Chapter 8:
Security in Computer Networks

- Security Goals
- Cryptography
- Authentication
- Digital Signature

Security Goals

- Confidentiality
  - to assure that information is available and disclosed only to the authorized parties
  - privacy - assures that individuals control what information related to them may be collected and stored and by whom and to whom that information may be disclosed
- Integrity
  - data integrity – assures that information can be modified only by authorized parties and only in authorized ways
  - system integrity – assures that a system performs its intended function in an authorized way, free from unauthorized manipulation of the system

Security Goals

Availability

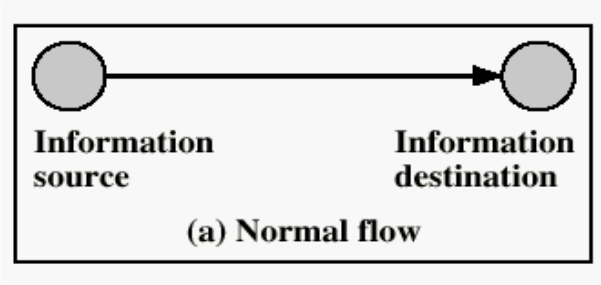
- assures that systems work promptly and service is not denied to authorized users

Authenticity

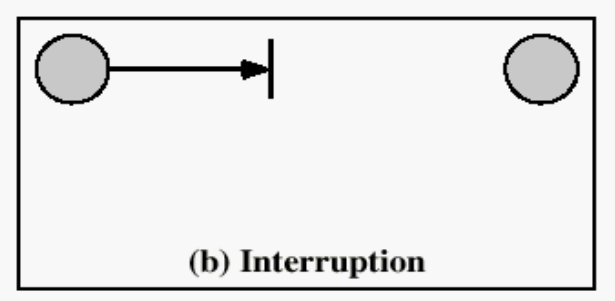
- user authenticity – individuals can assure the validity of the identity of peer
- message authenticity – receivers can assure the originality of the message

Security Attacks

- Normal information flow

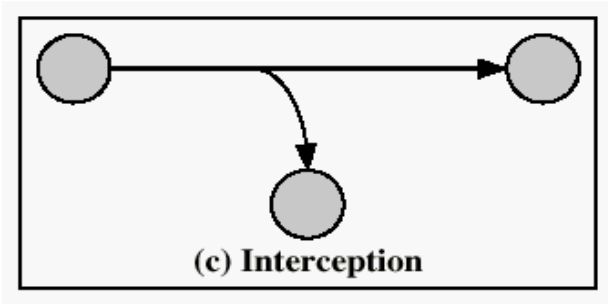


- Interruption: attack on availability

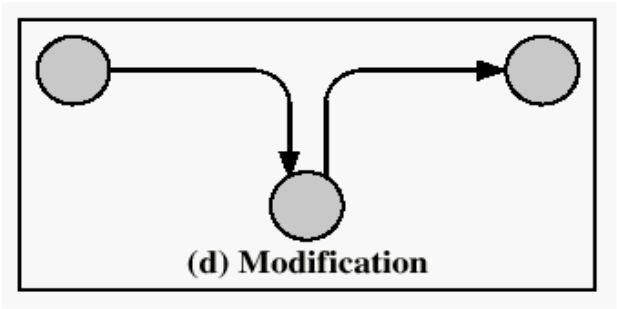


Security Attacks

- Interception: attack on confidentiality

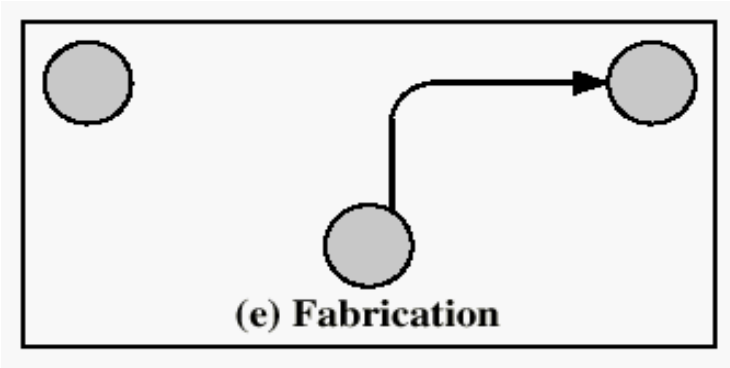


- Modification: attack on integrity



Security Attacks

- Fabrication: attack on authenticity



Security Attacks

Passive attacks:

- Interception
  - attacks confidentiality a.k.a., eavesdropping (or sniffing)
  - Encryption is an effective means to protect interception
- Traffic Analysis
  - attacks confidentiality, or anonymity
- Difficult to detect
  - the emphasis is on prevention

Security Attacks

Active attacks:

- Interruption: attacks availability
  - e.g., denial-of-service attacks
- Modification: attacks integrity
  - e.g., man-in-the-middle attacks, masquerading
- Fabrication: attacks authenticity
  - e.g., replay attacks

Security Manager

Security manager should consider

- Prevention
  - taking measures that prevent damage from possible attacks
  - (e.g.) strong passwords, one-time passwords
- Detection
  - measures that allow detection of when an asset has been damaged, altered, or copied
  - E.g., access logging, intrusion detection system

