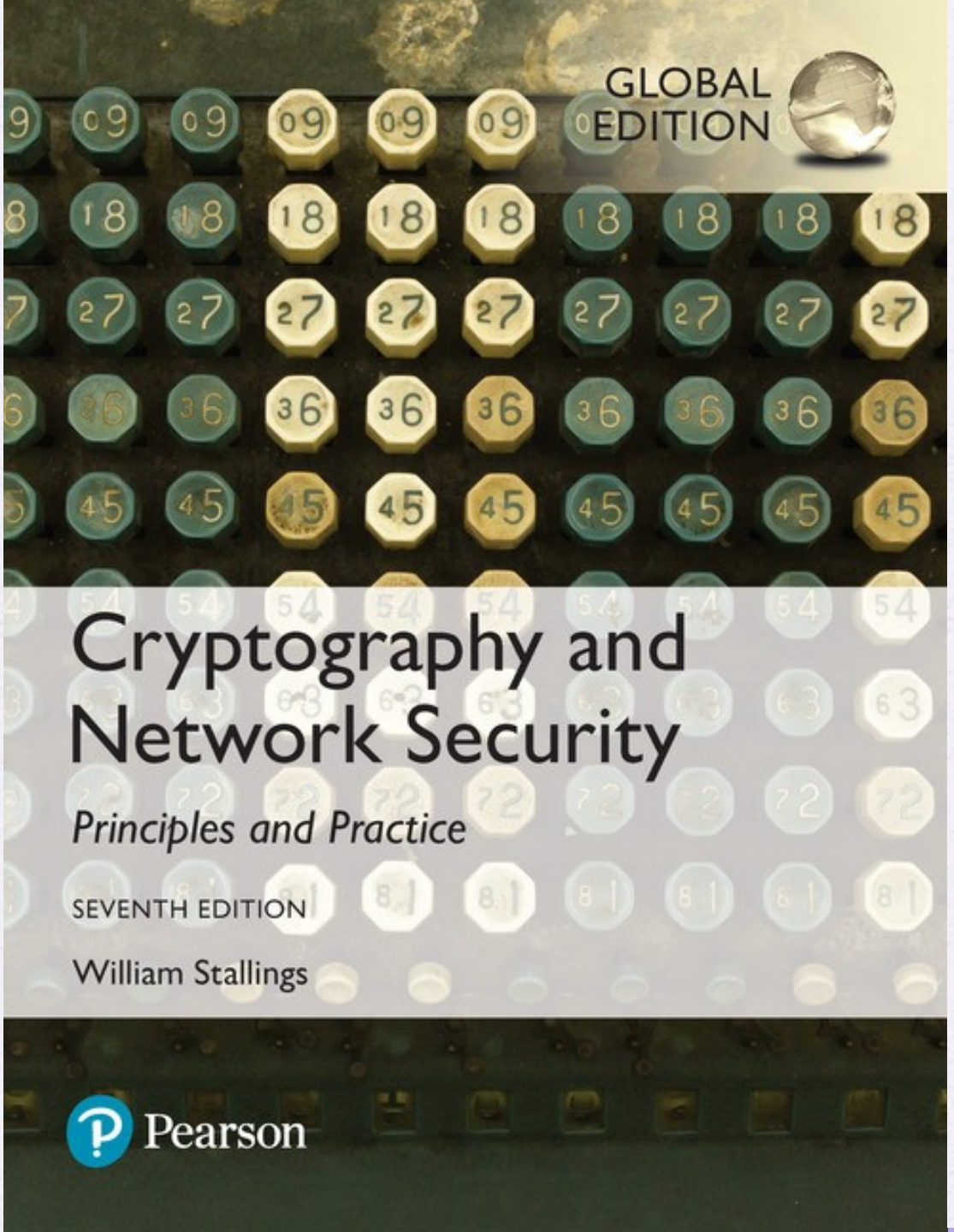
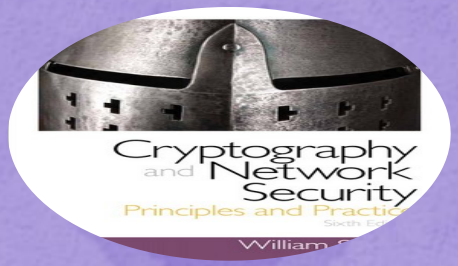

