KEY MANAGEMENT/DISTRIBUTION

LECTURE 14

Cryptography

Key Management and Distribution

- Topics of cryptographic key management / key distribution are complex
  - cryptographic, protocol & management issues
- Symmetric schemes require both parties to share a *common* secret key
- Public key schemes require parties to acquire *valid* public keys

Key Distribution

- Symmetric schemes require both parties to share a common secret key
- Issue is how to securely distribute this key
  - whilst protecting it from others
- Frequent key changes can be desirable
- Often secure system failure due to a break in the key distribution scheme

Key Distribution Alternatives

- Given parties *A* and *B* have various key distribution alternatives:
  - A can select key and physically deliver to *B*
  - third party can select & deliver key to *A* & *B*
  - if *A* & *B* have communicated previously can use previous key to encrypt a new key
  - if *A* & *B* have secure communications with a third party *C*, *C* can relay key between *A* & *B*

Key Hierarchy

- Typically have a hierarchy of keys
- Session key
  - temporary key
  - used for encryption of data between users
  - for one logical session then discarded
- Master key
  - used to encrypt session keys
  - shared by user & key distribution center

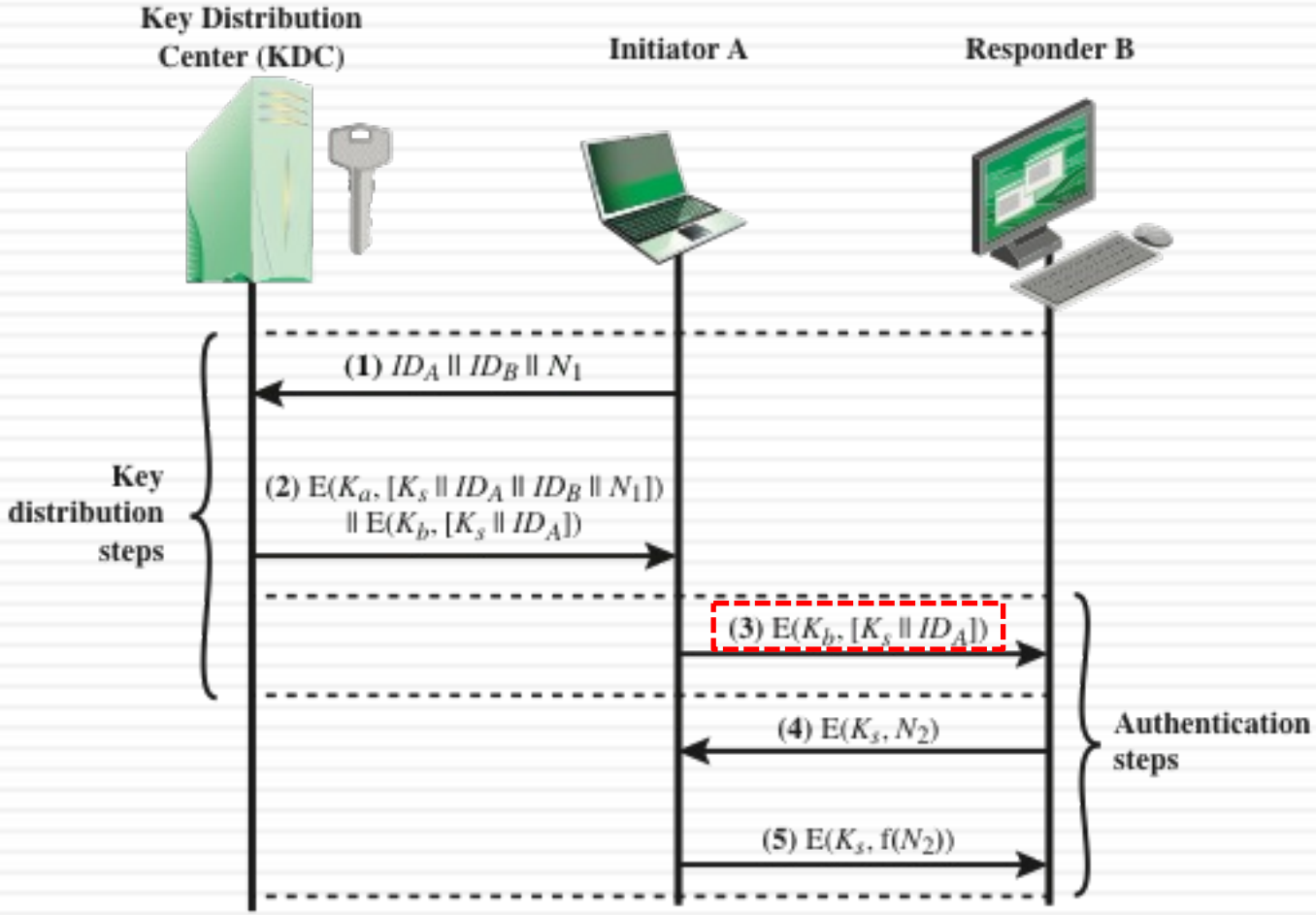


Figure 14.3 Key Distribution Scenario

Key Distribution Issues

- Hierarchies of KDC's required for large networks, but must trust each other
- Session key lifetimes should be limited for greater security
- Use of automatic key distribution on behalf of users, but must trust system
- Use of decentralized key distribution
- Controlling key usage

