Computer Networks 1
(Mạng Máy Tính 1)

Lectured by: Dr. Phạm Trần Vũ

MEng. Nguyễn Cao Đạt

Lecture 11:
Network Security

Reference:

Chapter 8 - "*Computer Networks*",
Andrew S. Tanenbaum, 4th Edition, Prentice Hall, 2003.

Outline

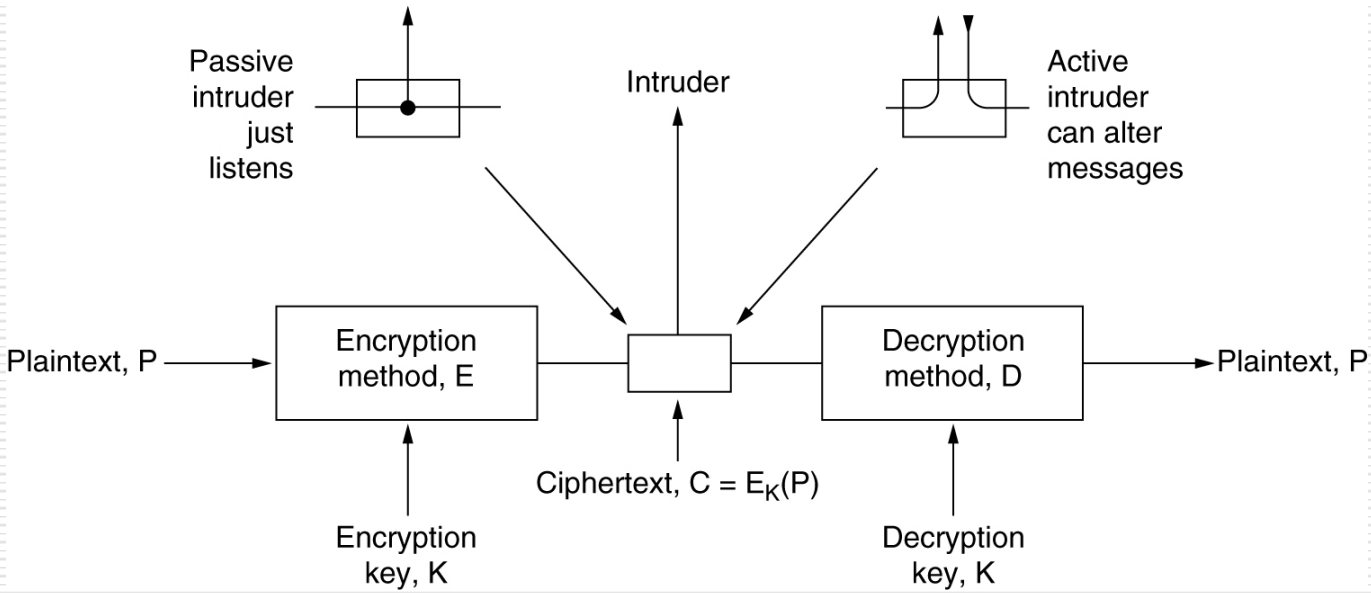
- **Cryptography**
  - Introduction
  - Symmetric-key algorithms
  - Public-key algorithms
  - Digital Signatures
  - Management of Public Keys
- **Apply to Computer Networks**
  - Terms: Authentication, Authorization, Message Protection
  - Secure Sockets Layer (SSL)
  - E-mail security
  - Web Security

Outline

- **Cryptography**
  - Introduction
  - Symmetric-key algorithms
  - Public-key algorithms
  - Digital Signatures
  - Management of Public Keys

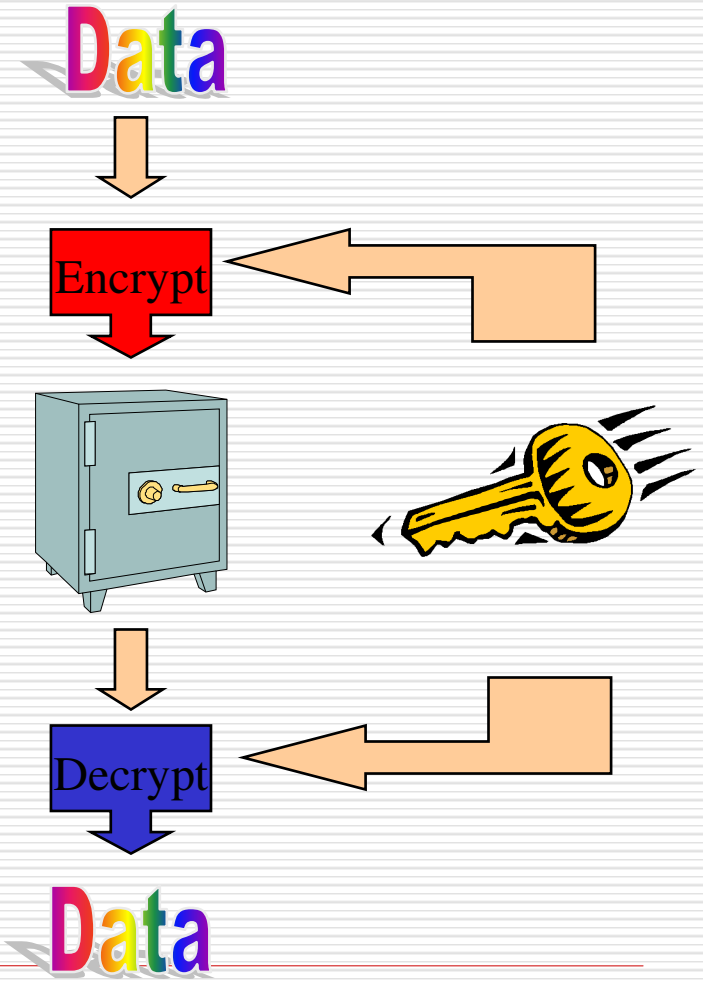
Crytography(1)