Security Manager

Security manager should consider

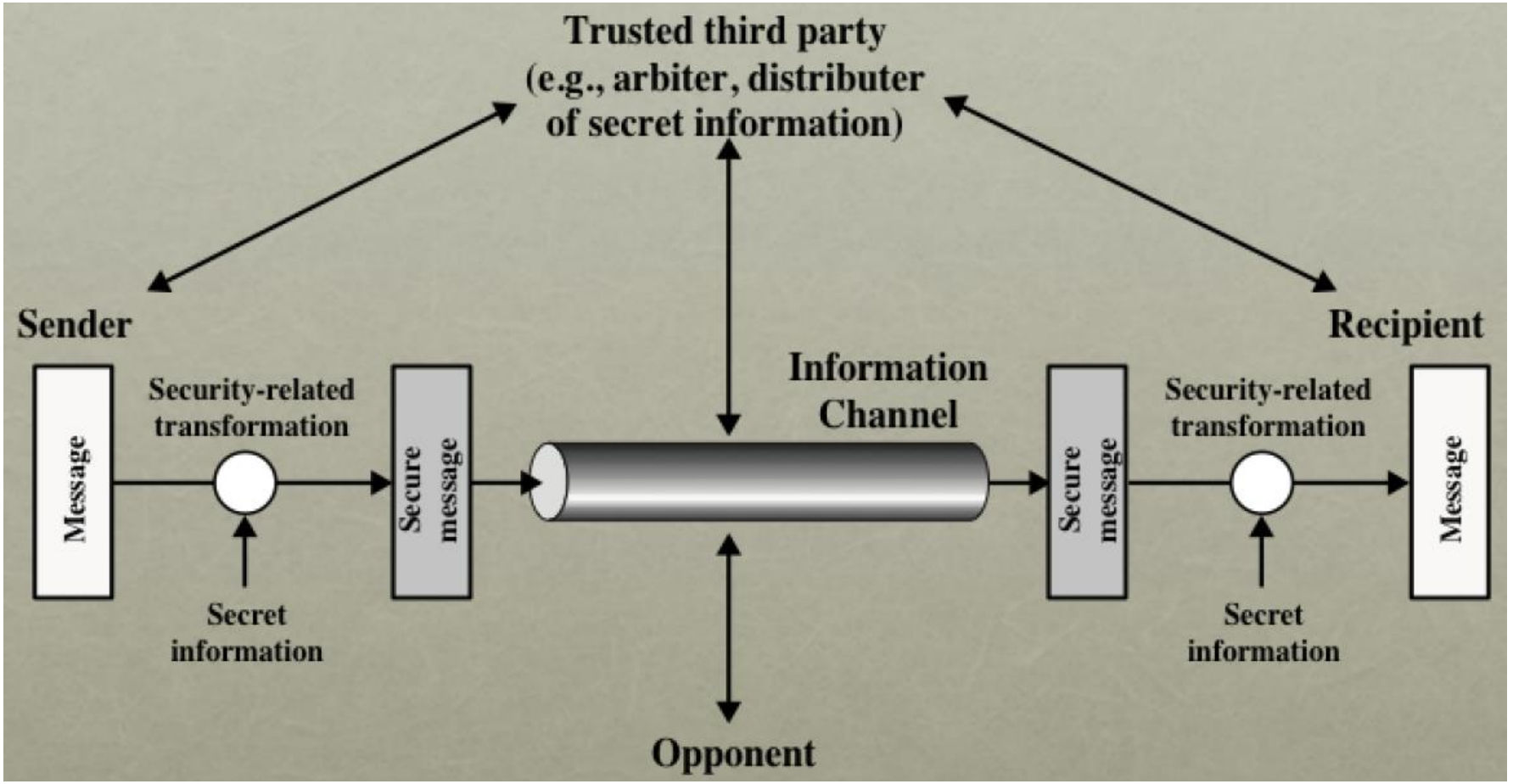
- Recovery
  - restoring systems that were compromised
  - (e.g.) periodic backup
- Assets
  - should know the assets to protect and the value of the assets
  - Assets: hardware, software, data, and person

Secure or Not?

What does it mean for information to be secure?

- The cost of breaking the security exceeds the value of the secured service or information
- The time required to break the security exceeds the useful lifetime of the information

Network Security Model



Network Security Model

- Security techniques has two components:
  - A security-related transformation on the information to be sent
  - Some secret information shared by the principals
- Trusted third party:
  - responsible for distributing the secret information to the principals
  - Arbitrate disputes among the principals

Cryptography

- Cryptography relies on
  - Ciphers: *mathematical functions used for encryption and decryption of a message*
  - ***Encryption*** : the process of disguising a message in such a way as to hide its substance
  - Ciphertext: an encrypted message
  - ***Decryption*** : the process of returning an encrypted message back into plaintext.

Ciphers

- The security of a cipher which depends on the secrecy of its *restricted* algorithm is not good
  - Whenever a users leaves a group, the algorithm must change
  - Secrecy can be broken by people smarter than you
- Modern cryptography relies on *keys, a selected value from a large set (a key-space)*
  - *e.g., a 1024-bit key => 2^{1024} values!*
  - Security is based on secrecy of the key, not the details of the algorithm
  - Change of authorized participants requires only a change in key