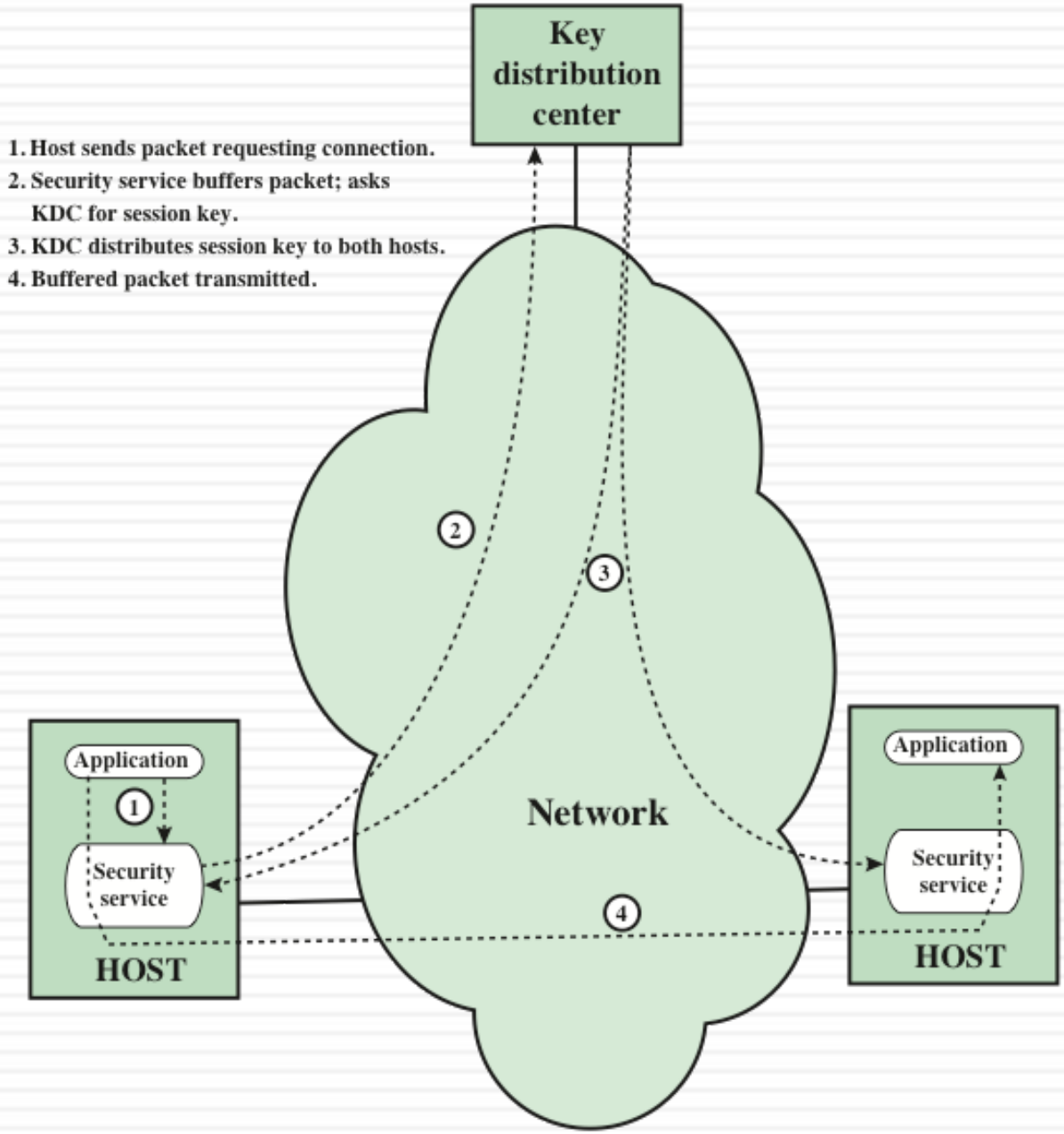


Figure 14.4 Automatic Key Distribution for Connection-Oriented Protocol

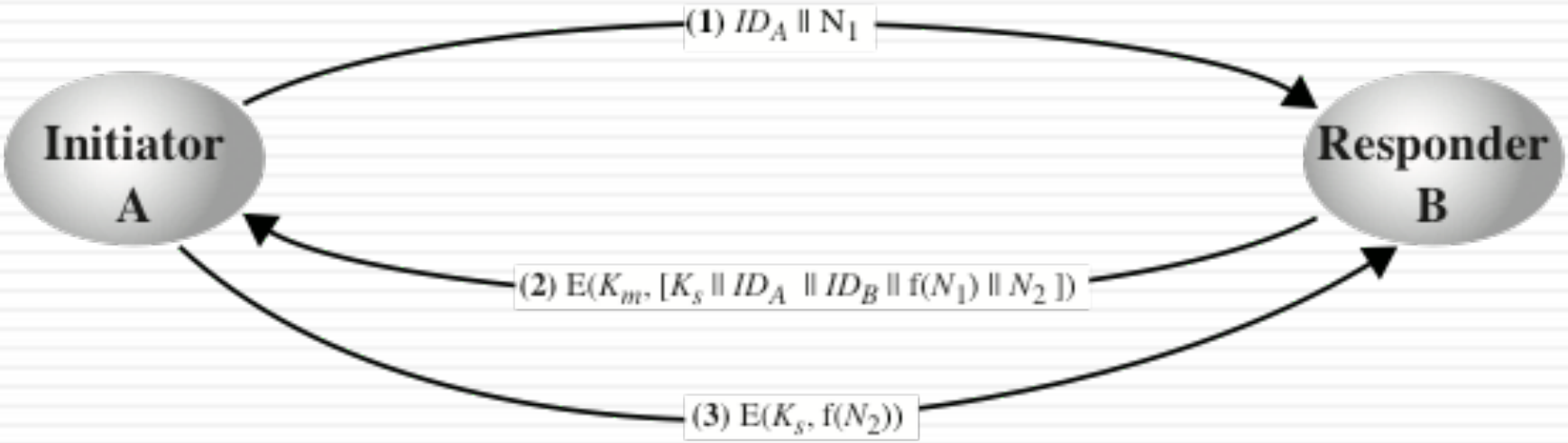