GLOBAL EDITION
Cryptography and Network Security
Principles and Practice
SEVENTH EDITION
William Stallings
Pearson



Chapter 14

Key Management and Distribution

Key Distribution Technique

- Term that refers to the means of delivering a key to two parties who wish to exchange data without allowing others to see the key
- For symmetric encryption to work, the two parties to an exchange must share the same key, and that key must be protected from access by others
- Frequent key changes are desirable to limit the amount of data compromised if an attacker learns the key

Symmetric Key Distribution

Given parties A and B, key distribution can be achieved in a number of ways:

- **A can select a key and physically ver it to B**
- **party can select the key ically deliver it to A and**
- **have previously and ed a key, one party it the new key to the rypted using the old**
- **B each has an encrypted tion to a third party C, C deliver a key on the encrypted links to A and B**

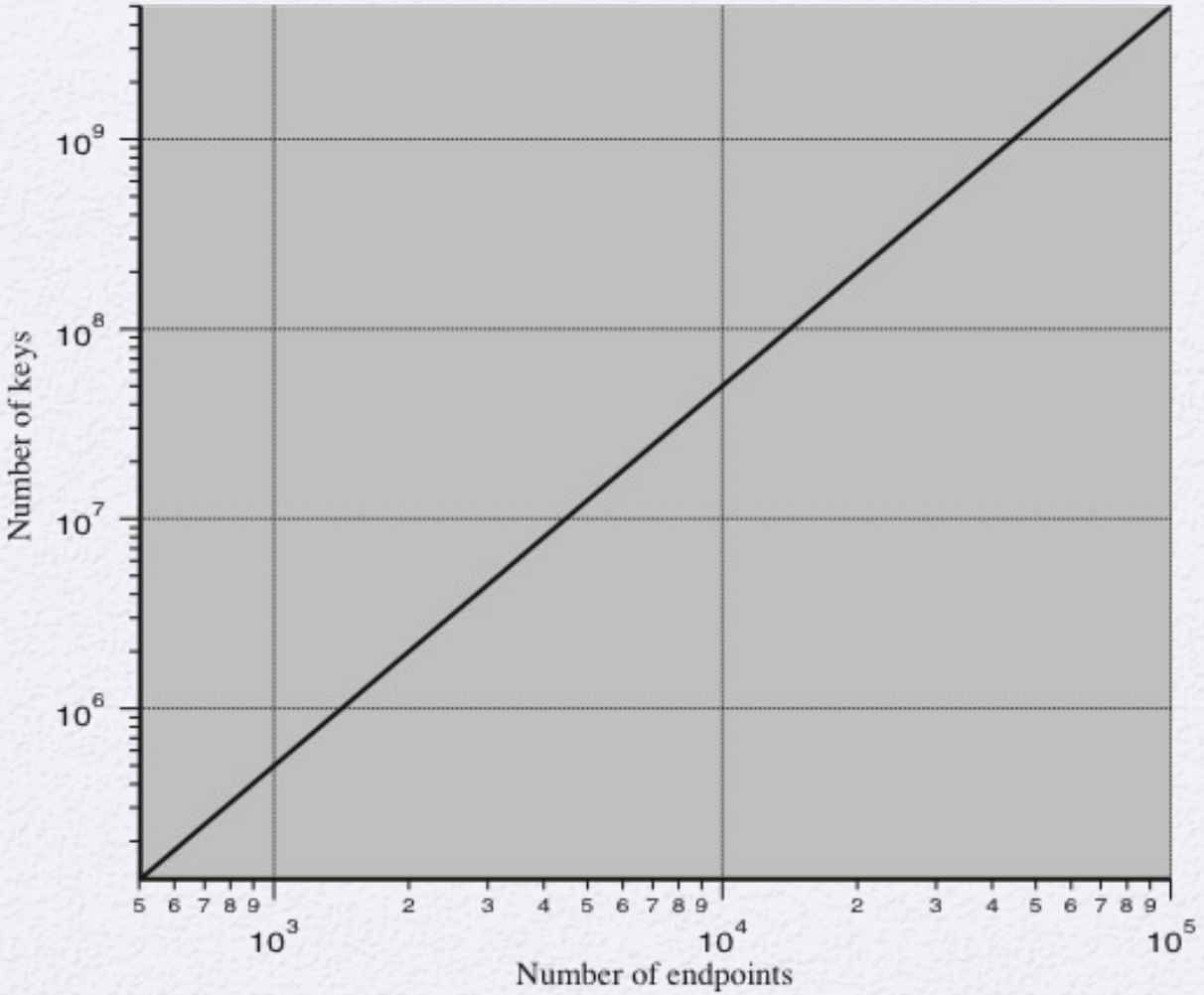


Figure 14.1 Number of Keys Required to Support Arbitrary Connections Between Endpoints