Cryptosystem

Conventional cryptosystem

- Secret-key cryptosystem, symmetric cryptosystem

- key distribution issue
- (e.g.) DES, 3-DES, AES, SEED-128, SEED-256

Cryptosystem

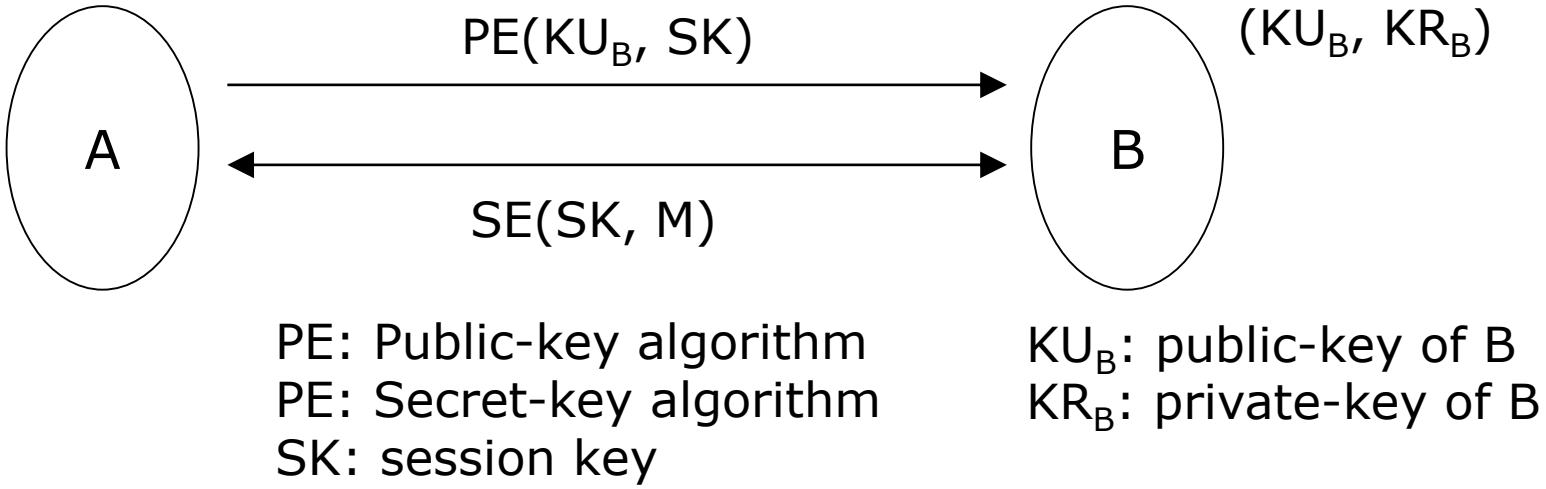
Public-key cryptosystem

- Asymmetric cryptosystem: (public-key, private-key)

- (e.g.) RSA, Elliptic curve
- encryption : only the private key can decrypt a message encrypted with the public key
- digital signature : only the public-key can decrypt a message encrypted with the private key
- slower than secret-key algorithms

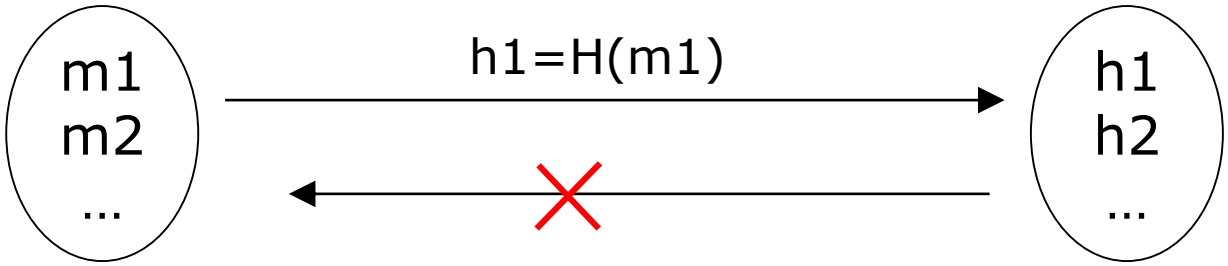
Cryptosystem

- Hybrid of symmetric and public-key approaches
  - Public key cryptosystem is used to distribute a session key (key for conventional cryptosystem) among peers
  - Conventional cryptosystem is used to encrypt/decrypt messages



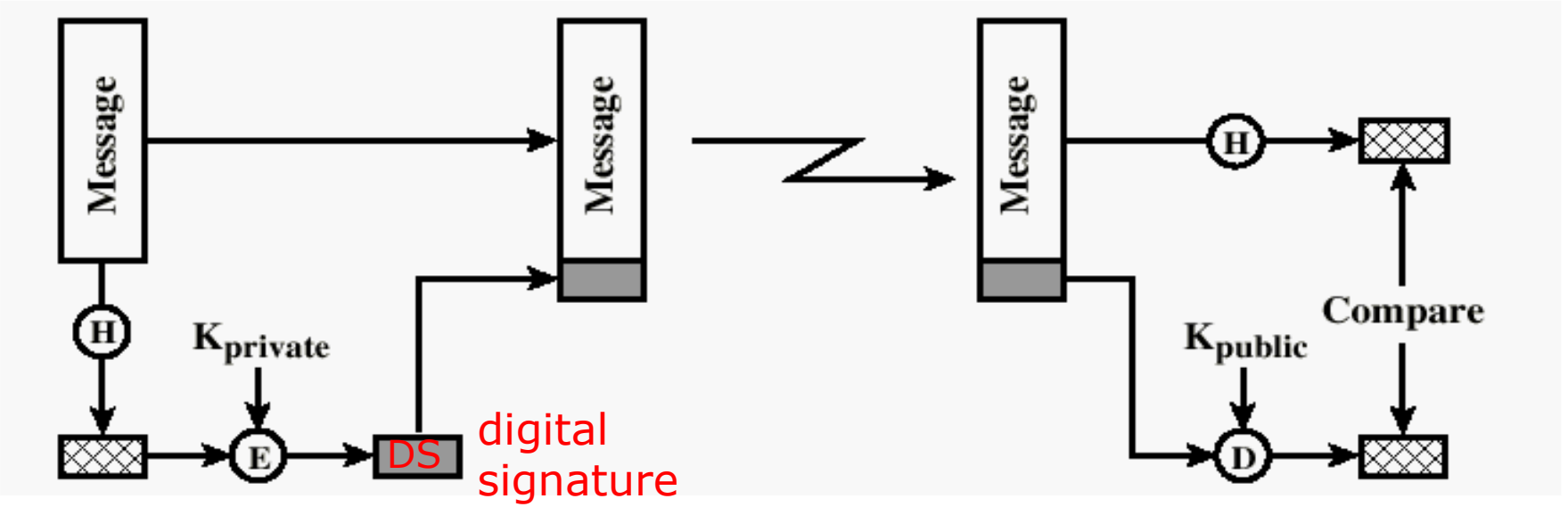
Cryptosystem

- Hash algorithms (H) : produce a ”fingerprint”
  - *H* : one-way function (SHA-1, SHA-256, MD5, etc.)
  - *H* can be applied to a block of data at any size and produces a fixed length output
  - *H(x)* is easy to compute for any given x
  - For any given block (x, h=H(x)), it is computationally infeasible to find y such that H(y) = h



Cryptosystem

- Hash algorithms and message authentication
  - Message Authentication using public-key algorithm