Figure 14.5 Decentralized Key Distribution

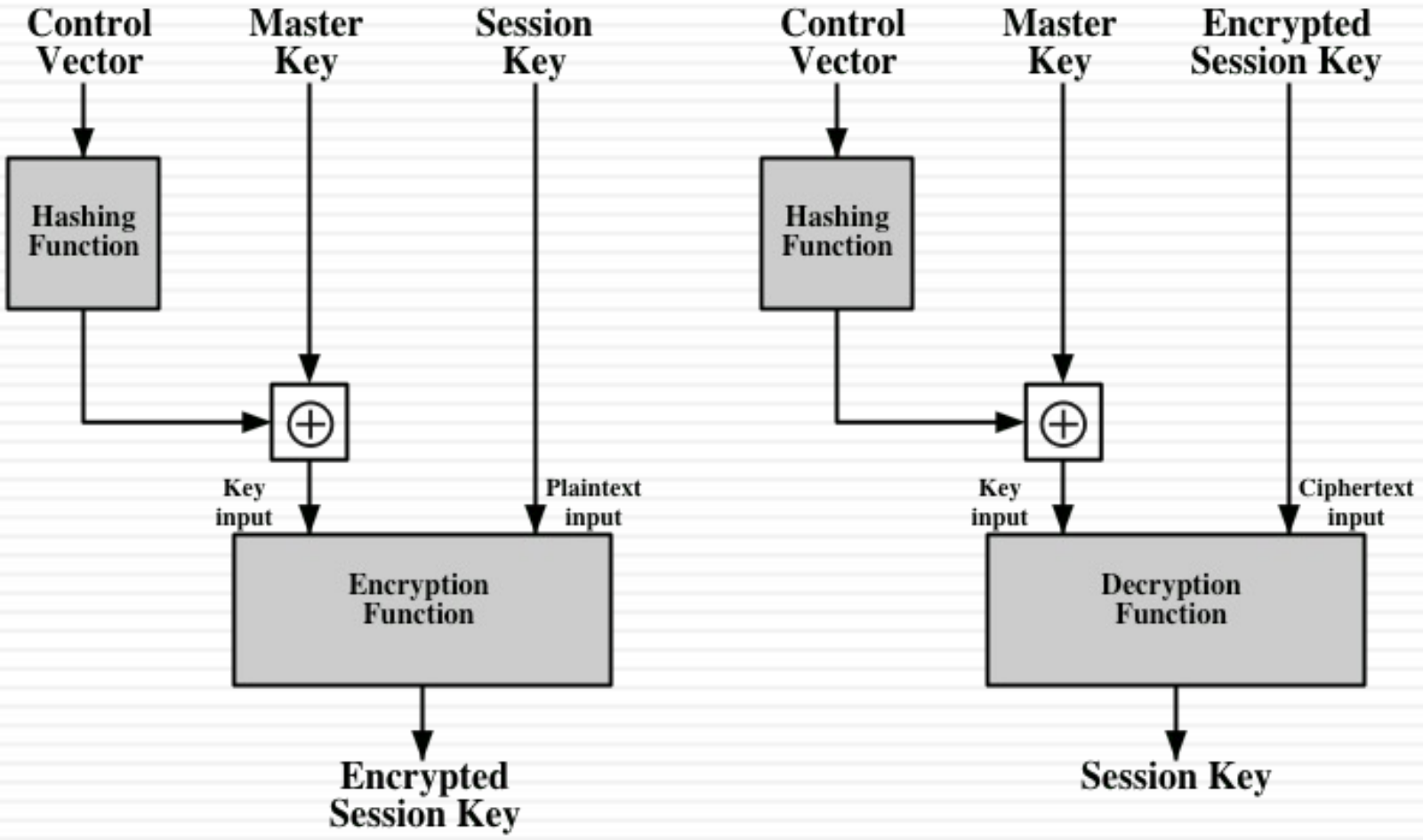
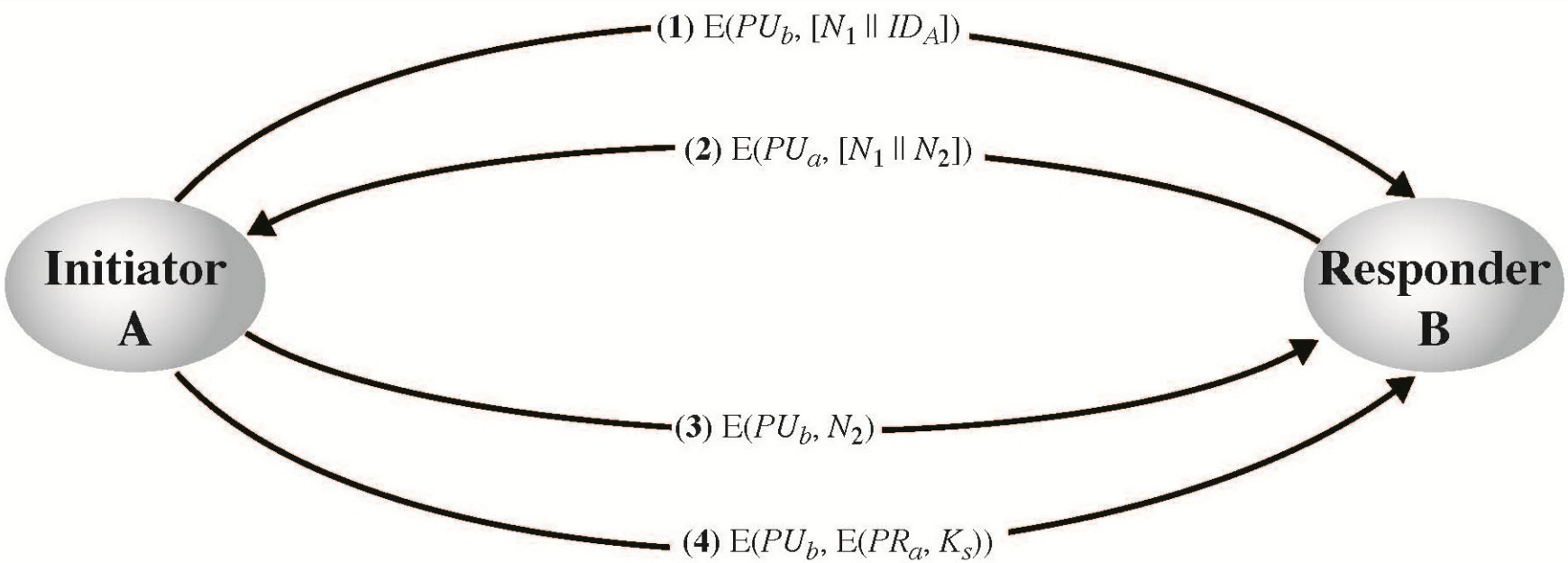