- Introduction
  - Cryptography referred almost exclusively to *encryption*, the process of converting ordinary information (plaintext) into unintelligible gibberish (*ciphertext*)



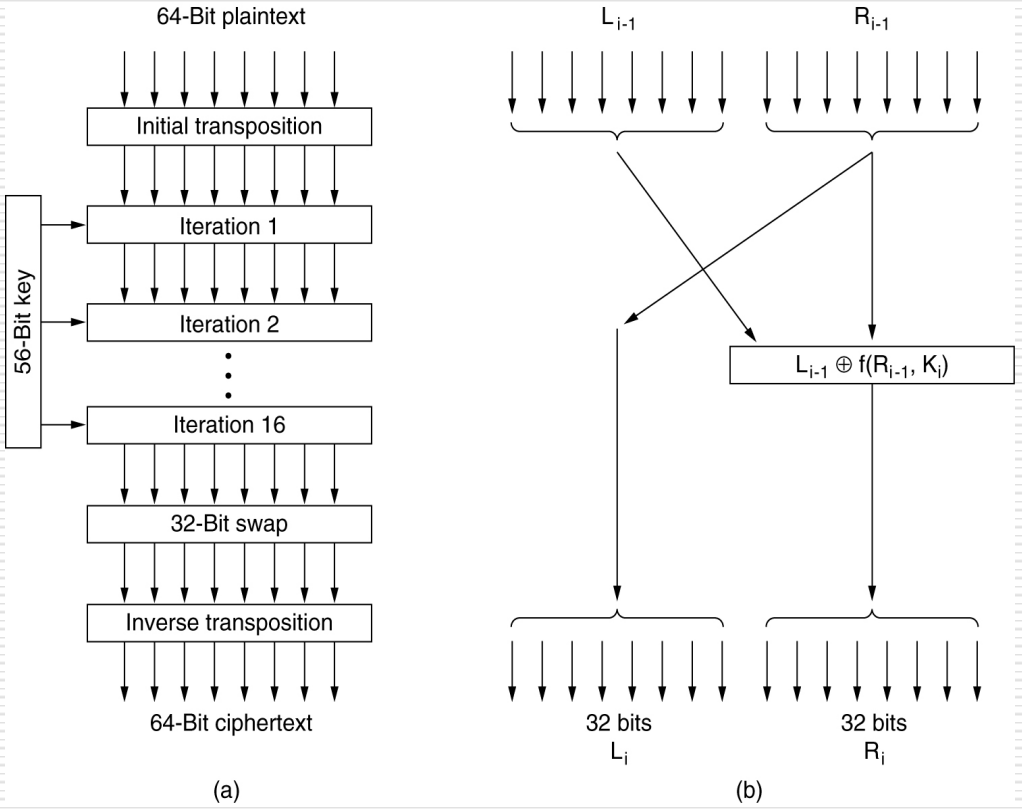
Crytography (2)

- **Symmetric-key algorithms**
  - Encryption and decryption functions that use the same key are called symmetric
  - In this case everyone wanting to read encrypted data must share the same key
  - DES is an example of symmetric-key algorithms



Crytography (3)

- **Data Encryption Standard**



(a) General outline.

(b) Detail of one iteration. The circled + means exclusive OR.

Crytography (4)

- **Advanced Encryption Standard(AES)**
  - Rules for AES proposals
  1. The algorithm must be a symmetric block cipher.
  2. The full design must be public.
  3. Key lengths of 128, 192, and 256 bits supported.
  4. Both software and hardware implementations required
  5. The algorithm must be public or licensed on nondiscriminatory terms.