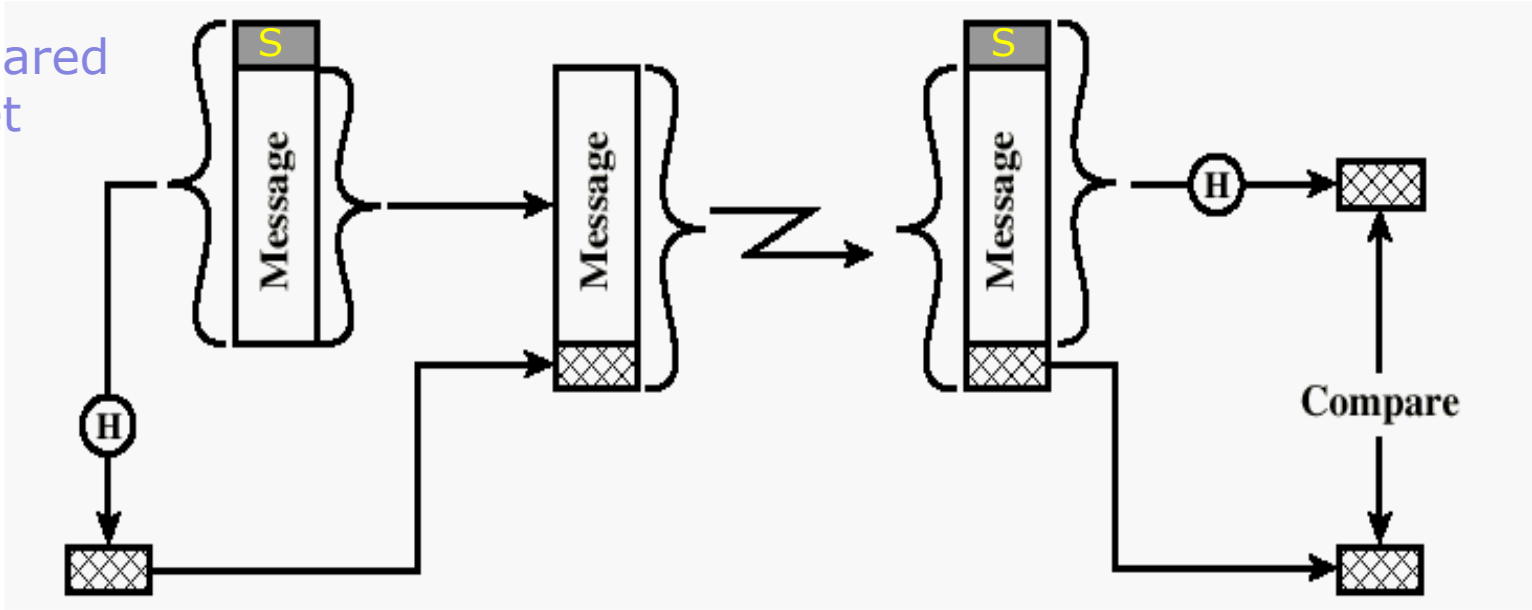


$K_{private}$: private-key of B
K_{public} : public-key of B

Cryptosystem

- Hash algorithms and message authentication
  - Message Authentication using shared secret

S: shared secret

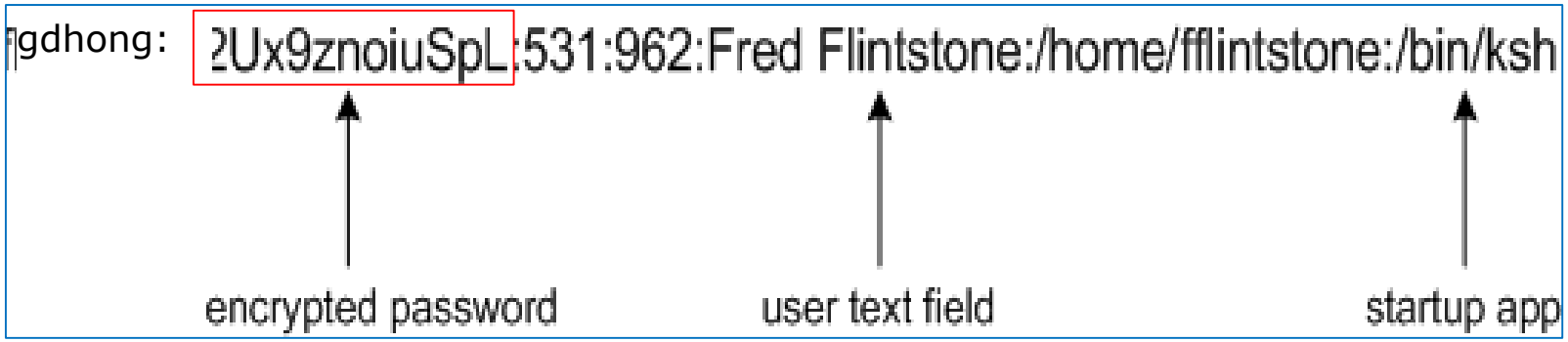


Authentication

- Password based authentication
  - The password file could be stolen
  - An eavesdropper can sniff the password off the network
- Authentication based on the source address
  - IP spoofing is possible
- Authentication based on biometrics : thumb prints, retinal scans
- Authentication using symmetric keys : Kerberos
- Authentication using asymmetric cryptosystem

Password-based Authentication

- Actual password is not stored -> one-way hashes of passwords are kept and are used for comparison
- encrypted password in /etc/passwd → dictionary attack is possible



- shadowed password: only the “root” user can read the password hashes in the /etc/shadow password file

Protecting Passwords over the network

- If Alice just sends the password, anyone can read it
- In *promiscuous* mode, Ethernet cards will pass to the operating system all received IP packets
- Attackers can use a “packet-sniffer”, like wireshark or tcpdump on Unix, to read all packets across your network
- Such programs require root privileges

