination Port: 62440  
[Stream index: 5]  
[Stream Packet Number: 2]  
> [Conversation completeness: Incomplete, DATA (15)]  
[TCP Segment Len: 0]  
Sequence Number: 0 (relative sequence number)  
Sequence Number (raw): 3039096018  
[Next Sequence Number: 1 (relative sequence number)]  
Acknowledgment Number: 1 (relative ack number)  
Acknowledgment number (raw): 2206069322  
1010 .... = Header Length: 40 bytes (10)  
> Flags: 0x012 (SYN, ACK)  
Window: 28960  
[Calculated window size: 28960]

0000	9c	3e	53	74	12	a4
0010	00	3c	00	00	40	00
0020	2b	c7	01	bb	f3	e8
0030	71	20	84	ee	00	00
0040	1f	04	26	1d	50	7a

# TCP Handshake: ACK

Screenshot of Wireshark showing a TCP handshake sequence. The packet list shows the following sequence:

- Packet 83: SYN (Seq=0, Win=65535, Len=0, MSS=1460, TSval=)
- Packet 99: SYN, ACK (Seq=0, Ack=1, Win=28960, Len=0, MSS=1360, TSval=)
- Packet 100: ACK (Seq=1, Ack=1, Win=132096, Len=0, TSval=63945543)
- Packet 101: Client Hello (SNI=www.pku.edu.cn)
- Packet 102: ACK (Seq=1, Ack=518, Win=30080, Len=0, TSval=2630623)
- Packet 103: Server Hello
- Packet 104: ACK (Seq=1349, Ack=518, Win=30080, Len=1348, TSval=2630623)
- Packet 105: ACK (Seq=2697, Ack=518, Win=30080, Len=1348, TSval=2630623)

The details pane for the selected ACK packet (packet 100) shows the following fields:

- Frame 100: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface en0,
- Ethernet II, Src: Apple\_74:12:a4 (9c:3e:53:74:12:a4), Dst: ae:80:ca:77:57:7d (ae:80:ca:77:57:7d)
- Internet Protocol Version 4, Src: 192.168.43.199, Dst: 162.105.131.160
- Transmission Control Protocol, Src Port: 62440, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
  - Source Port: 62440
  - Destination Port: 443
  - [Stream index: 5]
  - [Stream Packet Number: 3]
  - [Conversation completeness: Incomplete, DATA (15)]
  - [TCP Segment Len: 0]
    - Sequence Number: 1 (relative sequence number)
    - Sequence Number (raw): 2206069322
    - [Next Sequence Number: 1 (relative sequence number)]
    - Acknowledgment Number: 1 (relative ack number)
    - Acknowledgment number (raw): 3039096019
  - 1000 .... = Header Length: 32 bytes (8)
  - Flags: 0x010 (ACK)
  - Window: 2064
  - [Calculated window size: 132096]

The bytes pane shows the raw hex and ASCII data for the selected ACK packet:

0000	ae 80 ca 77 57 7d
0010	00 34 00 00 40 00
0020	83 a0 f3 e8 01 bb
0030	08 10 1c 1b 00 00
0040	1f 04

# TCP: Client Hello

Screenshot of Wireshark showing a TCP session between 192.168.43.199 and 162.105.131.160. The selected packet is the Client Hello (SNI=www.pku.edu.cn).

No.	Time	Source	Destination	Protocol	Length	Info
83	1.8439...	192.168.43...	162.105.131...	TCP	78	62440 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=132096 TStamp=1.843900000
99	1.9188...	162.105.131...	192.168.43...	TCP	74	443 → 62440 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1360 TSval=132096 TStamp=1.918800000
1...	1.9190...	192.168.43...	162.105.131...	TCP	66	62440 → 443 [ACK] Seq=1 Ack=1 Win=132096 Len=0 TSval=63945543 TStamp=1.919000000
1...	1.9190...	192.168.43...	162.105.131...	TLS...	5...	Client Hello (SNI=www.pku.edu.cn)
1...	1.9939...	162.105.131...	192.168.43...	TCP	66	443 → 62440 [ACK] Seq=1 Ack=518 Win=30080 Len=0 TSval=2630623 TStamp=1.993900000
1...	1.9998...	162.105.131...	192.168.43...	TLS...	1...	Server Hello
1...	1.9998...	162.105.131...	192.168.43...	TCP	1...	443 → 62440 [ACK] Seq=1349 Ack=518 Win=30080 Len=1348 TSval=2630623 TStamp=1.999800000
1...	1.9998...	162.105.131...	192.168.43...	TCP	1...	443 → 62440 [ACK] Seq=2697 Ack=518 Win=30080 Len=1348 TSval=2630623 TStamp=1.999800000

Selected packet details:

- Frame 101: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface
- Ethernet II, Src: Apple\_74:12:a4 (9c:3e:53:74:12:a4), Dst: ae:80:ca:77:57:7d (ae:80:ca:77:57:7d)
- Internet Protocol Version 4, Src: 192.168.43.199, Dst: 162.105.131.160
- Transmission Control Protocol, Src Port: 62440, Dst Port: 443, Seq: 1, Ack: 1, Len: 51
  - Source Port: 62440
  - Destination Port: 443
  - [Stream index: 5]
  - [Stream Packet Number: 4]
  - [Conversation completeness: Incomplete, DATA (15)]
  - [TCP Segment Len: 517]
  - Sequence Number: 1 (relative sequence number)
  - Sequence Number (raw): 2206069322
  - [Next Sequence Number: 518 (relative sequence number)]
  - Acknowledgment Number: 1 (relative ack number)
  - Acknowledgment number (raw): 3039096019
  - 1000 .... = Header Length: 32 bytes (8)
- Flags: 0x018 (PSH, ACK)
- Window: 2064
- [Calculated window size: 132096]

Selected packet bytes:

```

0000 ae 80 ca 77 57 7d
0010 02 39 00 00 40 00
0020 83 a0 f3 e8 01 bb
0030 08 10 99 e6 00 00
0040 1f 04 16 03 01 02
0050 b8 aa 12 39 d7 3b
0060 a0 1a 2d 95 09 bb
0070 31 a9 e2 53 d5 ff
0080 9a 1f 3d 11 6c e8
0090 6a 6a 13 01 13 02
00a0 c0 2f cc a8 c0 0a
00b0 00 35 00 2f c0 08
00c0 00 00 00 00 00 13
00d0 6b 75 2e 65 64 75
00e0 01 00 00 0a 00 0c
00f0 00 19 00 0b 00 02
0100 74 74 70 2f 31 2e
0110 00 0d 00 18 00 16
0120 08 05 08 05 05 01
0130 00 33 00 2b 00 29
0140 01 77 0a aa b1 63
0150 00 00 00 00 00 00