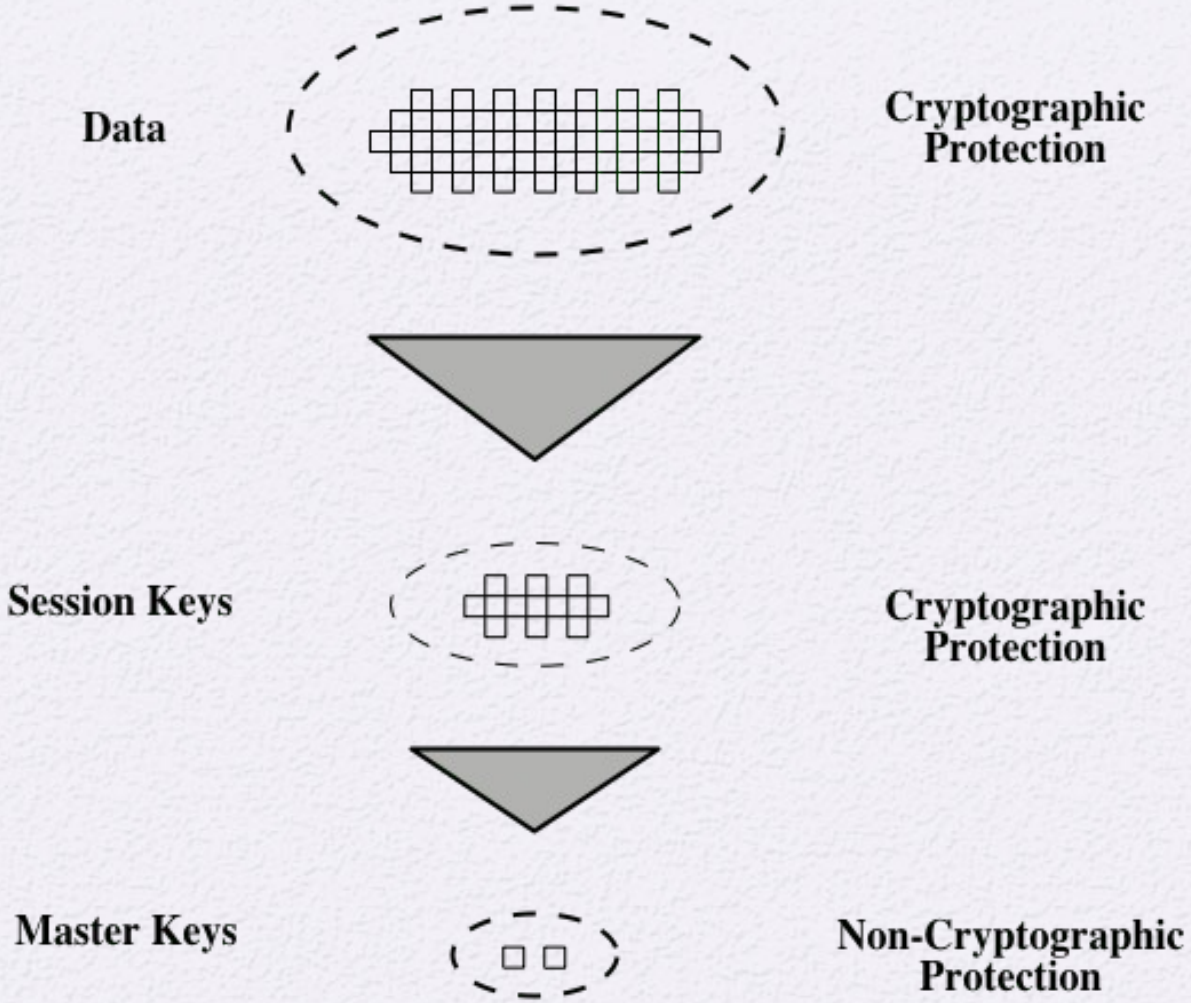


Figure 14.2 