# Key Distribution

Yih-Kuen Tsay

Department of Information Management
National Taiwan University

# The Key Distribution Problem

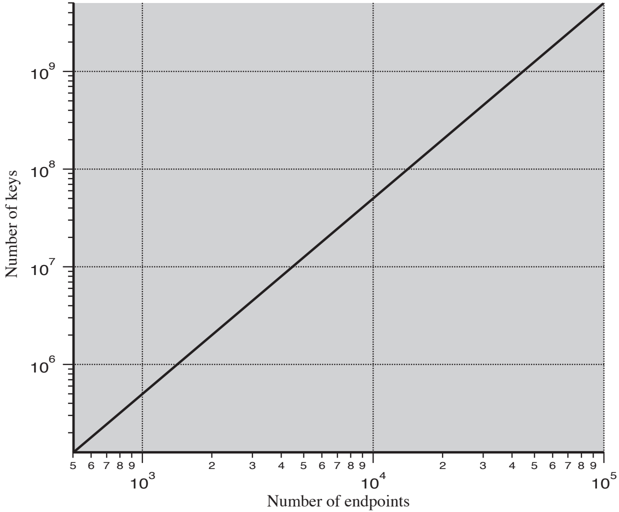
- For symmetric encryption to work, the two parties of an exchange must share the same key and that key must be protected.
- Frequent key changes may be desirable to limit the amount of data compromised.
- The strength of a cryptographic system rests with the technique for solving the key distribution problem—delivering a key to the two parties of an exchange.
- The scale of the problem depends on the number of communication pairs.

# Approaches to Key Distribution

Let A (Alice) and B (Bob) be the two parties.

- A key can be selected by A and physically delivered to B.
- A third party can select the key and physically deliver it to A and B.
- If A and B have previously and recently used a key, one party can transmit the new key to the other, encrypted using the old key.
- If A and B each has an encrypted connection to a third party C, C can deliver a key on the encrypted links to A and B.

# Number of Keys for Endpoints

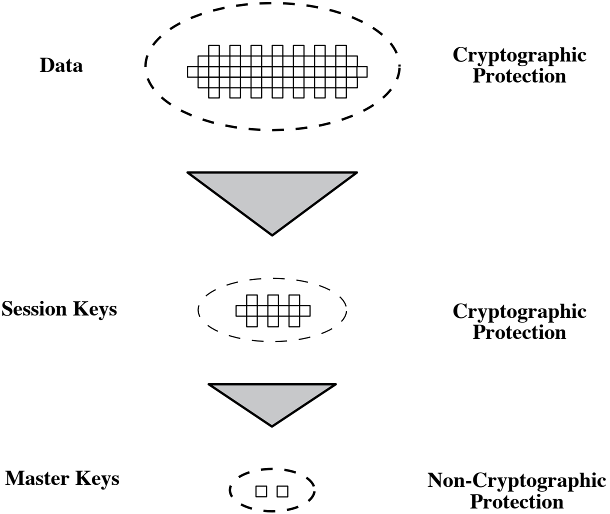


Source: Figure 14.1, Stallings 2010

# Using a Key Distribution Center

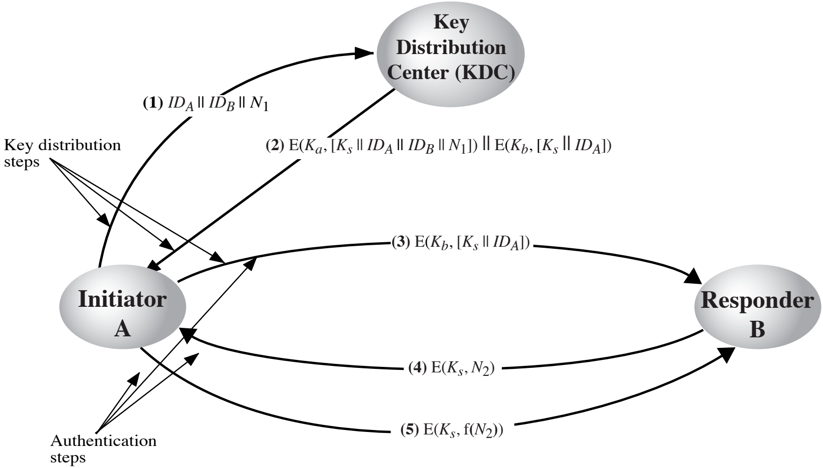
- A key distribution center is responsible for distributing keys to pairs of users as needed.
- Each user must share a unique key with the key distribution center for purposes of key distribution.
- At least two levels of keys must be used: session keys and master keys.
- If there are $N$ end users, $N(N-1)/2$ session keys are needed at any one time, but only $N$ master keys are required.

