Key distribution

Key distribution, symmetric encryption

From requirements for symmetric encryption:

“Sender and receiver must *have obtained copies of the secret key* in a secure way and must keep the key secure”

- **Important issue**: how to distribute secret keys?

Key distribution, manual delivery

For two parties A and B:

- A key could be created by A and delivered physically to B (or vice versa);
- A key could be created by the third trusted party C and delivered physically to A and B;

Difficult to use in wide area distributed systems, when dynamic connections are needed.

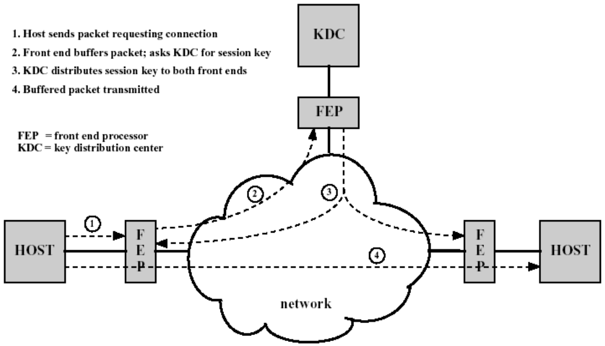
Key distribution, further techniques

- If A and B have used recently a secret key, one of them could create a new secret key and send it to the partner using old key;

  Potential problem: once an attacker learned one key, he can disclose all keys afterwards

- There is a third trusted party C connected by encrypted channels with both A and B. Then C creates a key and distributes it among A and B using encrypted channels;

Automated key distribution



Distribution of public keys

- **Simple approach**: a user sends the key to any other user, or broadcasts key to the group of users;
- **The problem**: possible forgery. A user **A** could pretend to be a user **B** and distribute his key as the key of **B;**
- **Solution:** public-key certificate issued by the trusted third party, certificate authority.

Public key certificate

- PK certificate:
  - Public key of a User + User ID
  - Everything is signed by certificate authority (CA)
- A user presents his public key to the authority in a secure manners and obtains the certificate.
- Then user can publish the certificate;
- Everyone then can obtain the certificate and verify the public key;
- Verification is based on the trust to CA!

Public-key certificate