The Use of a Key Hierarchy

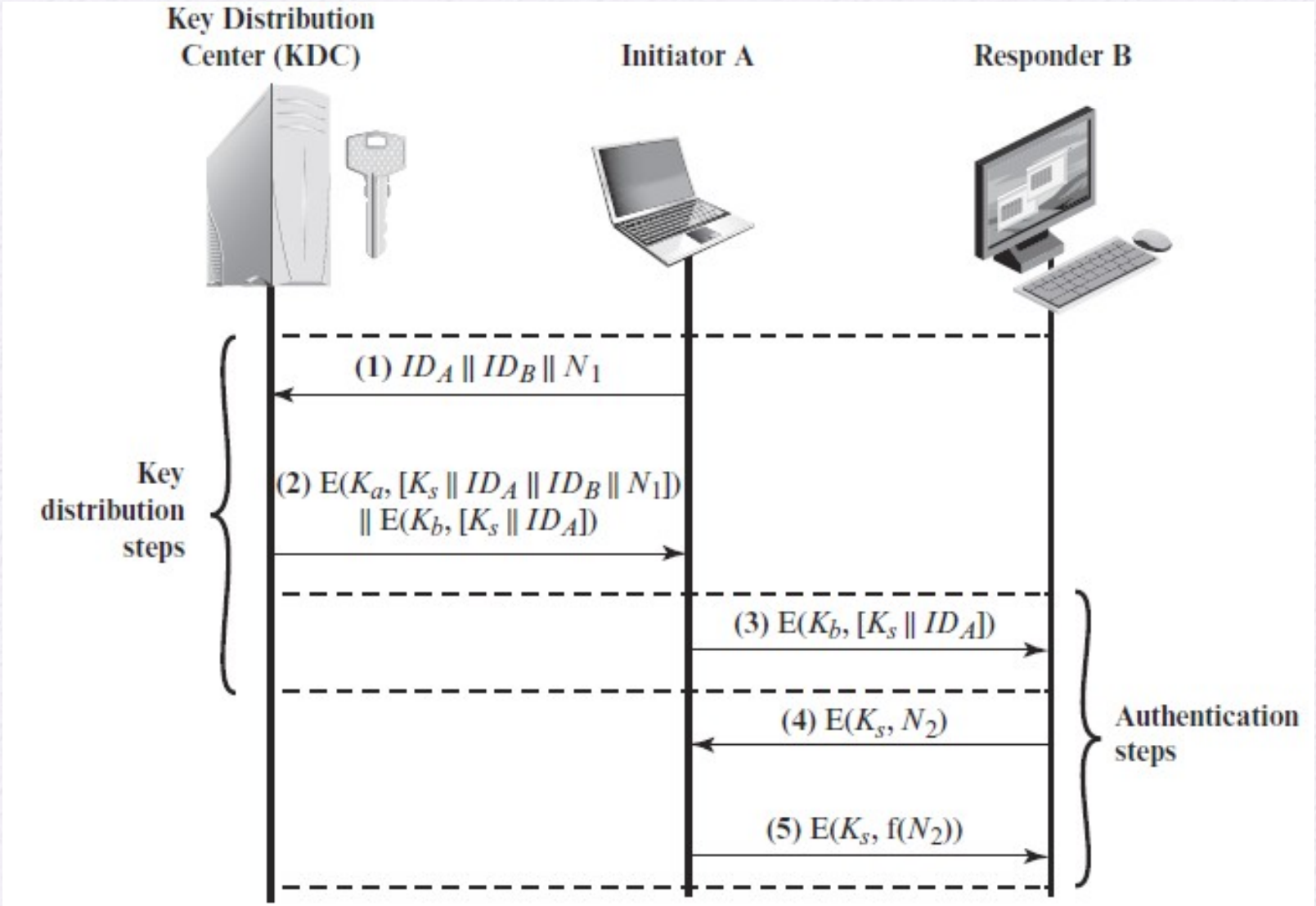