Crytography (5)

- Some common symmetric-key cryptographic algorithms

Cipher	Author	Key length	Comments
Blowfish	Bruce Schneier	1–448 bits	Old and slow
DES	IBM	56 bits	Too weak to use now
IDEA	Massey and Xuejia	128 bits	Good, but patented
RC4	Ronald Rivest	1–2048 bits	Caution: some keys are weak
RC5	Ronald Rivest	128–256 bits	Good, but patented
Rijndael	Daemen and Rijmen	128–256 bits	Best choice
Serpent	Anderson, Biham, Knudsen	128–256 bits	Very strong
Triple DES	IBM	168 bits	Second best choice
Twofish	Bruce Schneier	128–256 bits	Very strong; widely used

Crytography (6)

Public-Key Algorithms

- So is called Asymmetric-key Algorithms
- Based on some hard problems such as integer factoring, …
- When data is encrypted with one key, the other key must be used to decrypt the data, and vice versa.
- Each entity can be assigned a key pair: a private and public key

Private key is known only to owner

Public key is given away to the world

Crytography (7)

- **RSA(Rivest, Shamir, Adleman)**
  - Choose two large primes, p and q (typically 1024 bits).
  - Compute n = p x q and z = (p - 1) x (q - 1).
  - Choose a number relatively prime to z and call it d.
  - Find e such that e x d = 1 mod z.
  - Pair key: {(e, n), (d,n)}
  - Example
    - p = 3, q = 11 -> n = 33, z = 20
    - Choose d = 7
    - e = 3

Crytography (8)

- **RSA(Rivest, Shamir, Adleman)**

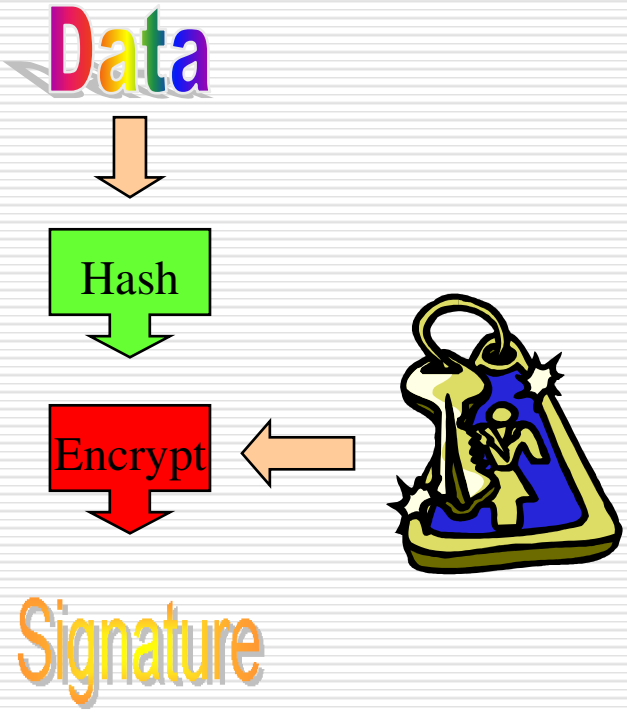
Plaintext (P)			Ciphertext (C)		After decryption	
Symbolic	Numeric	P^3	P^3 (mod 33)	C^7	C^7 (mod 33)	Symbolic
S	19	6859	28	13492928512	19	S
U	21	9261	21	1801088541	21	U
Z	26	17576	20	1280000000	26	Z
A	01	1	1	1	01	A
N	14	2744	5	78125	14	N
N	14	2744	5	78125	14	N
E	05	125	26	8031810176	05	E

Sender's computation

Receiver's computation

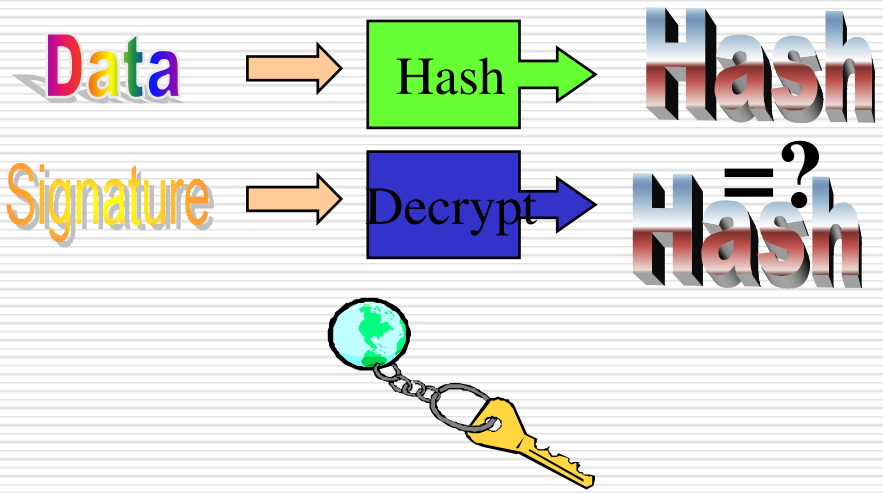
Crytography (9)

- **Digital Signatures**
  - Digital signatures allow the world to verify I created a hunk of data
  - e.g. email, code
  - Sign
    - Digital signatures are created by encrypting a hash of the data with my private key
    - The resulting encrypted data is the signature
    - This hash can then only be decrypted by my public key