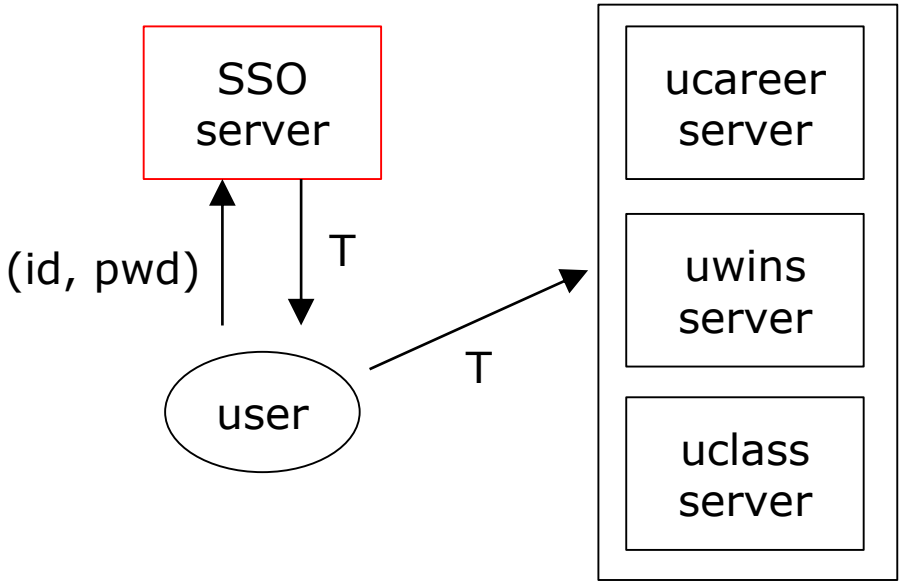
Authentication Using One-time Password (OTP)

Challenge-response method

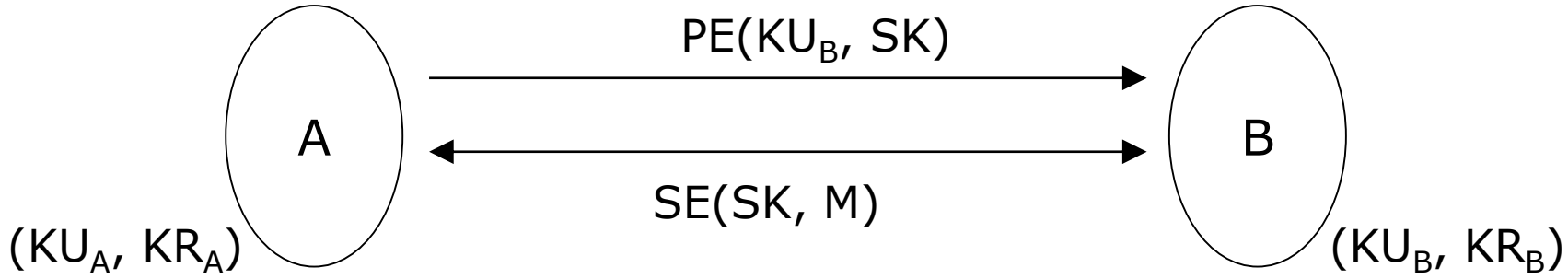
- Alice and Bob agree upon a shared, secret key (K_{AB})
- Alice requests a log-in challenge from Bob (the remote computer) : A->B: *access request*
- Bob sends Alice a *nonce N* (challenge): B->A: N
  - A nonce is a random string used only once ever
- Alice responds (response) : A->B: $E(K_{AB},N)$
- Changing nonces for each access prevents replay attack

Single-Sign-On (SSO)

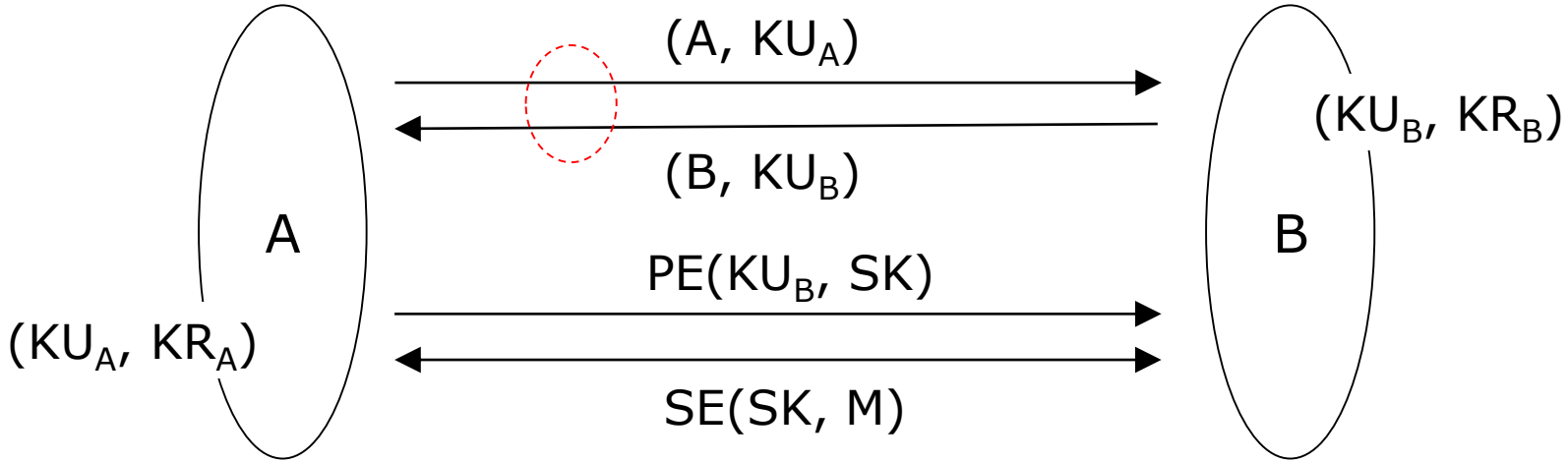
- SSO service
  - User receives an access token (T) after the authentication from SSO server; T can be used in a limited amount of time
  - User accesses the application server using the token T