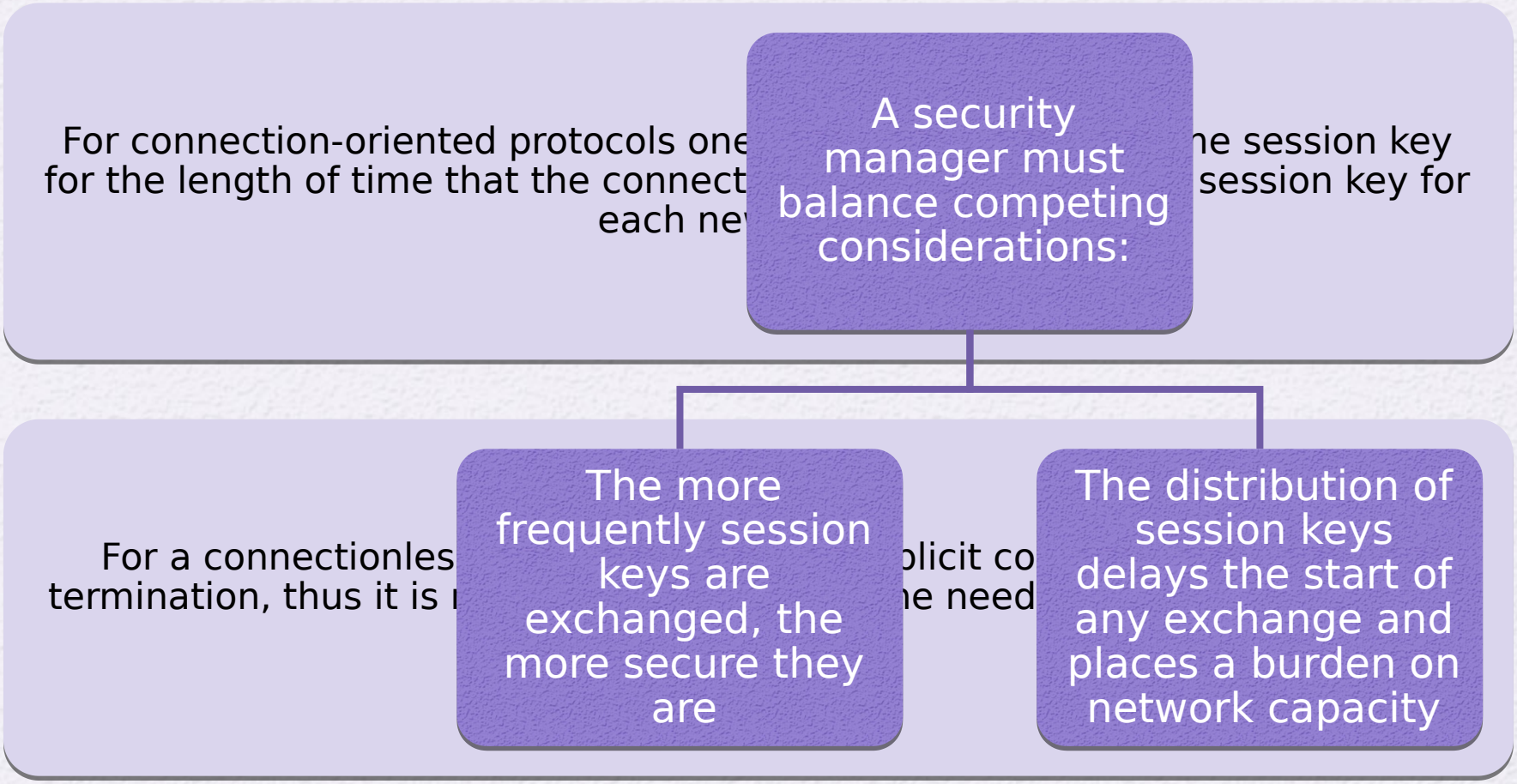