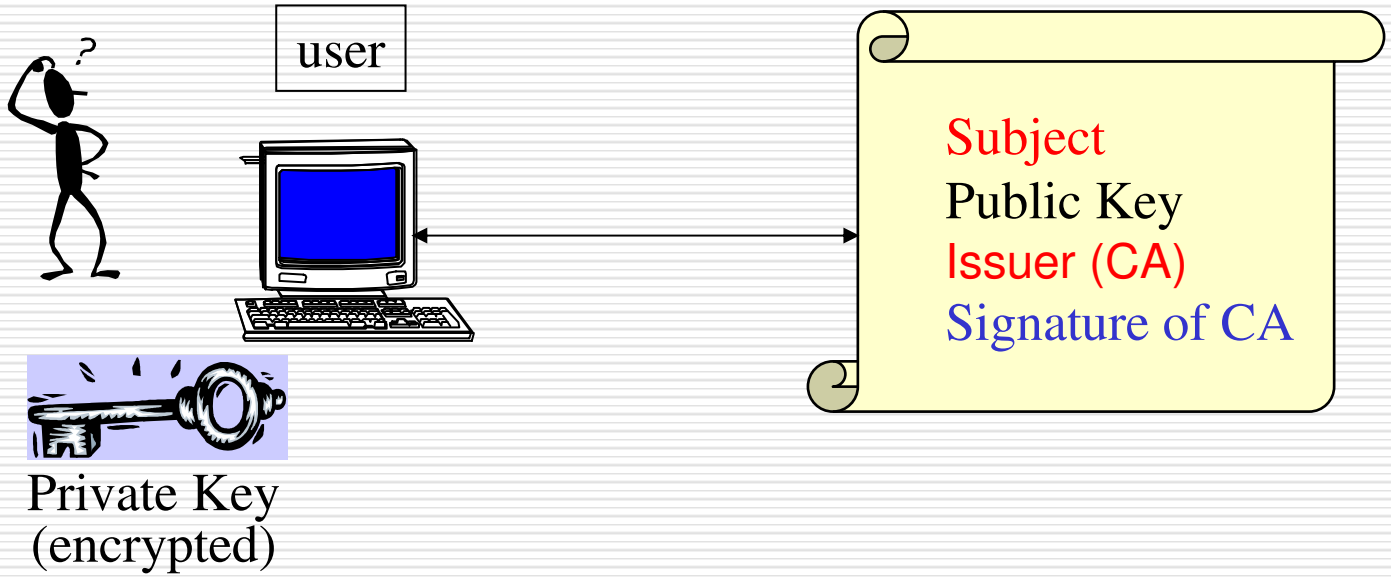
Crytography (10)

- **Digital Signatures**
  - **Verify**
    - Given some data with my signature, if you decrypt a signature with my public key and get the hash of the data, you know it was encrypted with my private key



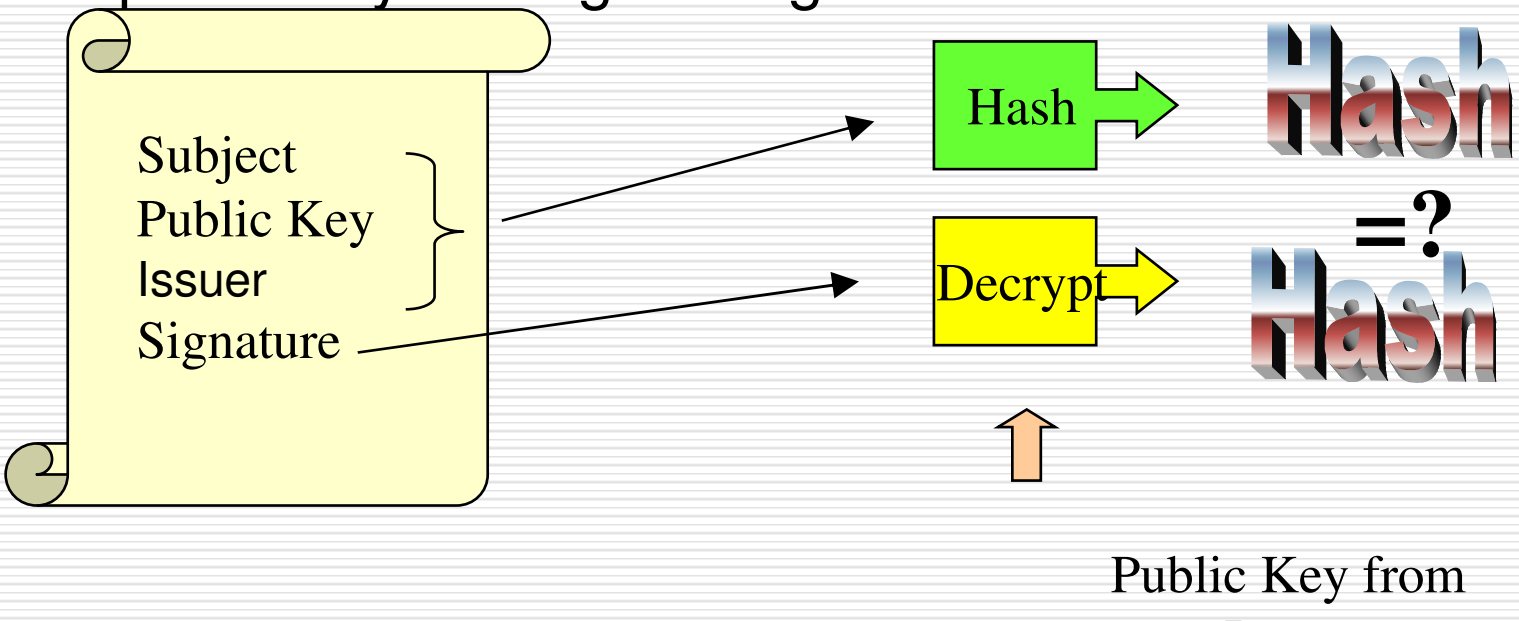
Crytography (11)