Public-key Certificate

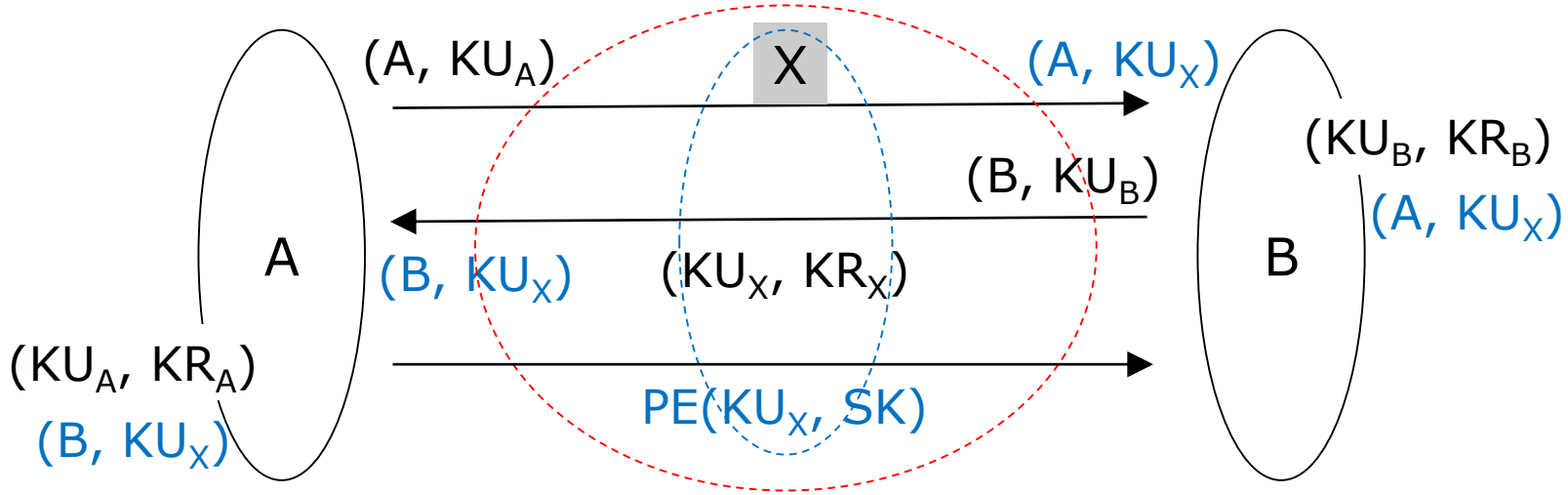


- How can we get public key of the peer?



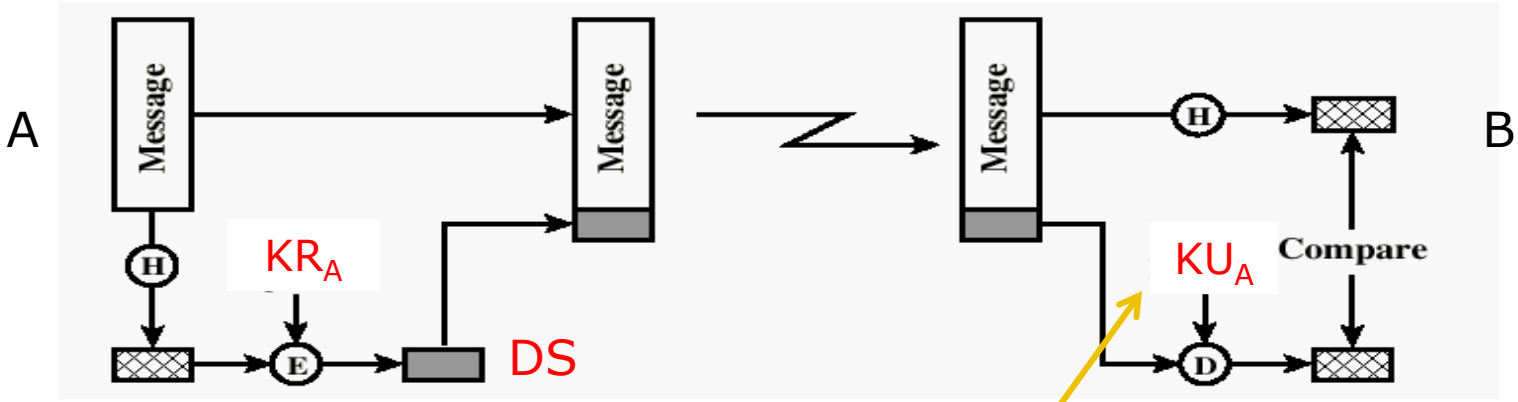
Public-key Certificate

- Man-in-the-middle (MITM) attack
  - attacker intervenes in the step of public key exchange



Public-key Certificate

- Certificate: (owner, public-key, DS of CA)
- Certification Authority (CA)
  - Issues a certificate for a user
  - Each certificate is signed by the CA



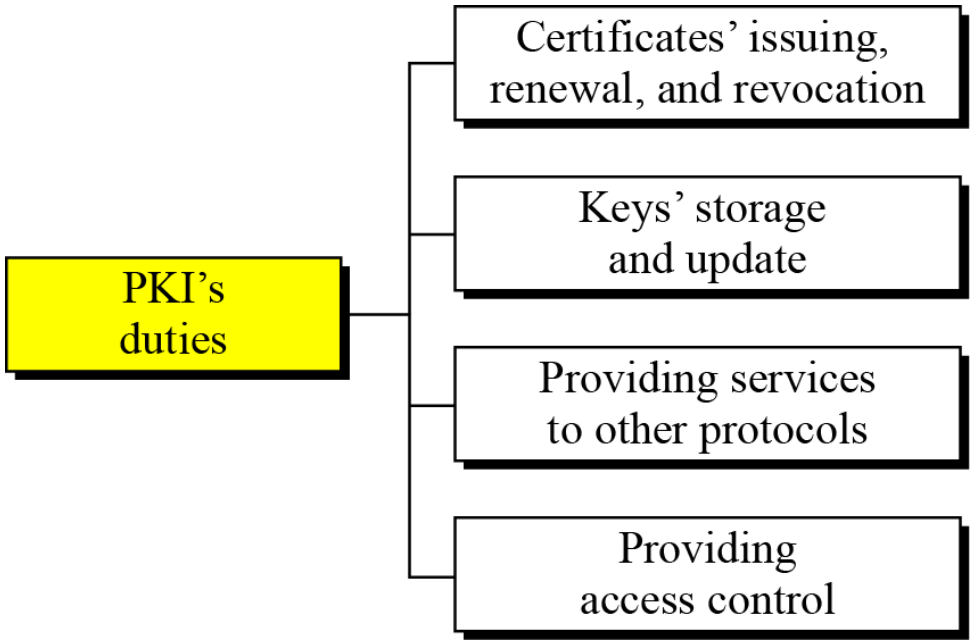
KR$_A$: private-key of A
KU$_A$: public-key of A

We need a correct peer's public key. How?