```

# TLS: Client Hello

tcp.stream eq 5

No.	Time	Source	Destination	Protocol	Length	Info
83	1.8439...	192.168.43...	162.105.131...	TCP	78	62440 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=
99	1.9188...	162.105.131...	192.168.43...	TCP	74	443 → 62440 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1360 S
1...	1.9190...	192.168.43...	162.105.131...	TCP	66	62440 → 443 [ACK] Seq=1 Ack=1 Win=132096 Len=0 TSval=63945543
1...	1.9190...	192.168.43...	162.105.131...	TLS...	5...	Client Hello (SNI=www.pku.edu.cn)
1...	1.9939...	162.105.131...	192.168.43...	TCP	66	443 → 62440 [ACK] Seq=1 Ack=518 Win=30080 Len=0 TSval=2630623
1...	1.9998...	162.105.131...	192.168.43...	TLS...	1...	Server Hello
1...	1.9998...	162.105.131...	192.168.43...	TCP	1...	443 → 62440 [ACK] Seq=1349 Ack=518 Win=30080 Len=1348 TSval=2
1...	1.9998...	162.105.131...	192.168.43...	TCP	1...	443 → 62440 [ACK] Seq=2697 Ack=518 Win=30080 Len=1348 TSval=2

> Frame 101: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface  
 > Ethernet II, Src: Apple\_74:12:a4 (9c:3e:53:74:12:a4), Dst: ae:80:ca:77:57:7d (ae:80:ca  
 > Internet Protocol Version 4, Src: 192.168.43.199, Dst: 162.105.131.160  
 > Transmission Control Protocol, Src Port: 62440, Dst Port: 443, Seq: 1, Ack: 1, Len: 51  
 > Transport Layer Security  
 >   TLSv1.2 Record Layer: Handshake Protocol: Client Hello  
     Content Type: Handshake (22)  
     Version: TLS 1.0 (0x0301)  
     Length: 512  
     Handshake Protocol: Client Hello  
       Handshake Type: Client Hello (1)  
       Length: 508  
       Version: TLS 1.2 (0x0303)  
       Random: 65a71eb8aa1239d73b12ae99f7817874e30ee2a01a2d9509bb51411a684da62a  
       Session ID Length: 32  
       Session ID: 339031a9e253d5ff5768831ad527a05e56149a1f3d116ce8c2b25cc01961d2aa  
       Cipher Suites Length: 42  
       Cipher Suites (21 suites)  
         Cipher Suite: Reserved (GREASE) (0x6a6a)  
         Cipher Suite: TLS\_AES\_128\_GCM\_SHA256 (0x1301)

0000	ae	80	ca	77	57	7d
0010	02	39	00	00	40	00
0020	83	a0	f3	e8	01	bb
0030	08	10	99	e6	00	00
0040	1f	04	16	03	01	02
0050	b8	aa	12	39	d7	3b
0060	a0	1a	2d	95	09	bb
0070	31	a9	e2	53	d5	ff
0080	9a	1f	3d	11	6c	e8
0090	6a	6a	13	01	13	02
00a0	c0	2f	cc	a8	c0	0a
00b0	00	35	00	2f	c0	08
00c0	00	00	00	00	00	13
00d0	6b	75	2e	65	64	75
00e0	01	00	00	0a	00	0c
00f0	00	19	00	0b	00	02
0100	74	74	70	2f	31	2e
0110	00	0d	00	18	00	16
0120	08	05	08	05	05	01
0130	00	33	00	2b	00	29
0140	01	77	0a	aa	b1	63
0150	cd	13	d8	1c	34	c7
0160	2d	00	02	01	01	00

# TCP: ACK Client Hello

No.	Time	Source	Destination	Protocol	Length	Info					
83	1.8439...	192.168.43...	162.105.131...	TCP	78	62440 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=					
99	1.9188...	162.105.131...	192.168.43...	TCP	74	443 → 62440 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1360 S					
1...	1.9190...	192.168.43...	162.105.131...	TCP	66	62440 → 443 [ACK] Seq=1 Ack=1 Win=132096 Len=0 TSval=63945543					
1...	1.9190...	192.168.43...	162.105.131...	TLS...	5...	Client Hello (SNI=www.pku.edu.cn)					
1...	1.9939...	162.105.131...	192.168.43...	TCP	66	443 → 62440 [ACK] Seq=1 Ack=518 Win=30080 Len=0 TSval=2630623					
1...	1.9998...	162.105.131...	192.168.43...	TLS...	1...	Server Hello					
1...	1.9998...	162.105.131...	192.168.43...	TCP	1...	443 → 62440 [ACK] Seq=1349 Ack=518 Win=30080 Len=1348 TSval=2					
1...	1.9998...	162.105.131...	192.168.43...	TCP	1...	443 → 62440 [ACK] Seq=2697 Ack=518 Win=30080 Len=1348 TSval=2					
> Frame 109: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface en0, Ethernet II, Src: ae:80:ca:77:57:7d (ae:80:ca:77:57:7d), Dst: Apple_74:12:a4 (9c:3e:53											
> Internet Protocol Version 4, Src: 162.105.131.160, Dst: 192.168.43.199											
↳ Transmission Control Protocol, Src Port: 443, Dst Port: 62440, Seq: 1, Ack: 518, Len: 0											
Source Port: 443											
Destination Port: 62440											
[Stream index: 5]											
[Stream Packet Number: 5]											
[Conversation completeness: Incomplete, DATA (15)]											
[TCP Segment Len: 0]											
Sequence Number: 1 (relative sequence number)											
Sequence Number (raw): 3039096019											
[Next Sequence Number: 1 (relative sequence number)]											
Acknowledgment Number: 518 (relative ack number)											
Acknowledgment number (raw): 2206069839											
1000 .... = Header Length: 32 bytes (8)											
Flags: 0x010 (ACK)											
Window: 235											
[Calculated window size: 30080]											
0000 9c 3e 53 74 12 a4											
0010 00 34 f3 9a 40 00											
0020 2b c7 01 bb f3 e8											
0030 00 eb 20 eb 00 00											
0040 50 c6											

# TCP: Server Hello

Screenshot of Wireshark showing a TLS handshake between two hosts. The timeline shows the sequence of packets, and the details pane provides a breakdown of the selected packet's structure.