- **Management of Public keys**
  - How do you know that you have my correct public key ?
  - Certificates



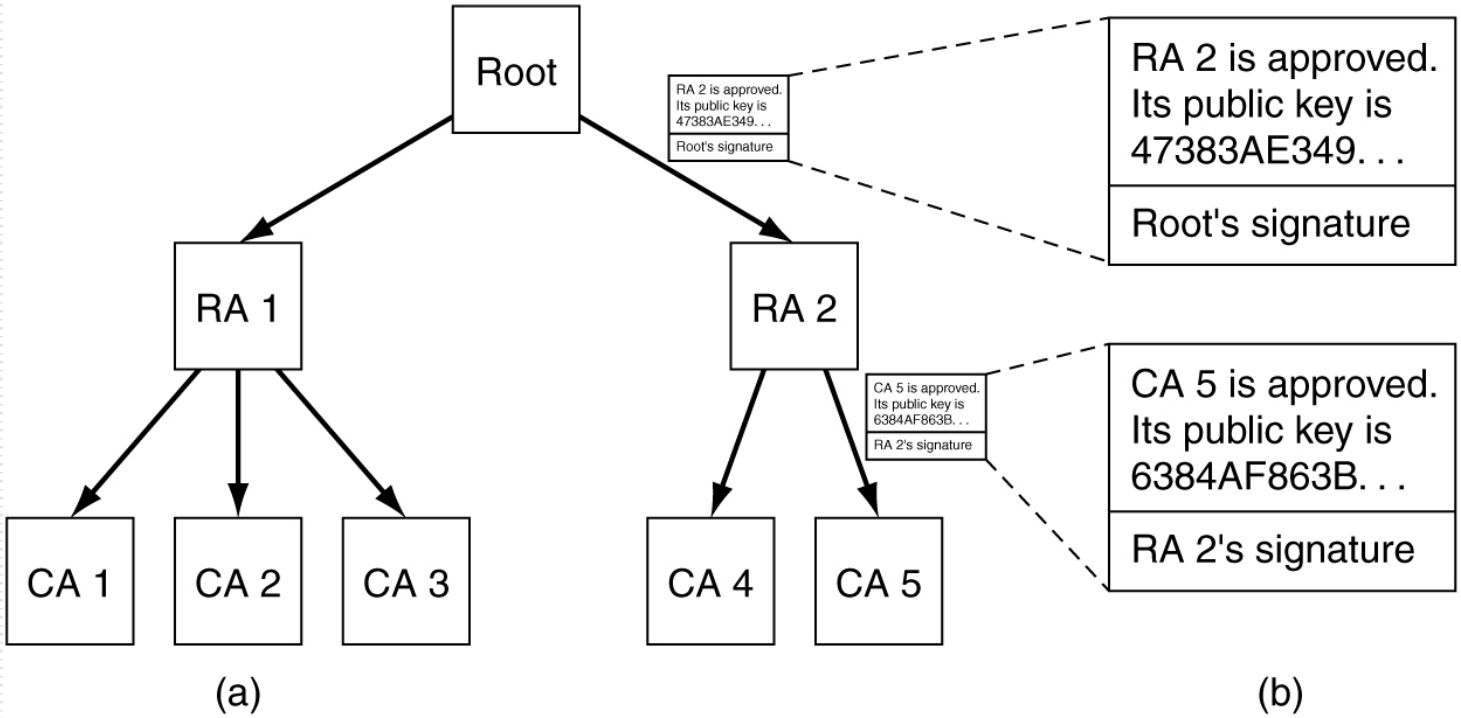
Crytography (12)

- **Management of Public keys**
  - By checking the signature, one can determine that a public key belongs to a given user.



Crytography (13)

- **Public-Key Infrastructure (PKI)**



(a) A hierarchical PKI. (b) A chain of certificates.