Figure 14.3 Key Distribution Scenario

Hierarchical Key Control

- For communication among entities within the same local domain, the local KDC is responsible for key distribution
  - If two entities in different domains desire a shared key, then the corresponding local KDC's can communicate through a global KDC
- The hierarchical concept can be extended to three or more layers
- Scheme minimizes the effort involved in master key distribution because most master keys are those shared by a local KDC with its local entities
  - Limits the range of a faulty or subverted KDC to its local area only

Session Key Lifetime



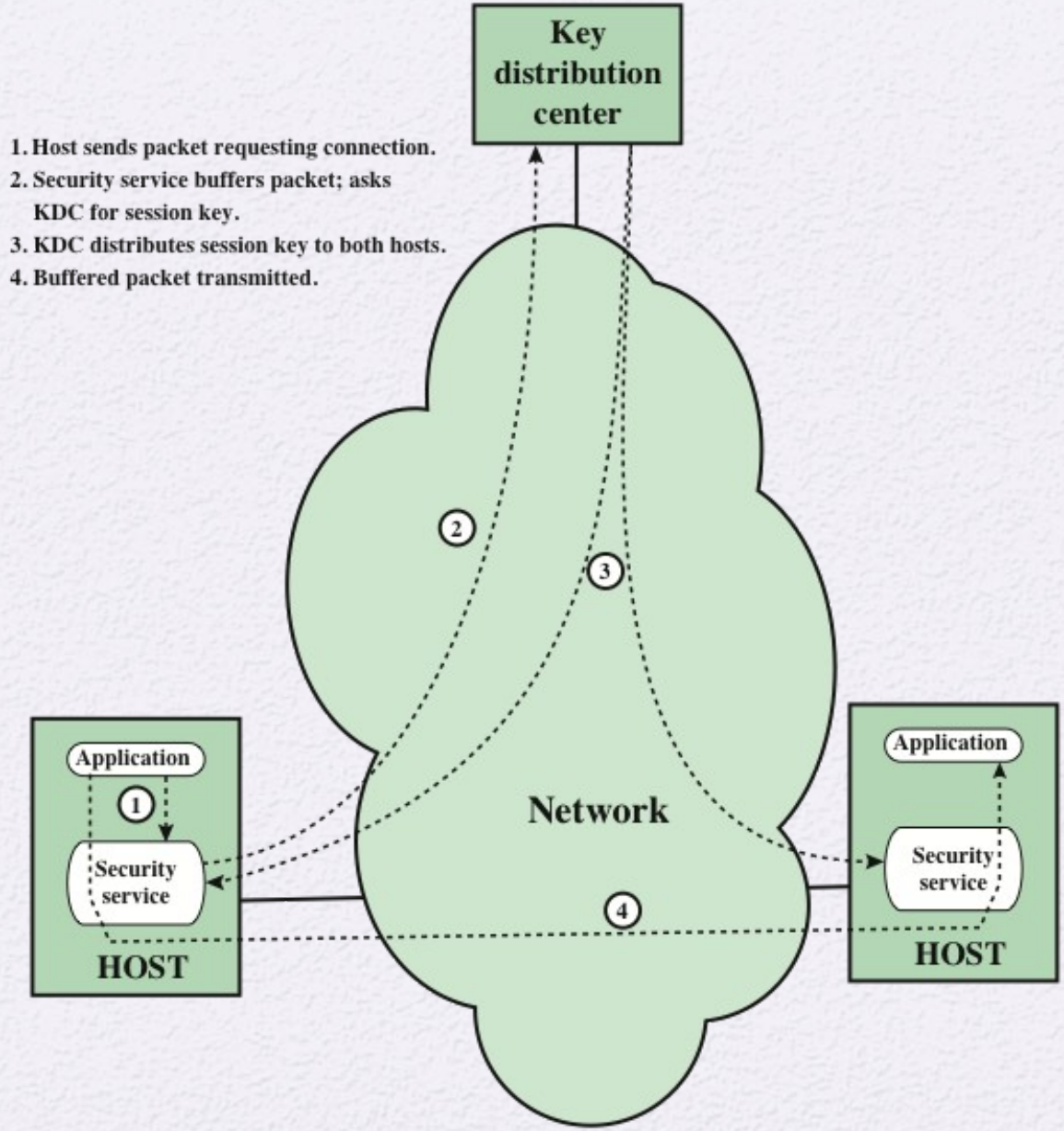


Figure 14.4 Automatic Key Distribution for Connection-Oriented Protocol

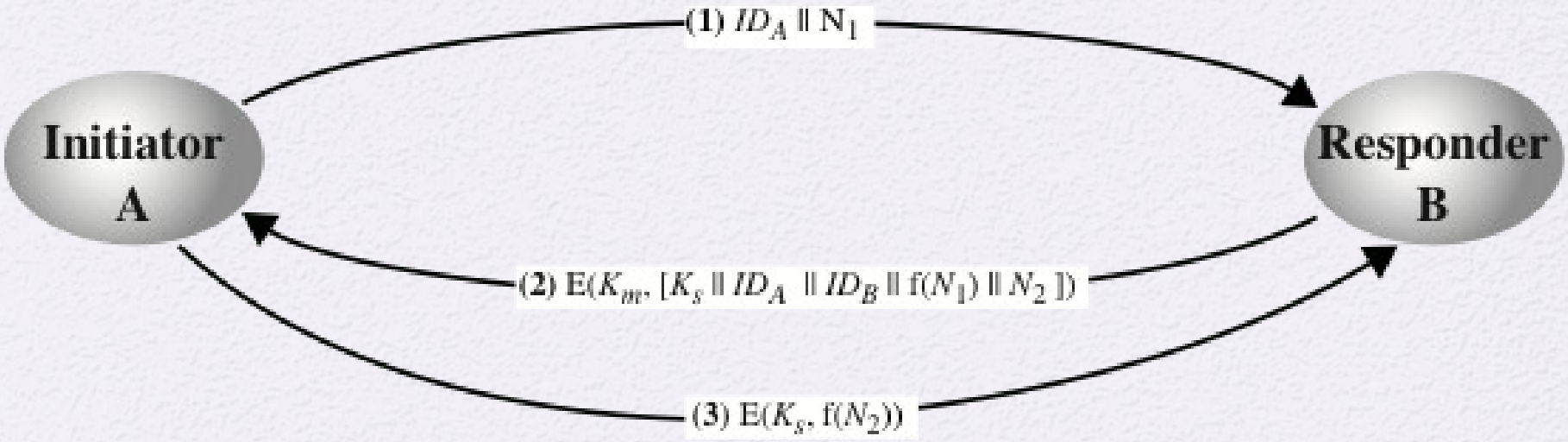


Figure 14.5 Decentralized Key Distribution

Controlling Key Usage

- The concept of a key hierarchy and the use of automated key distribution techniques greatly reduce the number of keys that must be manually managed and distributed
- It also may be desirable to impose some control on the way in which automatically distributed keys are used
  - For example, in addition to separating master keys from session keys, we may wish to define different types of session keys on the basis of use

Key Controls

- Associate a tag with each key
  - For use with DES and makes use of the extra 8 bits in each 64-bit DES key
  - The eight non-key bits ordinarily reserved for parity checking form the key tag
  - Because the tag is embedded in the key, it is encrypted along with the key when that key is distributed, thus providing protection

Drawbacks:

- The tag length is limited to 8 bits, limiting its flexibility and functionality
- Because the tag is not transmitted in clear form, it can be used only at the point of decryption, limiting the ways in which key use can be controlled