No.	Time	Source	Destination	Protocol	Length	Info
1...	1.9998...	162.105.131...	192.168.43...	TLS...	1...	Server Hello
1...	1.9998...	162.105.131...	192.168.43...	TCP	1...	443 → 62440 [ACK] Seq=1349 Ack=518 Win=30080 Len=1348 TSval=2
1...	1.9998...	162.105.131...	192.168.43...	TCP	1...	443 → 62440 [ACK] Seq=2697 Ack=518 Win=30080 Len=1348 TSval=2
1...	1.9998...	162.105.131...	192.168.43...	TLS...	1...	Certificate, Server Key Exchange, Server Hello Done
1...	2.0001...	192.168.43...	162.105.131...	TCP	66	62440 → 443 [ACK] Seq=518 Ack=5301 Win=131072 Len=0 TSval=639
1...	2.0026...	192.168.43...	162.105.131...	TLS...	1...	Client Key Exchange, Change Cipher Spec, Encrypted Handshake
1...	2.0648...	162.105.131...	192.168.43...	TLS...	1...	Change Cipher Spec, Encrypted Handshake Message
1...	2.0655...	192.168.43...	162.105.131...	TCP	66	62440 → 443 [ACK] Seq=644 Ack=5352 Win=131008 Len=0 TSval=639

Selected packet details:

- > Frame 110: 1414 bytes on wire (11312 bits), 1414 bytes captured (11312 bits) on interface
- > Ethernet II, Src: ae:80:ca:77:57:7d (ae:80:ca:77:57:7d), Dst: Apple\_74:12:a4 (9c:3e:53)
- > Internet Protocol Version 4, Src: 162.105.131.160, Dst: 192.168.43.199
- > Transmission Control Protocol, Src Port: 443, Dst Port: 62440, Seq: 1, Ack: 518, Len: 1348

Source Port: 443  
 Destination Port: 62440  
 [Stream index: 5]  
 [Stream Packet Number: 6]  
 [Conversation completeness: Incomplete, DATA (15)]

[TCP Segment Len: 1348]  
 Sequence Number: 1 (relative sequence number)  
 Sequence Number (raw): 3039096019  
 [Next Sequence Number: 1349 (relative sequence number)]  
 Acknowledgment Number: 518 (relative ack number)  
 Acknowledgment number (raw): 2206069839

1000 .... = Header Length: 32 bytes (8)  
 Flags: 0x010 (ACK)  
 Window: 235  
 [Calculated window size: 30080]

Hex dump of the selected packet:

0000	9c	3e	53	74	12	a4
0010	05	78	f3	9b	40	00
0020	2b	c7	01	bb	f3	e8
0030	00	eb	52	bc	00	00
0040	50	c6	16	03	03	00
0050	2c	b8	35	bc	f4	96
0060	70	79	1d	fa	b8	05
0070	0a	6d	2d	96	86	7c
0080	29	f1	24	d4	f7	65
0090	00	00	20	00	00	00
00a0	03	00	01	02	00	10
00b0	31	2e	31	16	03	03
00c0	06	eb	30	82	06	e7
00d0	10	20	8b	04	7b	1f
00e0	dc	30	0d	06	09	2a
00f0	30	59	31	0b	30	09
0100	25	30	23	06	03	55
0110	73	69	61	20	54	65
0120	2c	20	49	6e	63	2e
0130	1a	54	72	75	73	74
0140	56	20	54	4c	53	20

# TLS: Server Hello

Screenshot of Wireshark showing a TLS handshake between 192.168.43.1 and 162.105.131.1. The selected packet is the Server Hello message.

No.	Time	Source	Destination	Protocol	Length	Info
83	1.8439...	192.168.43...	162.105.131...	TCP	78	62440 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=
99	1.9188...	162.105.131...	192.168.43...	TCP	74	443 → 62440 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1360 S
1...	1.9190...	192.168.43...	162.105.131...	TCP	66	62440 → 443 [ACK] Seq=1 Ack=1 Win=132096 Len=0 TSval=63945543
1...	1.9190...	192.168.43...	162.105.131...	TLS...	5...	Client Hello (SNI=www.pku.edu.cn)
1...	1.9939...	162.105.131...	192.168.43...	TCP	66	443 → 62440 [ACK] Seq=1 Ack=518 Win=30080 Len=0 TSval=2630623
1...	1.9998...	162.105.131...	192.168.43...	TLS...	1...	Server Hello
1...	1.9998...	162.105.131...	192.168.43...	TCP	1...	443 → 62440 [ACK] Seq=1349 Ack=518 Win=30080 Len=1348 TSval=2
1...	1.9998...	162.105.131...	192.168.43...	TCP	1...	443 → 62440 [ACK] Seq=2697 Ack=518 Win=30080 Len=1348 TSval=2

Selected packet details:

- Transport Layer Security
  - TLSv1.2 Record Layer: Handshake Protocol: Server Hello
    - Content Type: Handshake (22)
    - Version: TLS 1.2 (0x0303)
    - Length: 108
  - Handshake Protocol: Server Hello
    - Handshake Type: Server Hello (2)
    - Length: 104
    - Version: TLS 1.2 (0x0303)
    - > Random: 54d4f32cb835bcf496e632a3e0161630900ba170791dfab805d99b4684736a26
    - Session ID Length: 32
    - Session ID: c90f0a6d2d96867c74771ec1abb7d1942b9f29f124d4f76548240b77a3568a77
    - Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02f)
    - Compression Method: null (0)
    - Extensions Length: 32
    - > Extension: server\_name (len=0)
    - > Extension: renegotiation\_info (len=1)
    - > Extension: ec\_point\_formats (len=4)
    - > Extension: application\_layer\_protocol\_negotiation (len=11)
      - [JA3S Fullstring: 771,49199,0-65281-11-16]

# TCP: Certificate, Server Key Exchange, Done

Screenshot of Wireshark showing a TLS handshake between two hosts.