Outline

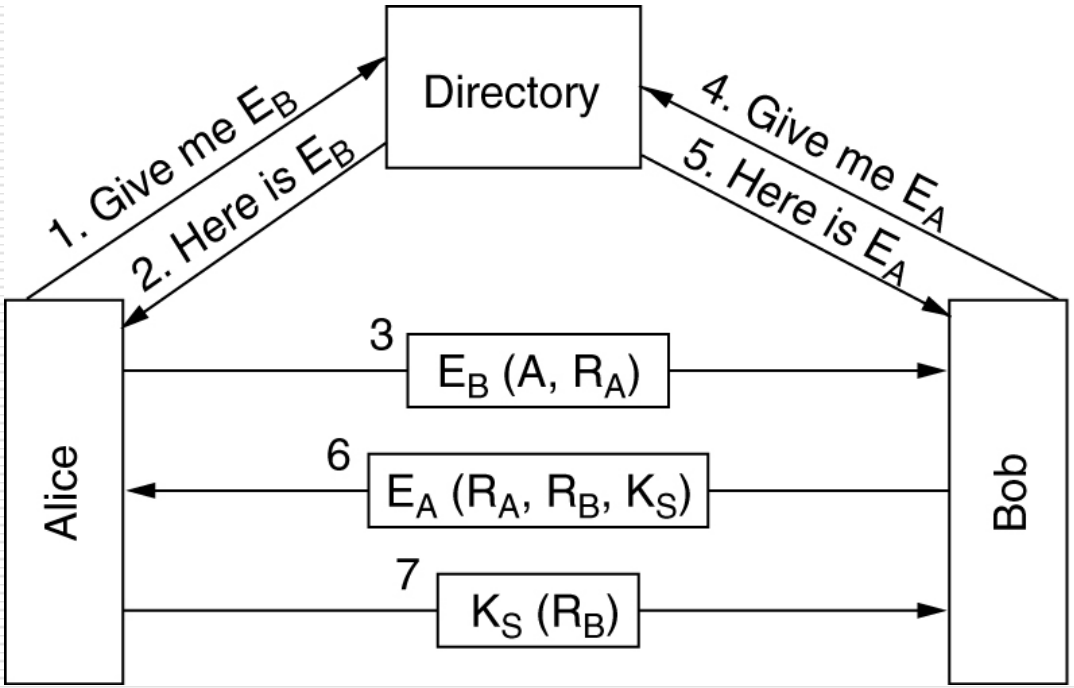
- **Apply to Computer Networks**
  - Terms
    - Authentication
    - Authorization
    - Message Protection
  - Secure Sockets Layer (SSL)
  - E-mail security
  - Web Security

Apply to Computer Networks(1)

- **Authentication**
  - Verification of identity.
  - Many mechanisms exist:
    - Username/password
    - Kerberos
    - Public key Cryptography

Apply to Computer Networks(2)

- **Authentication**
  - Authentication Using Public-Key Cryptography



Apply to Computer Networks(3)

- **Authorization**
  - Verification of rights
  - Many mechanisms exist for specification and enforcement:
    - By operating system (e.g., unix file permissions)
    - By application (e.g., permissions within a DBMS)
  - Usually requires authentication, but doesn't always.

Apply to Computer Networks(4)

- **Message Protection**
  - Integrity
    - Authenticate the message.
    - Verify that the message received is the same message that was sent.
    - A signature is a message integrity mechanism that can be verified even if the sender is offline.
  - Confidentiality
    - Ensure that no one but the sender and recipient can read the message.

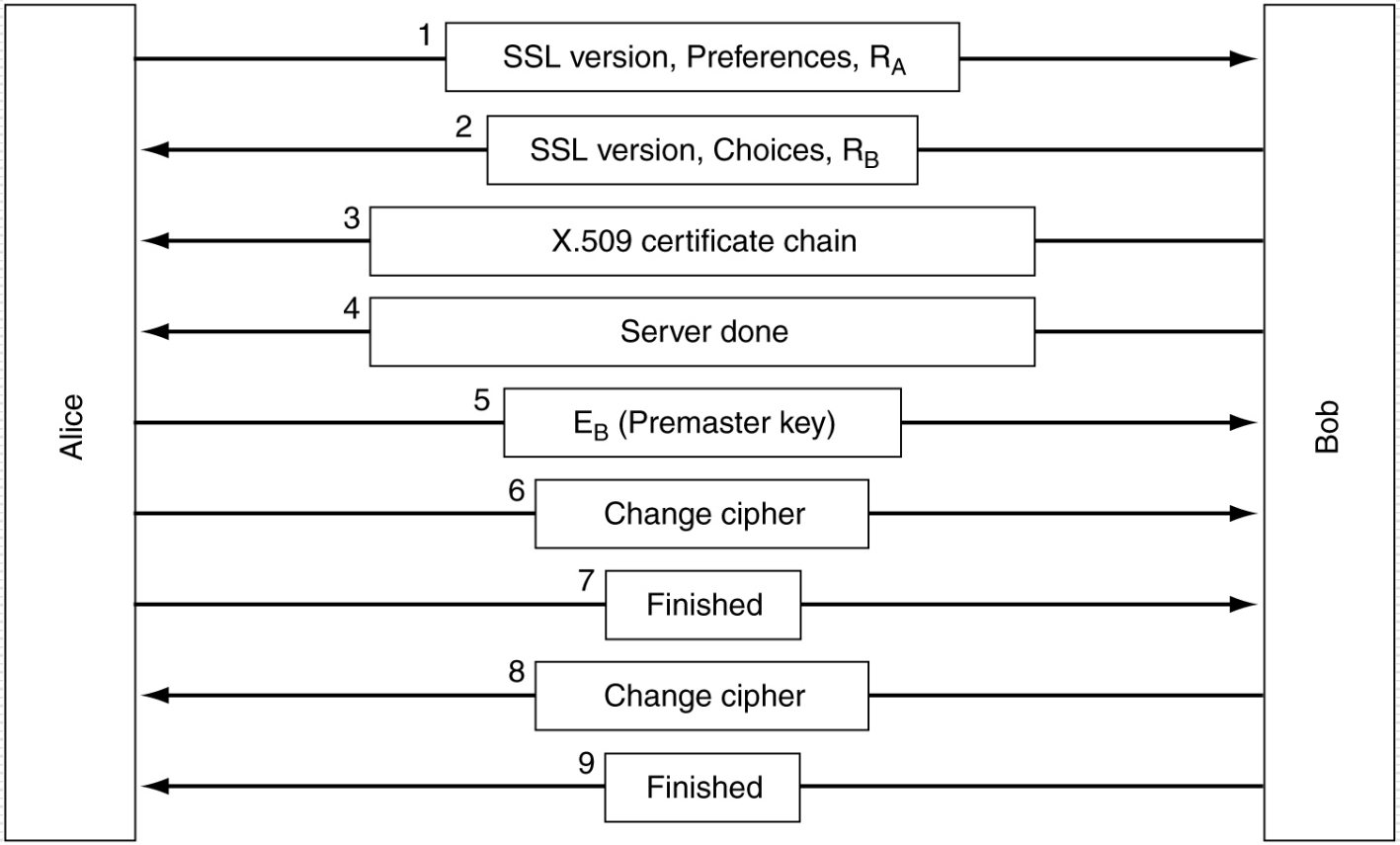
Apply to Computer Networks(5)