Public-Key Infrastructure

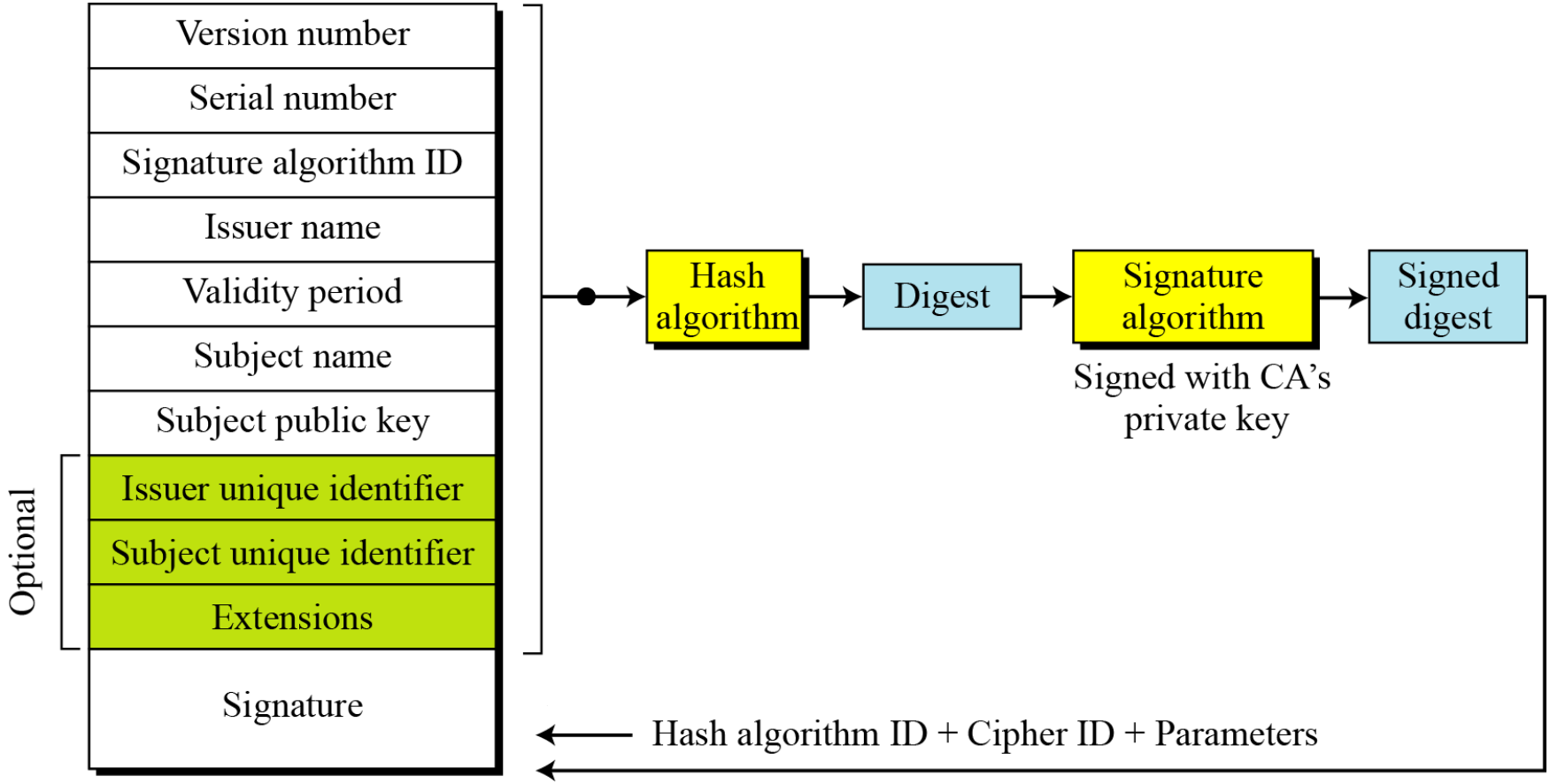
Public-Key Infrastructure (PKI)