The timeline shows the following sequence of packets:

- 1... 1.9998... 162.105.131.160 → 192.168.43.199 TLS... 1... Server Hello
- 1... 1.9998... 162.105.131.160 → 192.168.43.199 TCP 1... 443 → 62440 [ACK] Seq=1349 Ack=518 Win=30080 Len=1348 TSval=2
- 1... 1.9998... 162.105.131.160 → 192.168.43.199 TCP 1... 443 → 62440 [ACK] Seq=2697 Ack=518 Win=30080 Len=1348 TSval=2
- 1... 1.9998... 162.105.131.160 → 192.168.43.199 TLS... 1... Certificate, Server Key Exchange, Server Hello Done
- 1... 2.0001... 192.168.43.199 → 162.105.131.160 TCP 66 62440 → 443 [ACK] Seq=518 Ack=5301 Win=131072 Len=0 TSval=639
- 1... 2.0026... 192.168.43.199 → 162.105.131.160 TLS... 1... Client Key Exchange, Change Cipher Spec, Encrypted Handshake
- 1... 2.0648... 162.105.131.160 → 192.168.43.199 TLS... 1... Change Cipher Spec, Encrypted Handshake Message
- 1... 2.0655... 192.168.43.199 → 162.105.131.160 TCP 66 62440 → 443 [ACK] Seq=644 Ack=5352 Win=131008 Len=0 TSval=639

Details for the selected packet (Frame 111):

- Frame 111: 1414 bytes on wire (11312 bits), 1414 bytes captured (11312 bits) on interface
- Ethernet II, Src: ae:80:ca:77:57:7d (ae:80:ca:77:57:7d), Dst: Apple\_74:12:a4 (9c:3e:53)
- Internet Protocol Version 4, Src: 162.105.131.160, Dst: 192.168.43.199
- Transmission Control Protocol, Src Port: 443, Dst Port: 62440, Seq: 1349, Ack: 518, Len: 1348

Source Port: 443  
Destination Port: 62440  
[Stream index: 5]  
[Stream Packet Number: 7]  
[Conversation completeness: Incomplete, DATA (15)]

[TCP Segment Len: 1348]

Sequence Number: 1349 (relative sequence number)  
Sequence Number (raw): 3039097367  
[Next Sequence Number: 2697 (relative sequence number)]

Acknowledgment Number: 518 (relative ack number)  
Acknowledgment number (raw): 2206069839

1000 .... = Header Length: 32 bytes (8)  
Flags: 0x010 (ACK)  
Window: 235  
[Calculated window size: 30080]

0000	9c	3e	53	74	12	a4
0010	05	78	f3	9c	40	00
0020	2b	c7	01	bb	f3	e8
0030	00	eb	d1	ab	00	00
0040	50	c6	74	b3	f2	ee
0050	7c	6c	53	4a	0f	27
0060	4e	75	a3	27	5c	9a
0070	1d	f0	e0	8e	1b	8d
0080	00	00	01	8e	5a	71
0090	02	20	70	eb	8b	3b
00a0	bf	52	42	f0	e4	d5
00b0	d0	d7	02	21	00	de
00c0	51	9b	df	bf	72	db
00d0	76	20	d1	a4	9d	30
00e0	01	0c	05	00	03	82
00f0	25	32	07	f9	2a	28
0100	87	ff	0f	4f	af	71
0110	2f	45	a6	3b	c4	3c
0120	07	25	1f	cb	d8	ac
0130	60	74	da	67	b8	9e
0140	da	eb	fe	18	66	e1

# TCP: Certificate, Server Key Exchange, Done

tcp.stream eq 5

No.	Time	Source	Destination	Protocol	Length	Info
1...	1.9998...	162.105.131...	192.168.43...	TLS...	1...	Server Hello
1...	1.9998...	162.105.131...	192.168.43...	TCP	1...	443 → 62440 [ACK] Seq=1349 Ack=518 Win=30080 Len=1348 TSval=2
1...	1.9998...	162.105.131...	192.168.43...	TCP	1...	443 → 62440 [ACK] Seq=2697 Ack=518 Win=30080 Len=1348 TSval=2
1...	1.9998...	162.105.131...	192.168.43...	TLS...	1...	Certificate, Server Key Exchange, Server Hello Done
1...	2.0001...	192.168.43...	162.105.131...	TCP	66	62440 → 443 [ACK] Seq=518 Ack=5301 Win=131072 Len=0 TSval=639
1...	2.0026...	192.168.43...	162.105.131...	TLS...	1...	Client Key Exchange, Change Cipher Spec, Encrypted Handshake
1...	2.0648...	162.105.131...	192.168.43...	TLS...	1...	Change Cipher Spec, Encrypted Handshake Message
1...	2.0655...	192.168.43...	162.105.131...	TCP	66	62440 → 443 [ACK] Seq=644 Ack=5352 Win=131008 Len=0 TSval=639

> Frame 112: 1414 bytes on wire (11312 bits), 1414 bytes captured (11312 bits) on interface  
 > Ethernet II, Src: ae:80:ca:77:57:7d (ae:80:ca:77:57:7d), Dst: Apple\_74:12:a4 (9c:3e:53)  
 > Internet Protocol Version 4, Src: 162.105.131.160, Dst: 192.168.43.199  
 > Transmission Control Protocol, Src Port: 443, Dst Port: 62440, Seq: 2697, Ack: 518, Len: 1348  
 Source Port: 443  
 Destination Port: 62440  
 [Stream index: 5]  
 [Stream Packet Number: 8]  
 > [Conversation completeness: Incomplete, DATA (15)]  
 [TCP Segment Len: 1348]  
 Sequence Number: 2697 (relative sequence number)  
 Sequence Number (raw): 3039098715  
 [Next Sequence Number: 4045 (relative sequence number)]  
 Acknowledgment Number: 518 (relative ack number)  
 Acknowledgment number (raw): 2206069839  
 1000 .... = Header Length: 32 bytes (8)  
 > Flags: 0x010 (ACK)  
 Window: 235  
 [Calculated window size: 30080]