- **Secure Sockets Layer(SSL)**

Application (HTTP)
Security (SSL)
Transport (TCP)
Network (IP)
Data link (PPP)
Physical (modem, ADSL, cable TV)

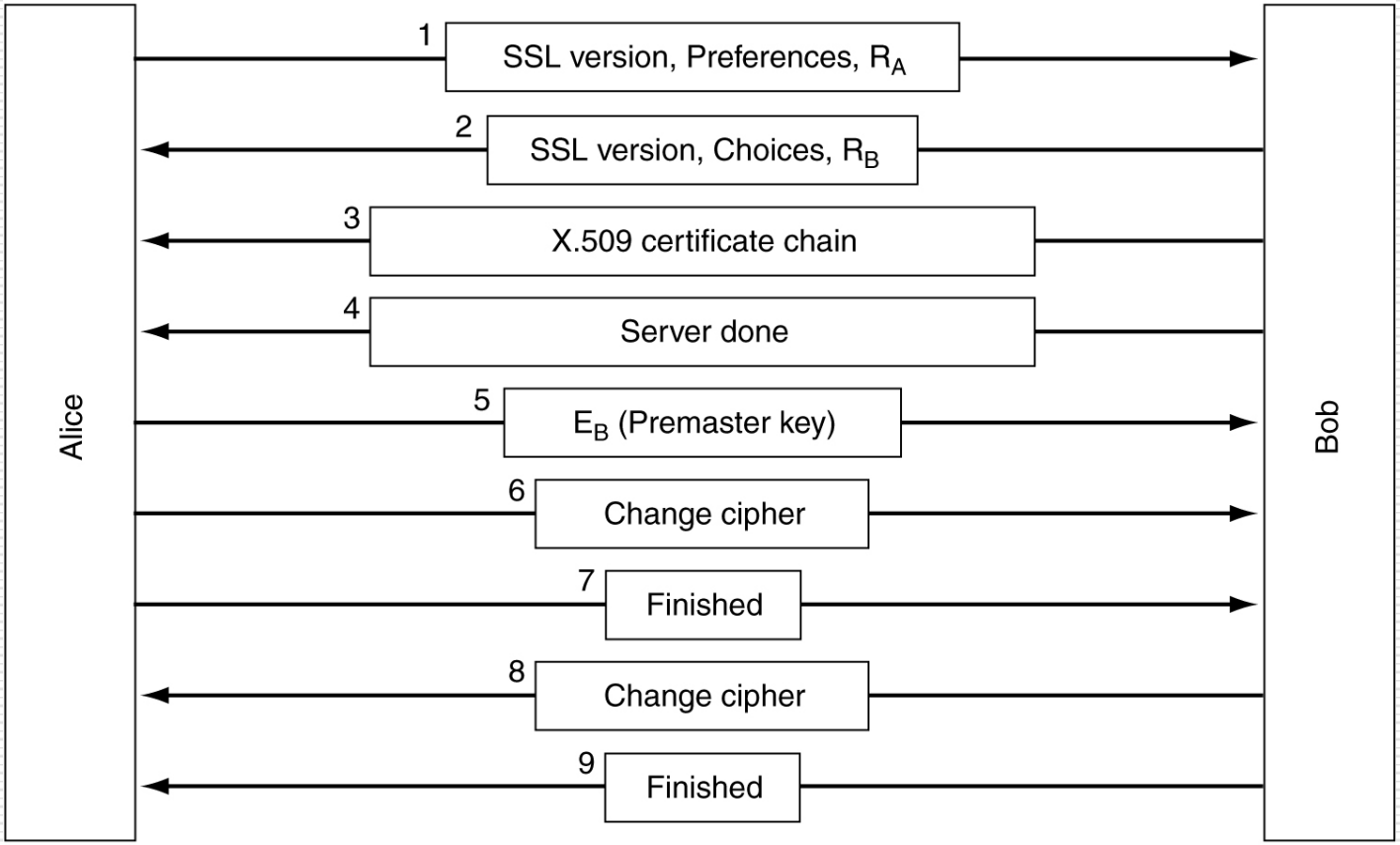
Apply to Computer Networks(6)