Figure 14.6 Control Vector Encryption and Decryption

Secret Key Distribution



Distribution of Public Keys

- Can be considered as using one of:
  - public announcement
  - publicly available directory
  - public-key authority
  - public-key certificates (공인인증서)

Public Announcement

- Users distribute public keys to recipients or broadcast to community at large
  - e.g. append PGP keys to email messages or post to news groups or email list
- Major weakness is forgery
  - anyone can create a key claiming to be someone else and broadcast it
  - until forgery is discovered can masquerade as claimed user

Public Announcement

Figure 14.10 Uncontrolled Public Key Distribution

Publicly Available Directory

- Can obtain greater security by registering keys with a public directory
- Directory must be trusted with properties:
  - contains {name,public-key} entries
  - participants register securely with directory
  - participants can replace key at any time
  - directory is periodically published
  - directory can be accessed electronically
- Still vulnerable to tampering or forgery

Publicly Available Directory

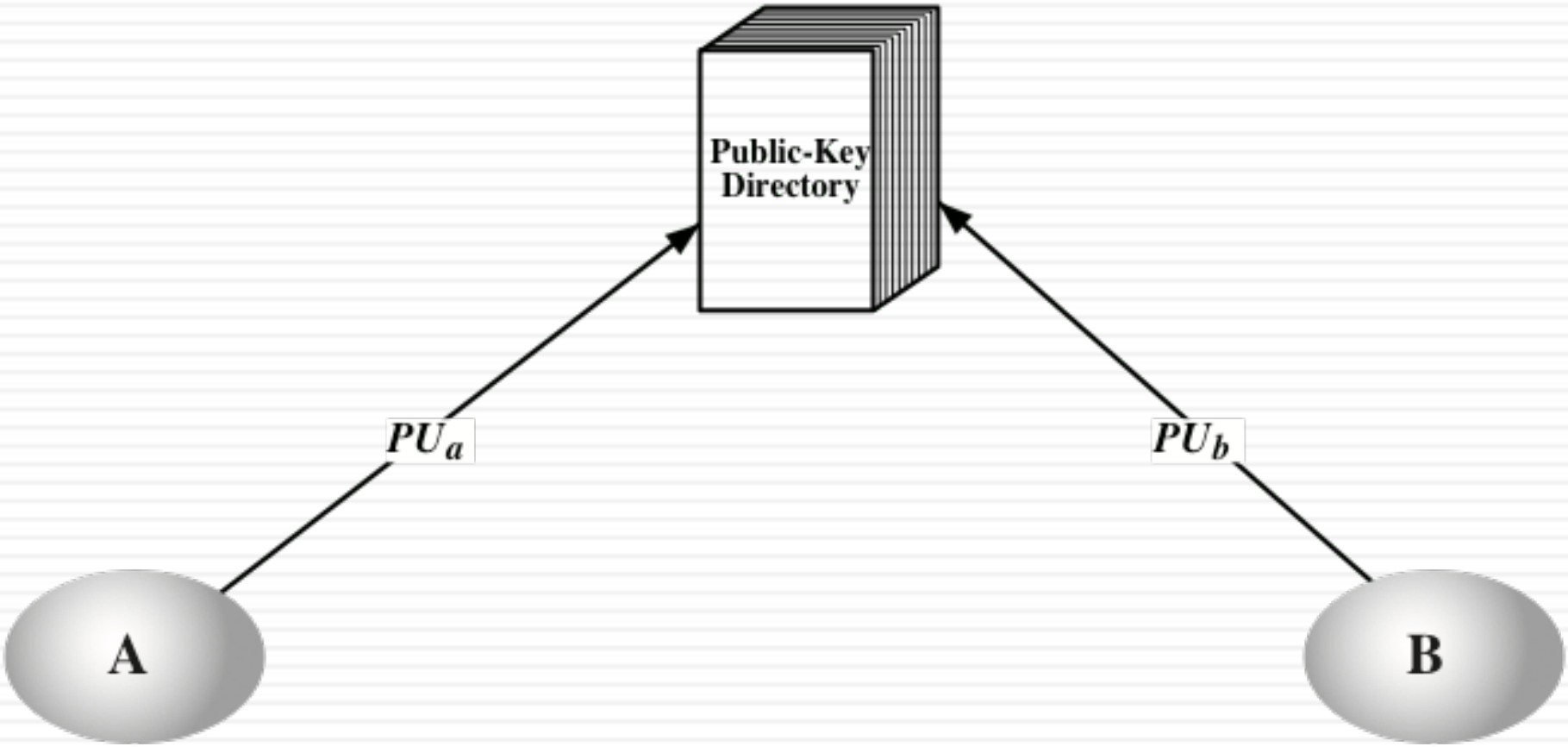


Figure 14.11 Public Key Publication

Public-Key Authority

- Improve security by tightening control over distribution of keys from directory
- Has properties of directory and requires users to know public key for the directory
- Then users interact with directory to obtain any desired public key securely
  - does require real-time access to directory when keys are needed
  - may be vulnerable to tampering