- An intra-structure to enable users to get correct public keys of others



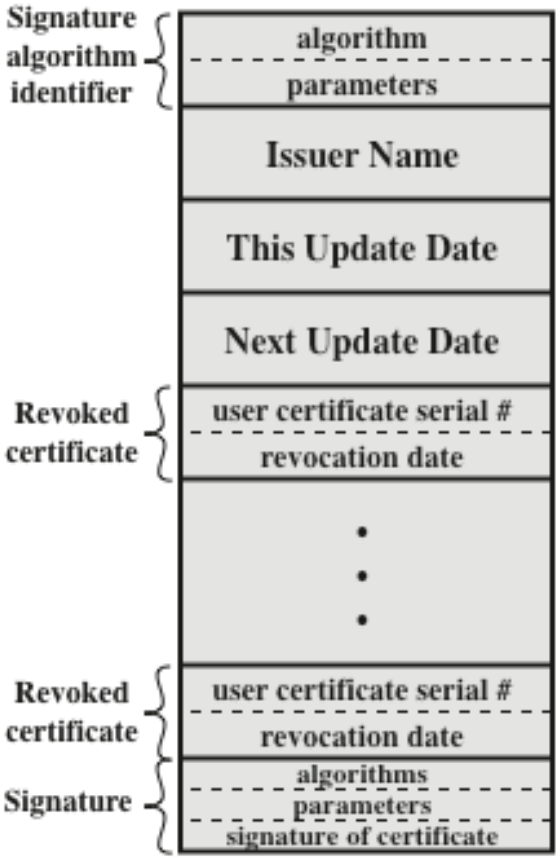
X.509 Public-key Certificate

- X.509 certificate format



Revocation of Certificates

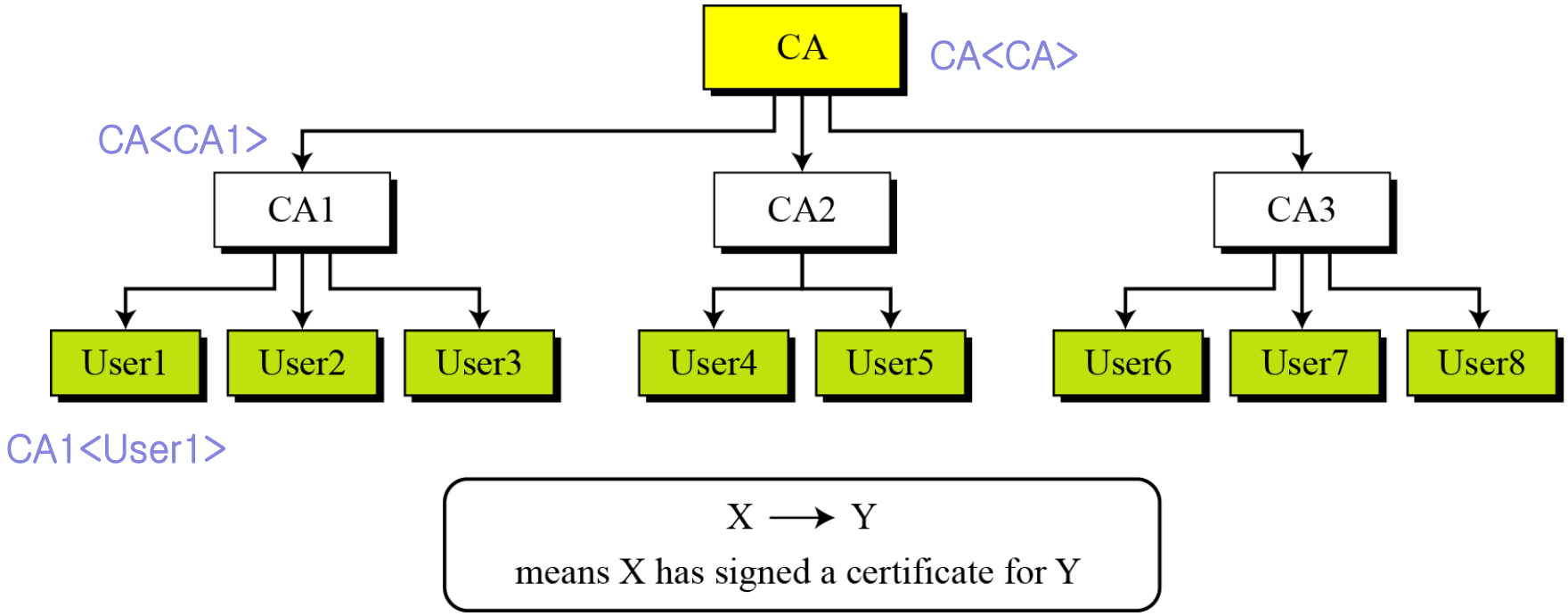
- Reasons for revocation:
  - The users private key is assumed to be compromised
  - The user is no longer certified by this CA
- CRL (Certification Revocation List)
  - Each CA keeps CRL and updates CRL periodically
  - Checks certificate's validity from CRL
- Delta Revocation
  - To make revocation more efficient, the delta CRL has been introduced



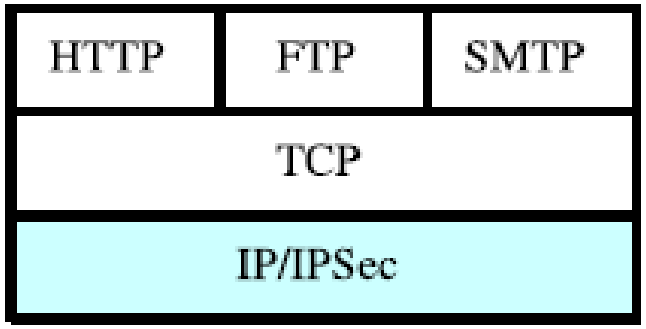
(b) Certificate Revocation List

Public-Key Infrastructure

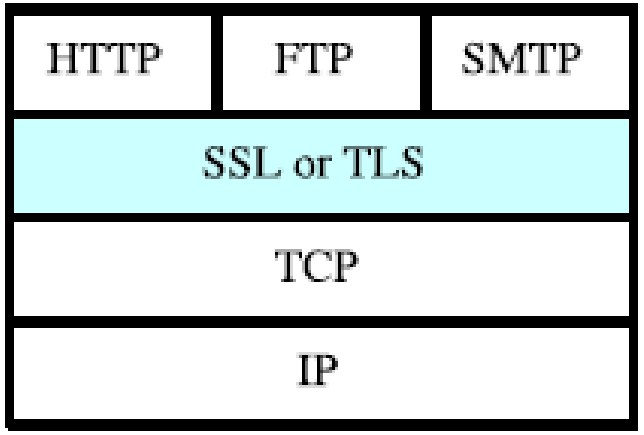
- PKI trust model
  - Hierarchical model



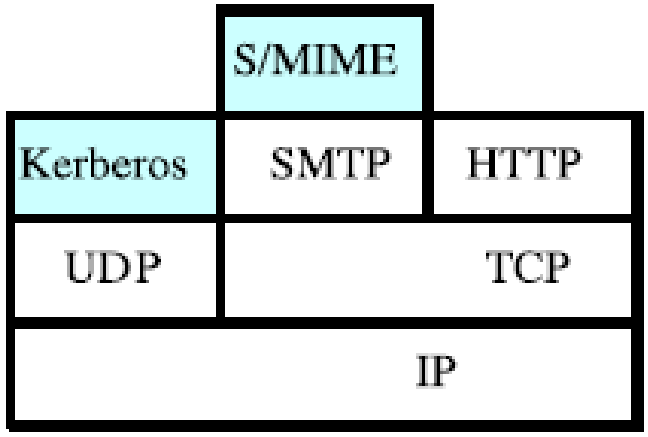
Security in Internet Protocols



IP layer security



Transport layer security



Application layer security

Security in Internet Protocols

- Security protocols in application layer
  - E-mail service : S/MIME, PGP
  - DNS service : DNSSEC
  - SET protocol
- Security protocols in transport layer
  - SSL (TLS) protocol
  - HTTP service (https) : http – SSL – tcp
- Security protocols in IP layer
  - IPsec : VPN