0000	9c	3e	53	74	12	a4
0010	05	78	f3	9d	40	00
0020	2b	c7	01	bb	f3	e8
0030	00	eb	6b	65	00	00
0040	50	c6	0d	00	63	5e
0050	1d	0f	01	01	ff	04
0060	1d	13	01	01	ff	04
0070	1d	06	03	55	1d	25
0080	05	07	03	01	06	08
0090	06	03	55	1d	20	04
00a0	04	01	b2	31	01	02
00b0	02	02	30	50	06	03
00c0	43	a0	41	86	3f	68
00d0	75	73	65	72	74	72
00e0	45	52	54	72	75	73
00f0	69	63	61	74	69	6f
0100	2e	63	72	6c	30	71
0110	04	65	30	63	30	3a
0120	86	2e	68	74	74	70
0130	72	74	72	75	73	74
0140	72	75	73	74	52	53

# TCP: Certificate, Server Key Exchange, Done

Screenshot of Wireshark showing a TLS handshake between two hosts. The timeline shows the following sequence of packets:

- 1... 1.9998... 162.105.131.160 → 192.168.43.199 TLS... 1... Server Hello
- 1... 1.9998... 162.105.131.160 → 192.168.43.199 TCP 1... 443 → 62440 [ACK] Seq=1349 Ack=518 Win=30080 Len=1348 TSval=2
- 1... 1.9998... 162.105.131.160 → 192.168.43.199 TCP 1... 443 → 62440 [ACK] Seq=2697 Ack=518 Win=30080 Len=1348 TSval=2
- 1... 1.9998... 162.105.131.160 → 192.168.43.199 TLS... 1... Certificate, Server Key Exchange, Server Hello Done
- 1... 2.0001... 192.168.43.199 → 162.105.131.160 TCP 66 62440 → 443 [ACK] Seq=518 Ack=5301 Win=131072 Len=0 TSval=639
- 1... 2.0026... 192.168.43.199 → 162.105.131.160 TLS... 1... Client Key Exchange, Change Cipher Spec, Encrypted Handshake
- 1... 2.0648... 162.105.131.160 → 192.168.43.199 TLS... 1... Change Cipher Spec, Encrypted Handshake Message
- 1... 2.0655... 192.168.43.199 → 162.105.131.160 TCP 66 62440 → 443 [ACK] Seq=644 Ack=5352 Win=131008 Len=0 TSval=639

Details for the fourth packet (Server Hello Done):

- Frame 113: 1322 bytes on wire (10576 bits), 1322 bytes captured (10576 bits) on interface
- Ethernet II, Src: ae:80:ca:77:57:7d (ae:80:ca:77:57:7d), Dst: Apple\_74:12:a4 (9c:3e:53)
- Internet Protocol Version 4, Src: 162.105.131.160, Dst: 192.168.43.199
- Transmission Control Protocol, Src Port: 443, Dst Port: 62440, Seq: 4045, Ack: 518, Len: 1256
- Source Port: 443
- Destination Port: 62440
- [Stream index: 5]
- [Stream Packet Number: 9]
- [Conversation completeness: Incomplete, DATA (15)]
- [TCP Segment Len: 1256]
- Sequence Number: 4045 (relative sequence number)
- Sequence Number (raw): 3039100063
- [Next Sequence Number: 5301 (relative sequence number)]
- Acknowledgment Number: 518 (relative ack number)
- Acknowledgment number (raw): 2206069839
- 1000 .... = Header Length: 32 bytes (8)
- Flags: 0x018 (PSH, ACK)
- Window: 235
- [Calculated window size: 30080]

The bytes column shows the raw hex and ASCII data for the packet.

# TLS: Certificate

Screenshot of Wireshark showing a TLS handshake. The packet list shows several TLS frames, with the fourth frame (Sequence 1) highlighted. The details pane shows the TLS Record Layer Handshake Protocol: Certificate message, and the bytes pane shows the hex and ASCII representation of the certificate data.

No.	Time	Source	Destination	Protocol	Length	Info
1..	1.9998...	162.105.131...	192.168.43...	TLS...	1...	Server Hello
1..	1.9998...	162.105.131...	192.168.43...	TCP	1...	443 → 62440 [ACK] Seq=1349 Ack=518 Win=30080 Len=1348 TSval=2
1..	1.9998...	162.105.131...	192.168.43...	TCP	1...	443 → 62440 [ACK] Seq=2697 Ack=518 Win=30080 Len=1348 TSval=2
1..	1.9998...	162.105.131...	192.168.43...	TLS...	1...	Certificate, Server Key Exchange, Server Hello Done
1..	2.0001...	192.168.43...	162.105.131...	TCP	66	62440 → 443 [ACK] Seq=518 Ack=5301 Win=131072 Len=0 TSval=639
1..	2.0026...	192.168.43...	162.105.131...	TLS...	1...	Client Key Exchange, Change Cipher Spec, Encrypted Handshake
1..	2.0648...	162.105.131...	192.168.43...	TLS...	1...	Change Cipher Spec, Encrypted Handshake Message
1	2.0655	192.168.43	162.105.131	TCP	66	62440 → 443 [ACK] Seq=644 Ack=5352 Win=131008 Len=0 TSval=639

Transport Layer Security

- TLSv1.2 Record Layer: Handshake Protocol: Certificate
  - Content Type: Handshake (22)
  - Version: TLS 1.2 (0x0303)
  - Length: 4835
  - Handshake Protocol: Certificate
    - Handshake Type: Certificate (11)
    - Length: 4831
    - Certificates Length: 4828
  - Certificates (4828 bytes)
    - Certificate Length: 1771
      - Certificate [...] : 308206e73082054fa0030201020210208b047b1fdae0e4cd79175912e5b7dc3
      - Certificate Length: 1635
    - Certificate [...] : 3082065f30820447a00302010202110099f0ab6dc9b12e7f05ffd72284d1d1f
      - Certificate Length: 1413
    - Certificate [...] : 3082058130820469a00302010202103972443af922b751d7d36c10dd3135953

0000	9c 3e 53 74 12 a4
0010	05 1c f3 9e 40 00
0020	2b c7 01 bb f3 e8
0030	00 eb 37 c7 00 00
0040	50 c6 14 54 3f bc
0050	51 8e 35 a6 a7 66
0060	03 c0 50 3a e8 cc
0070	1f 57 5a b7 ff ce
0080	12 3a 4d ae 4c 8a
0090	34 ae 7e 3b 68 66
00a0	f7 94 be 53 37 90
00b0	74 4e 69 c7 6b 8c
00c0	cc 93 3b 51 78 95
00d0	1b 0f f3 25 26 6b
00e0	0e a5 66 b1 29 7c
00f0	30 19 13 ac d3 7d
0100	d7 12 da a9 49 0b
0110	cf 25 88 cd 84 b8