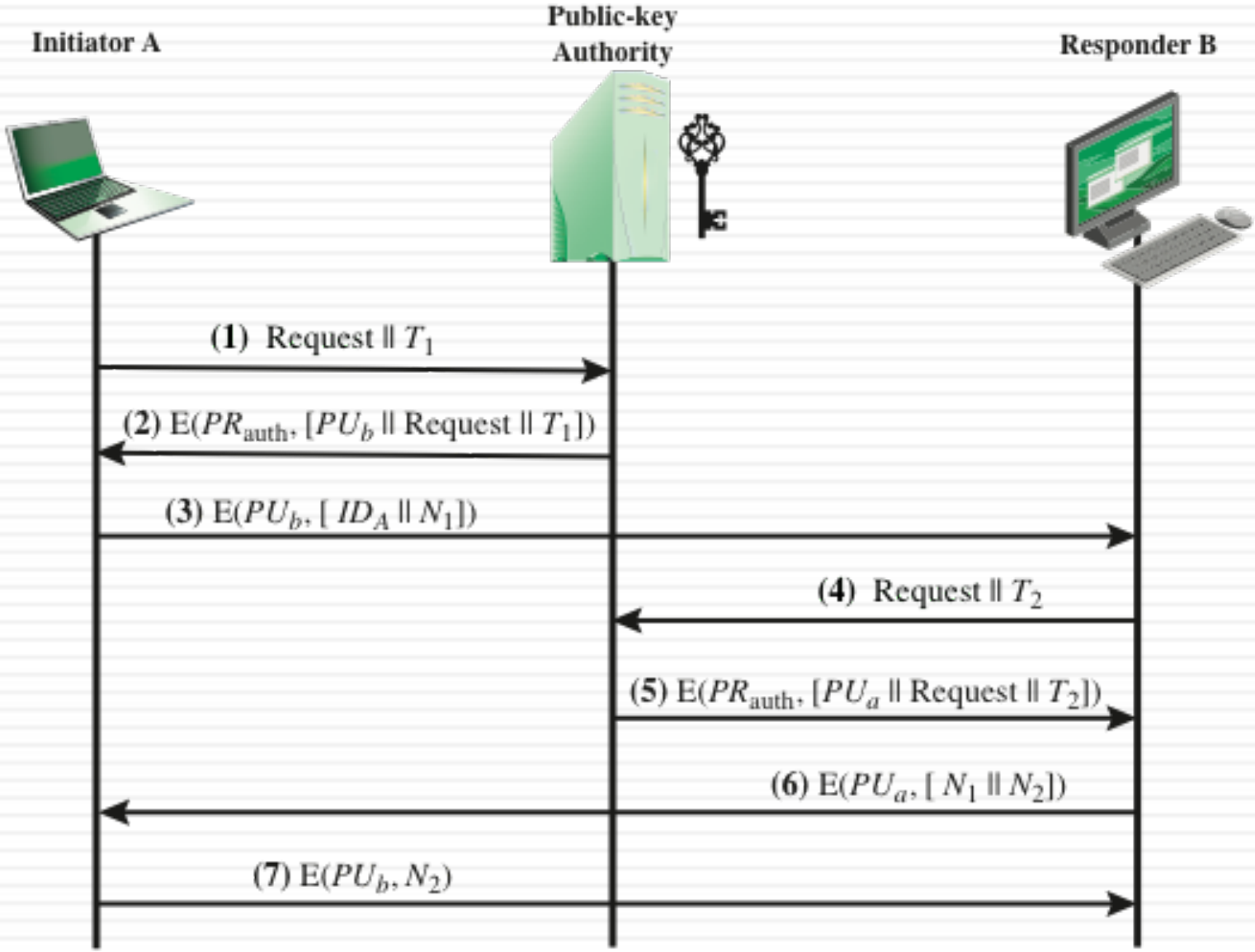
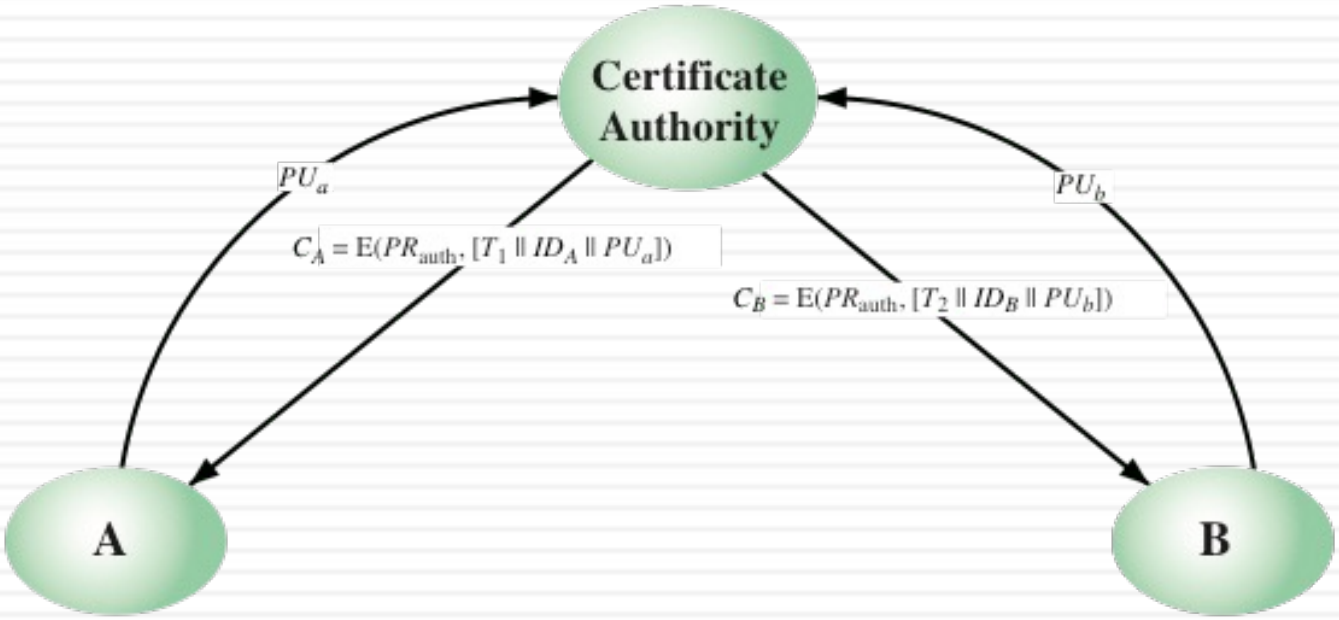