# Key Hierarchy



Source: Figure 14.2, Stallings 2010

# Key Distribution Scenario


Key Distribution Center (KDC)
(1) $ID_A \| ID_B \| N_1$
Key distribution steps
(2) $E(K_a, [K_s \| ID_A \| ID_B \| N_1]) \| E(K_b, [K_s \| ID_A])$
(3) $E(K_b, [K_s \| ID_A])$
Initiator A
Responder B
(4) $E(K_s, N_2)$
(5) $E(K_s, f(N_2))$
Authentication steps

Source: Figure 14.3, Stallings 2010

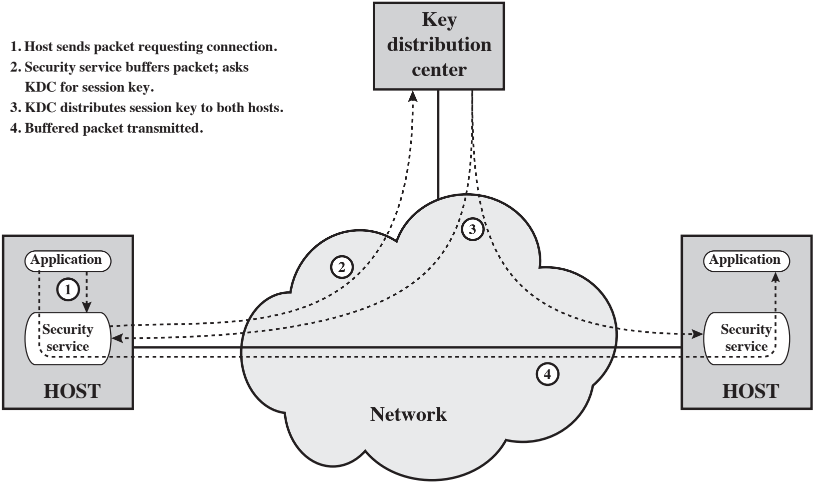
# Hierarchical Key Control

- For large networks, a single KDC is inadequate.
- In a hierarchy of KDCs, each local KDC is responsible for a small domain.
- If the two parties are within the same local domain, their KDC is responsible for key distribution.
- Otherwise, the two corresponding local KDCs can communicate through a global KDC. Any of the three KDCs involved can select the key.
- Advantages: distributing the effort of master key distribution and isolating the damage of a fault.

# Session Key Lifetime

- Two competing considerations in determining the lifetime of a session key:
    - The more frequently session keys are changed, the more secure they are.
    - The distribution of session keys delays the start of an exchange and places a burden on network capacity.
- The decision can be based on whether the communication protocol is connection-oriented or connectionless.

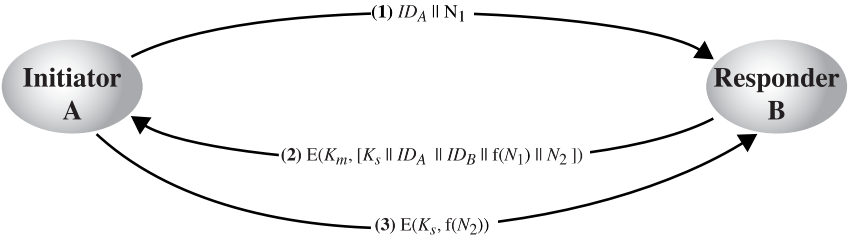
# Automatic Key Distribution



1. Host sends packet requesting connection.
2. Security service buffers packet; asks KDC for session key.
3. KDC distributes session key to both hosts.
4. Buffered packet transmitted.

Source: Figure 14.4, Stallings 2010

# Decentralized Key Distribution



Source: Figure 14.5, Stallings 2010

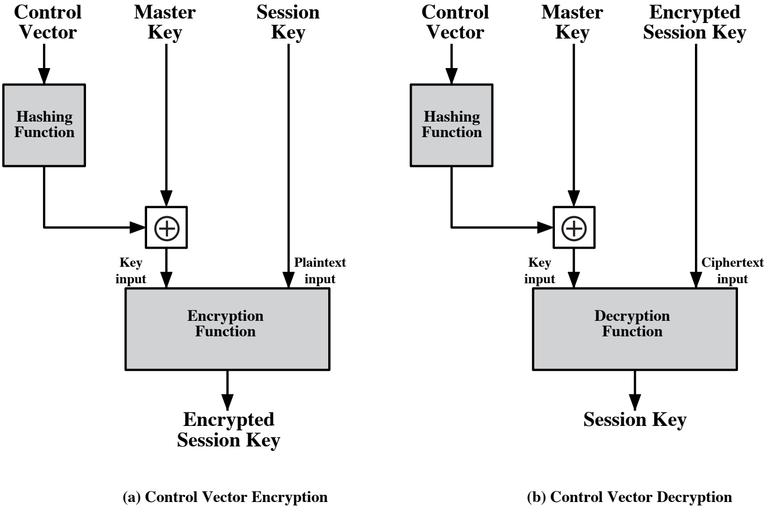
# Decentralized Key Control

- The KDC must be trusted and be protected from subversion.
- This requirement can be avoided if the key distribution is fully decentralized.
- A fully decentralized key control, though not feasible for large networks, may be useful within a local context.
- A decentralized approach requires that each end system be able to communicate in a secure manner with all potential partner end systems for purposes of session key distribution.

# Controlling Key Usage

- It may be desirable to impose some control on the way in which automatically distributed keys are used.
- Possible types of session keys include: data-encrypting key, PIN-encrypting key, file-encrypting key, etc.
- Key use controlling schemes:
    - Tags
    - Control vectors

# Control Vector



Source: Figure 14.6, Stallings 2010