# TLS: Certificate

```
✓ Certificates (4828 bytes)
  Certificate Length: 1771
  ✓ Certificate [...]: 308206e73082054fa0030201020210208b047b1fdae0e4cd79175912e5b7dc300d06092a864886f70d01...
    ✓ signedCertificate
      version: v3 (2)
      serialNumber: 0x208b047b1fdae0e4cd79175912e5b7dc
      > signature (sha384WithRSAEncryption)
      ✓ issuer: rdnSequence (0)
        > rdnSequence: 3 items (id-at-commonName=TrustAsia RSA OV TLS CA G3, id-at-organizationName=TrustAsi...
      > validity
      ✓ subject: rdnSequence (0)
        > rdnSequence: 4 items (id-at-commonName=www.pku.edu.cn, id-at-organizationName=北京大学, id-at-state0...
        > subjectPublicKeyInfo
        > extensions: 10 items
      > algorithmIdentifier (sha384WithRSAEncryption)
      Padding: 0
      encrypted [...]: 46cd8ac5a0e18a253207f92a280120e0d97df9dd5f6aa587ff0f4faf710b74131e678536d6e1b52f45a63...
      Certificate Length: 1635
    > Certificate [...]: 3082065f30820447a00302010202110099f0ab6dc9b12e7f05ffd72284d1d1ff300d06092a864886f70d...
```

# TLS: Server Key Exchange, Server Hello Done

Screenshot of Wireshark showing a TLS handshake between two hosts. The timeline shows the following sequence:

No.	Time	Source	Destination	Protocol	Length	Info
1...	1.9998...	162.105.131...	192.168.43...	TLS...	1...	Server Hello
1...	1.9998...	162.105.131...	192.168.43...	TCP	1...	443 → 62440 [ACK] Seq=1349 Ack=518 Win=30080 Len=1348 TSval=2
1...	1.9998...	162.105.131...	192.168.43...	TCP	1...	443 → 62440 [ACK] Seq=2697 Ack=518 Win=30080 Len=1348 TSval=2
1...	1.9998...	162.105.131...	192.168.43...	TLS...	1...	Certificate, Server Key Exchange, Server Hello Done
1...	2.0001...	192.168.43...	162.105.131...	TCP	66	62440 → 443 [ACK] Seq=518 Ack=5301 Win=131072 Len=0 TSval=639
1...	2.0026...	192.168.43...	162.105.131...	TLS...	1...	Client Key Exchange, Change Cipher Spec, Encrypted Handshake
1...	2.0648...	162.105.131...	192.168.43...	TLS...	1...	Change Cipher Spec, Encrypted Handshake Message
1	2.0655	192.168.43	162.105.131	TCP	66	62440 → 443 [ACK] Seq=644 Ack=5352 Win=131008 Len=0 TSval=639

The details pane shows the expanded structure of the Server Key Exchange message:

- > Transport Layer Security
  - > Transport Layer Security
    - > TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
      - Content Type: Handshake (22)
      - Version: TLS 1.2 (0x0303)
      - Length: 333
    - > Handshake Protocol: Server Key Exchange
      - Handshake Type: Server Key Exchange (12)
      - Length: 329
    - > EC Diffie-Hellman Server Params
      - Curve Type: named\_curve (0x03)
      - Named Curve: secp256r1 (0x0017)
      - Pubkey Length: 65
      - Pubkey: 04d088206076fc9dffe130e322ad56b771a4971c77afb6495d6e16aacfc112d292cdf634ba510518c0faa0f6c5e8...
    - > Signature Algorithm: rsa\_pkcs1\_sha512 (0x0601)
      - Signature Length: 256
      - Signature [...]: a9da86c57a6dfdb90fc0a82e5af46f1f9d8d775fef31210cc30e4d9c4e9ef851f2024629c2b59fef4c1d03...
  - > TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
    - Content Type: Handshake (22)
    - Version: TLS 1.2 (0x0303)

# TCP: ACK Server Hello

Screenshot of Wireshark showing a TCP session. The packet list shows several TLS handshake messages. The selected packet is a TCP ACK from port 443 to 62440.

No.	Time	Source	Destination	Protoc	Len	Info
1...	1.9998...	162.105.131...	192.168.43...	TLS...	1...	Server Hello
1...	1.9998...	162.105.131...	192.168.43...	TCP	1...	443 → 62440 [ACK] Seq=1349 Ack=518 Win=30080 Len=1348 TSval=2
1...	1.9998...	162.105.131...	192.168.43...	TCP	1...	443 → 62440 [ACK] Seq=2697 Ack=518 Win=30080 Len=1348 TSval=2
1...	1.9998...	162.105.131...	192.168.43...	TLS...	1...	Certificate, Server Key Exchange, Server Hello Done
1...	2.0001...	192.168.43...	162.105.131...	TCP	66	62440 → 443 [ACK] Seq=518 Ack=5301 Win=131072 Len=0 TSval=639
1...	2.0026...	192.168.43...	162.105.131...	TLS...	1...	Client Key Exchange, Change Cipher Spec, Encrypted Handshake
1...	2.0648...	162.105.131...	192.168.43...	TLS...	1...	Change Cipher Spec, Encrypted Handshake Message
1...	2.0655...	192.168.43...	162.105.131...	TCP	66	62440 → 443 [ACK] Seq=644 Ack=5352 Win=131008 Len=0 TSval=639

Selected packet details:

- Frame 114: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface en0,
- Ethernet II, Src: Apple\_74:12:a4 (9c:3e:53:74:12:a4), Dst: ae:80:ca:77:57:7d (ae:80:ca:77:57:7d)
- Internet Protocol Version 4, Src: 192.168.43.199, Dst: 162.105.131.160
- Transmission Control Protocol, Src Port: 62440, Dst Port: 443, Seq: 518, Ack: 5301, Len: 66

Source Port: 62440  
Destination Port: 443  
[Stream index: 5]  
[Stream Packet Number: 10]  
[Conversation completeness: Incomplete, DATA (15)]  
[TCP Segment Len: 0]  
Sequence Number: 518 (relative sequence number)  
Sequence Number (raw): 2206069839  
[Next Sequence Number: 518 (relative sequence number)]  
Acknowledgment Number: 5301 (relative ack number)  
Acknowledgment number (raw): 3039101319  
1000 .... = Header Length: 32 bytes (8)  
Flags: 0x010 (ACK)  
Window: 2048  
[Calculated window size: 131072]