- **Secure Sockets Layer(SSL)**



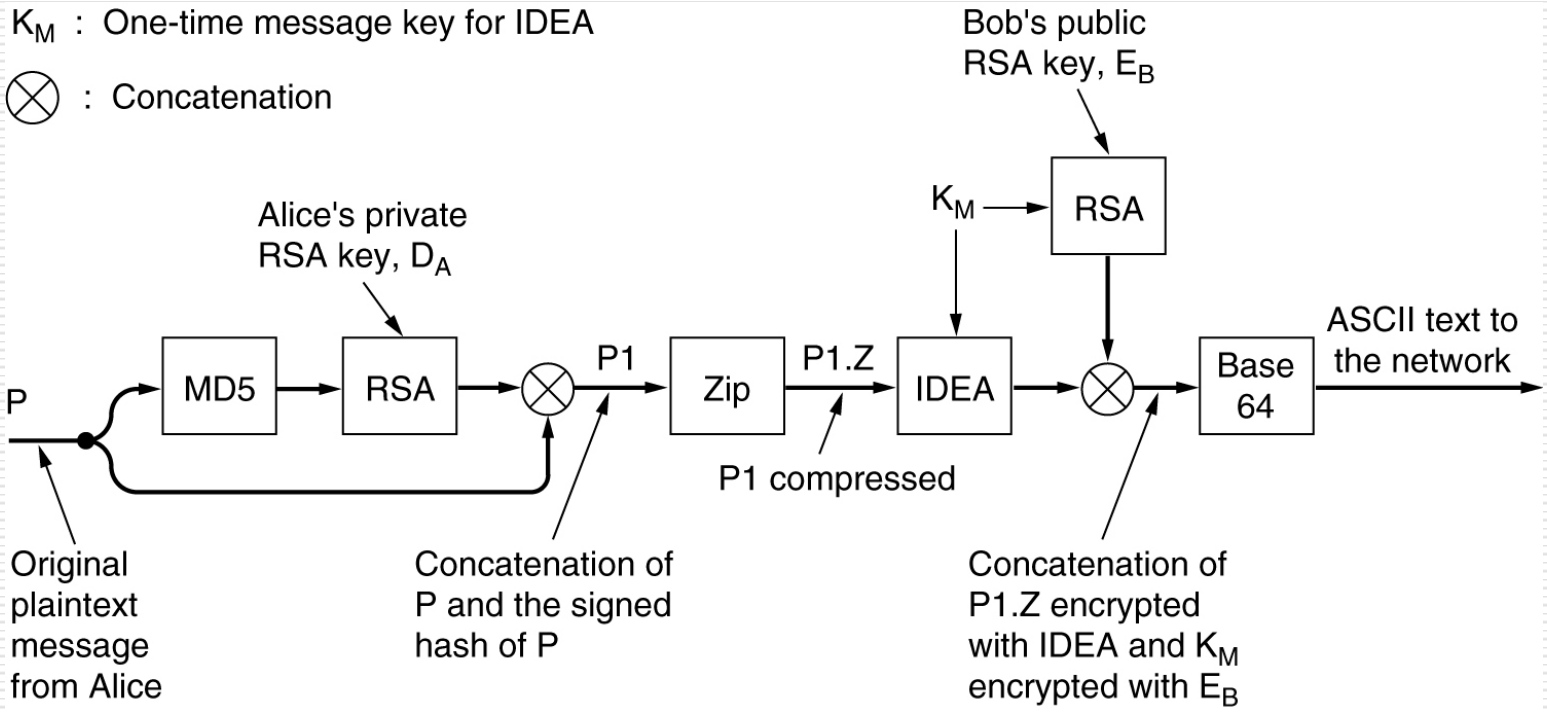
Apply to Computer Networks(7)

- **Secure Sockets Layer(SSL)**



Apply to Computer Networks(8)

- **Mail security**
  - Pretty Good Privacy(PGP)



Apply to Computer Networks(9)

- **Web security**
  - HTTPS (HTTP + SSL)