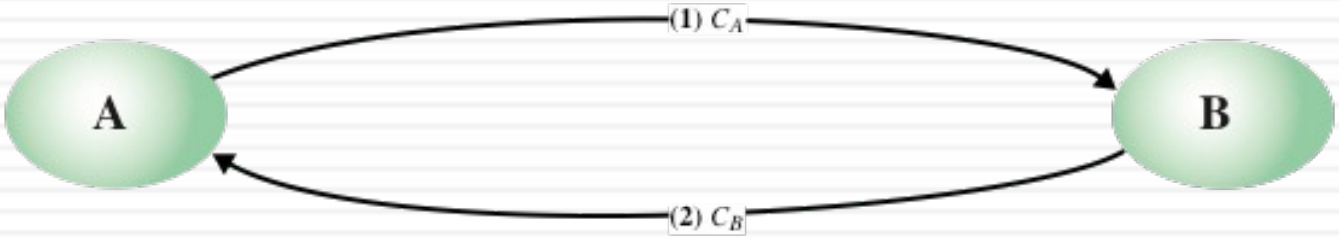
Figure 14.12 Public-Key Distribution Scenario

Public-Key Certificates

- Certificates allow key exchange without real-time access to public-key authority
- A certificate binds *identity* to *public key*
- Usually with other info such as period of validity, rights of use etc
- With all contents *signed* by a trusted Public-Key or Certificate Authority (CA)
- Can be verified by anyone who knows the public-key authorities public-key