Hex dump of the selected packet:

0000	ae	80	ca	77	57	7d
0010	00	34	00	00	40	00
0020	83	a0	f3	e8	01	bb
0030	08	00	04	ce	00	00
0040	1f	57				

# TCP: Client Key Exchange, Change Cipher Spec

Screenshot of Wireshark showing a TLS handshake between two hosts. The timeline shows the sequence of messages:

No.	Time	Source	Destination	Protocol	Length	Info
1...	1.9998...	162.105.131...	192.168.43...	TLS...	1...	Server Hello
1...	1.9998...	162.105.131...	192.168.43...	TCP	1...	443 → 62440 [ACK] Seq=1349 Ack=518 Win=30080 Len=1348 TSval=2
1...	1.9998...	162.105.131...	192.168.43...	TCP	1...	443 → 62440 [ACK] Seq=2697 Ack=518 Win=30080 Len=1348 TSval=2
1...	1.9998...	162.105.131...	192.168.43...	TLS...	1...	Certificate, Server Key Exchange, Server Hello Done
1...	2.0001...	192.168.43...	162.105.131...	TCP	66	62440 → 443 [ACK] Seq=518 Ack=5301 Win=131072 Len=0 TSval=639
1...	2.0026...	192.168.43...	162.105.131...	TLS...	1...	Client Key Exchange, Change Cipher Spec, Encrypted Handshake
1...	2.0648...	162.105.131...	192.168.43...	TLS...	1...	Change Cipher Spec, Encrypted Handshake Message
1...	2.0655...	192.168.43...	162.105.131...	TCP	66	62440 → 443 [ACK] Seq=644 Ack=5352 Win=131008 Len=0 TSval=639

Details for the selected Client Key Exchange, Change Cipher Spec, Encrypted Handshake message (Frame 115):

- Frame 115: 192 bytes on wire (1536 bits), 192 bytes captured (1536 bits) on interface
- Ethernet II, Src: Apple\_74:12:a4 (9c:3e:53:74:12:a4), Dst: ae:80:ca:77:57:7d (ae:80:ca)
- Internet Protocol Version 4, Src: 192.168.43.199, Dst: 162.105.131.160
- Transmission Control Protocol, Src Port: 62440, Dst Port: 443, Seq: 518, Ack: 5301, Len: 126, Source Port: 62440, Destination Port: 443, [Stream index: 5], [Stream Packet Number: 11], [Conversation completeness: Incomplete, DATA (15)], [TCP Segment Len: 126], Sequence Number: 518 (relative sequence number), Sequence Number (raw): 2206069839, [Next Sequence Number: 644 (relative sequence number)], Acknowledgment Number: 5301 (relative ack number), Acknowledgment number (raw): 3039101319
- 1000 .... = Header Length: 32 bytes (8)
- Flags: 0x018 (PSH, ACK)
- Window: 2048
- [Calculated window size: 131072]

Hex dump of the selected packet:

0000	ae	80	ca	77	57	7d
0010	00	b2	00	00	40	00
0020	83	a0	f3	e8	01	bb
0030	08	00	d6	13	00	00
0040	1f	57	16	03	03	00
0050	af	d5	e8	ab	93	b4
0060	f9	19	59	4a	38	21
0070	fe	93	ee	f7	50	7c
0080	0c	a9	3a	ab	b6	8c
0090	00	01	01	16	03	03
00a0	36	d2	fa	7a	e0	d3
00b0	3e	c0	9e	65	17	9d

# TLS: Client Key Exchange

Screenshot of Wireshark showing a TLS handshake between two hosts. The timeline shows several TCP and TLS frames. The details pane shows the structure of the Client Key Exchange message.

No.	Time	Source	Destination	Protocol	Length	Info
1...	1.9998...	162.105.131...	192.168.43...	TCP	1...	443 → 62440 [ACK] Seq=1349 Ack=518 Win=30080 Len=1348 TSval=2
1...	1.9998...	162.105.131...	192.168.43...	TCP	1...	443 → 62440 [ACK] Seq=2697 Ack=518 Win=30080 Len=1348 TSval=2
1...	1.9998...	162.105.131...	192.168.43...	TLS...	1...	Certificate, Server Key Exchange, Server Hello Done
1...	2.0001...	192.168.43...	162.105.131...	TCP	66	62440 → 443 [ACK] Seq=518 Ack=5301 Win=131072 Len=0 TSval=639
1...	2.0026...	192.168.43...	162.105.131...	TLS...	1...	Client Key Exchange, Change Cipher Spec, Encrypted Handshake
1...	2.0648...	162.105.131...	192.168.43...	TLS...	1...	Change Cipher Spec, Encrypted Handshake Message
1...	2.0655...	192.168.43...	162.105.131...	TCP	66	62440 → 443 [ACK] Seq=644 Ack=5352 Win=131008 Len=0 TSval=639
1...	2.0660...	162.105.131...	192.168.43...	TLS...	7	Application Data

Transport Layer Security

- TLSSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
  - Content Type: Handshake (22)
  - Version: TLS 1.2 (0x0303)
  - Length: 70
- Handshake Protocol: Client Key Exchange
  - Handshake Type: Client Key Exchange (16)
  - Length: 66
    - EC Diffie-Hellman Client Params
      - Pubkey Length: 65
      - Pubkey: 04a9c353af5e8ab93b44d7a2eb3d83e583c05b4f919594a382199d148f048888e2ec6cbfe93eef7507c938fb0a5256...
- TLSSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
  - Content Type: Change Cipher Spec (20)
  - Version: TLS 1.2 (0x0303)
  - Length: 1
  - Change Cipher Spec Message
- TLSSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
  - Content Type: Handshake (22)
  - Version: TLS 1.2 (0x0303)

# TCP: Change Cipher Spec

Screenshot of Wireshark showing a TLS handshake. The packet list shows several TLS frames, with the fourth one (Change Cipher Spec) highlighted. The details pane shows the frame structure and the bytes pane shows the raw hex and ASCII data.