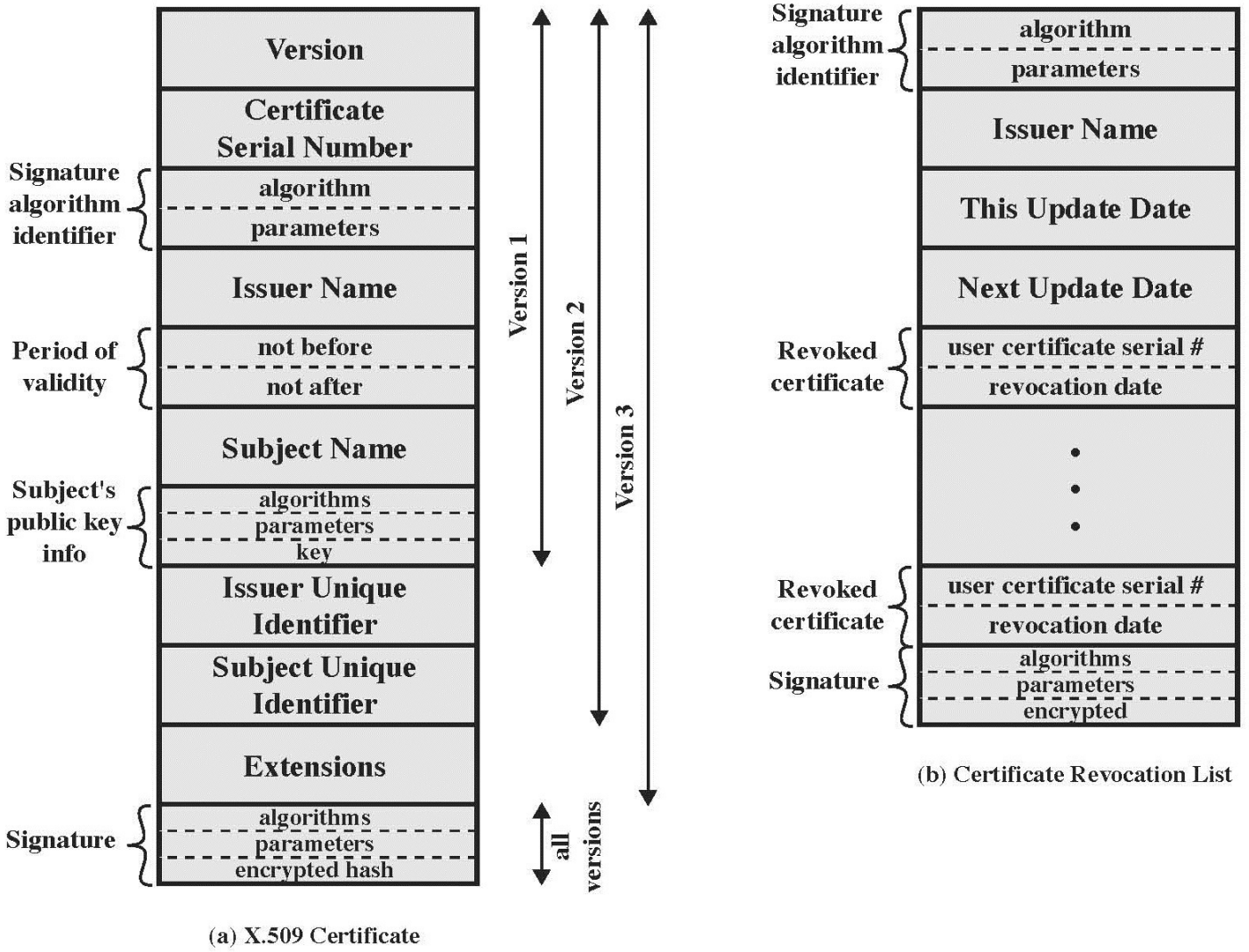
(a) Obtaining certificates from CA



(b) Exchanging certificates

Figure 14.13 Exchange of Public-Key Certificates

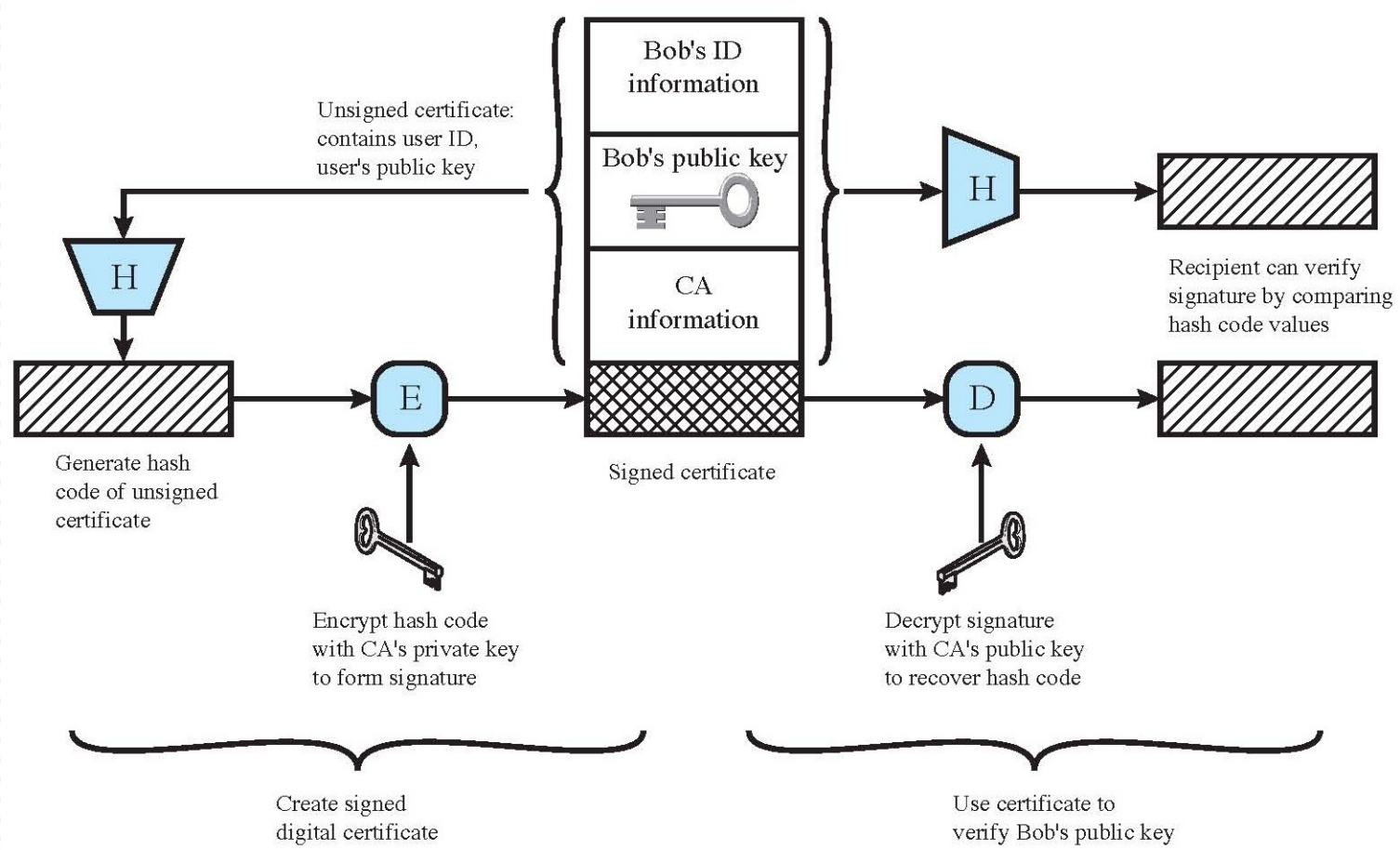
X.509 Certificate



Certificate Extensions

- Key and policy information
  - convey info about subject & issuer keys, plus indicators of certificate policy
- Certificate subject and issuer attributes
  - support alternative names, in alternative formats for certificate subject and/or issuer
- Certificate path constraints
  - allow constraints on use of certificates by other CA's

X.509 Certificate Use



Certificate Revocation

- Certificates have a period of validity
- May need to revoke before expiry, e.g.:
  - user's private key is compromised
  - user is no longer certified by this CA
  - CA's certificate is compromised
- CA’s maintain list of revoked certificates
  - the Certificate Revocation List (CRL)
- Users should check certificates with CA’s CRL

Public Key Infrastructure