tcp.stream eq 5

No.	Time	Source	Destination	Protocol	Length	Info
1...	1.9998...	162.105.131...	192.168.43...	TLS	1...	Certificate, Server Key Exchange, Server Hello Done
1...	2.0001...	192.168.43...	162.105.131...	TCP	66	62440 → 443 [ACK] Seq=518 Ack=5301 Win=131072 Len=0 TSval=639
1...	2.0026...	192.168.43...	162.105.131...	TLS	1...	Client Key Exchange, Change Cipher Spec, Encrypted Handshake
1...	2.0648...	162.105.131...	192.168.43...	TLS	1...	Change Cipher Spec, Encrypted Handshake Message
1...	2.0655...	192.168.43...	162.105.131...	TCP	66	62440 → 443 [ACK] Seq=644 Ack=5352 Win=131008 Len=0 TSval=639
1...	2.0660...	192.168.43...	162.105.131...	TLS	7...	Application Data
1...	2.1343...	162.105.131...	192.168.43...	TLS	3...	Application Data
1...	2.1347...	192.168.43...	162.105.131...	TCP	66	62440 → 443 [ACK] Seq=1310 Ack=5602 Win=130816 Len=0 TSval=63

> Frame 121: 117 bytes on wire (936 bits), 117 bytes captured (936 bits) on interface en  
> Ethernet II, Src: ae:80:ca:77:57:7d (ae:80:ca:77:57:7d), Dst: Apple\_74:12:a4 (9c:3e:53)  
> Internet Protocol Version 4, Src: 162.105.131.160, Dst: 192.168.43.199  
> Transmission Control Protocol, Src Port: 443, Dst Port: 62440, Seq: 5301, Ack: 644, Len: 117  
    Source Port: 443  
    Destination Port: 62440  
    [Stream index: 5]  
    [Stream Packet Number: 12]  
    [Conversation completeness: Incomplete, DATA (15)]  
    [TCP Segment Len: 51]  
    Sequence Number: 5301 (relative sequence number)  
    Sequence Number (raw): 3039101319  
    [Next Sequence Number: 5352 (relative sequence number)]  
    Acknowledgment Number: 644 (relative ack number)  
    Acknowledgment number (raw): 2206069965  
    1000 .... = Header Length: 32 bytes (8)  
> Flags: 0x018 (PSH, ACK)  
Window: 235  
[Calculated window size: 30080]

0000	9c	3e	53	74	12	a4
0010	00	67	f3	9f	40	00
0020	2b	c7	01	bb	f3	e8
0030	00	eb	7e	6b	00	00
0040	51	19	14	03	03	00
0050	b7	46	ac	96	d7	3f
0060	4a	d1	6f	80	24	33
0070	3e	00	a3	68	d9	

# TCP: ACK Change Cipher Spec

Screenshot of Wireshark showing a TLS handshake. The selected packet is a TCP ACK from the server (192.168.43.199) to the client (162.105.131.160), sequence number 644, acknowledgment number 5352.

No.	Time	Source	Destination	Protocol	Length	Info
1...	1.9998...	162.105.131...	192.168.43...	TLS...	1...	Certificate, Server Key Exchange, Server Hello Done
1...	2.0001...	192.168.43...	162.105.131...	TCP	66	62440 → 443 [ACK] Seq=518 Ack=5301 Win=131072 Len=0 TSval=639
1...	2.0026...	192.168.43...	162.105.131...	TLS...	1...	Client Key Exchange, Change Cipher Spec, Encrypted Handshake
1...	2.0648...	162.105.131...	192.168.43...	TLS...	1...	Change Cipher Spec, Encrypted Handshake Message
1...	2.0655...	192.168.43...	162.105.131...	TCP	66	62440 → 443 [ACK] Seq=644 Ack=5352 Win=131008 Len=0 TSval=639
1...	2.0660...	192.168.43...	162.105.131...	TLS...	7...	Application Data
1...	2.1343...	162.105.131...	192.168.43...	TLS...	3...	Application Data
1...	2.1347...	192.168.43...	162.105.131...	TCP	66	62440 → 443 [ACK] Seq=1310 Ack=5602 Win=130816 Len=0 TSval=63

Selected packet details:

- Frame 122: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface en0,
- Ethernet II, Src: Apple\_74:12:a4 (9c:3e:53:74:12:a4), Dst: ae:80:ca:77:57:7d (ae:80:ca:77:57:7d)
- Internet Protocol Version 4, Src: 192.168.43.199, Dst: 162.105.131.160
- Transmission Control Protocol, Src Port: 62440, Dst Port: 443, Seq: 644, Ack: 5352, Len: 66

Source Port: 62440  
Destination Port: 443  
[Stream index: 5]  
[Stream Packet Number: 13]  
[Conversation completeness: Incomplete, DATA (15)]  
[TCP Segment Len: 0]  
Sequence Number: 644 (relative sequence number)  
Sequence Number (raw): 2206069965  
[Next Sequence Number: 644 (relative sequence number)]  
Acknowledgment Number: 5352 (relative ack number)  
Acknowledgment number (raw): 3039101370  
1000 .... = Header Length: 32 bytes (8)  
Flags: 0x010 (ACK)  
Window: 2047  
[Calculated window size: 131008]

Selected bytes (hex dump):

0000	ae	80	ca	77	57	7d
0010	00	34	00	00	40	00
0020	83	a0	f3	e8	01	bb
0030	07	ff	03	9b	00	00
0040	1f	9a				

## 4. In-class Practice

---

# Step 1

- Assume the RSA key of the root CA:
  - $p=3, q=11, e=7$
  - $\Rightarrow$  public key: (7, 33), private key: 3
- Demonstrate the full process to issue a digital cert to yourself.
  - Generate a key pair
  - Sign the cert
  - Assume the hash function:  $Hash(M) = (\sum_{i=1}^l m_i) \text{mod } 256$

**Version:** x509.v3

**Serial Number:** 100100

**Subject:** CN = YOURNAME, O = Fudan University, C = CN

**Issuer:** CN = RootCA, O = Fudan University, C = CN

**Validity:** 2024 - 0901 to 2027-07-31

## Step 2

- Sign the message with FISF's digital certificate
  - "FISF is a great school of Fudan University"
- Demonstrate the full process of signature verification
  - Verify the message signature
  - Verify the certificate signature

## Step 3: Experiment

- Repeat the process with a real PKI tool: <https://pkitools.net>
  - Generate a certificate
  - Sign a message and verify the signed message