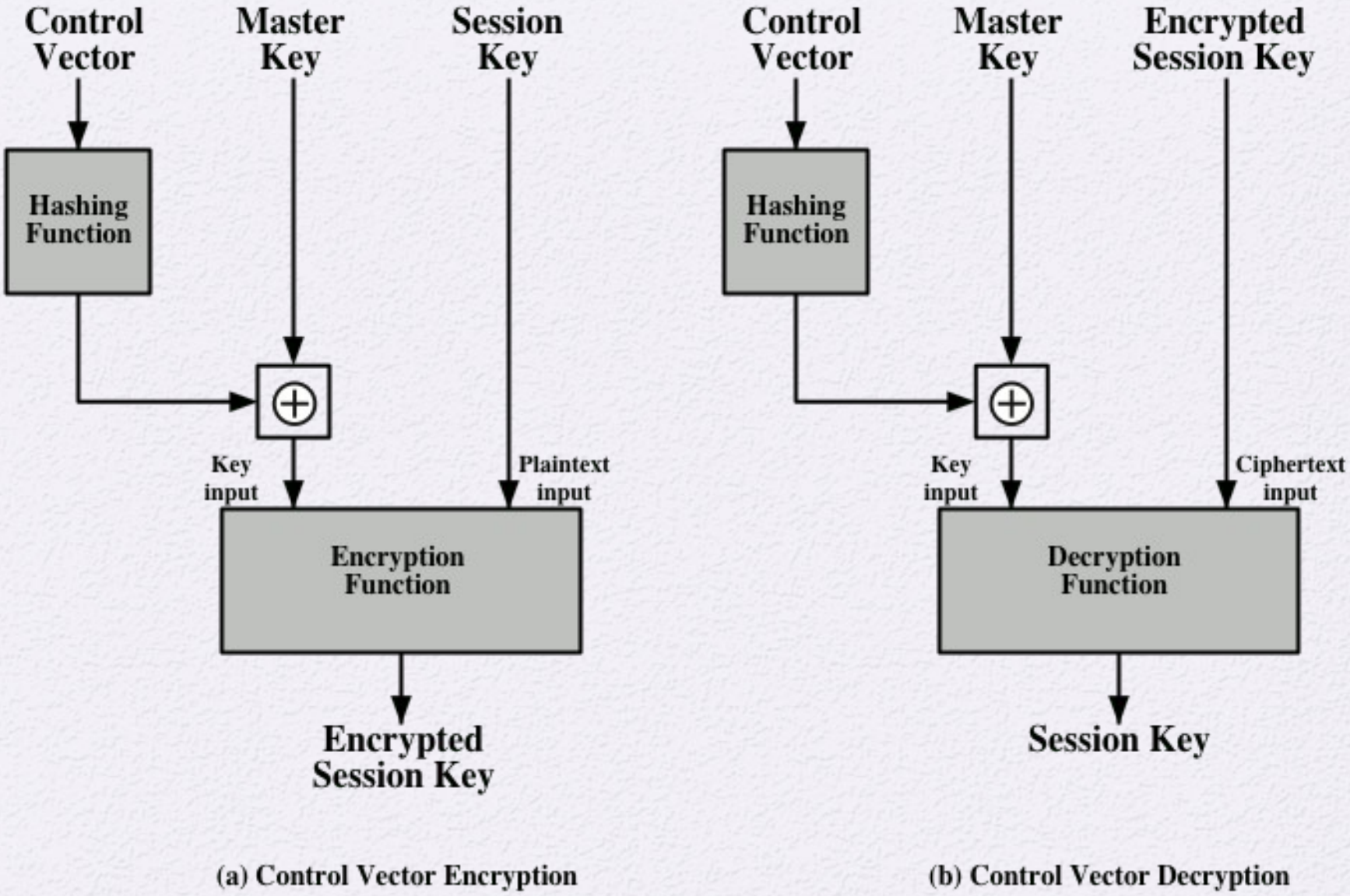


Figure 14.6 Control Vector Encryption and Decryption

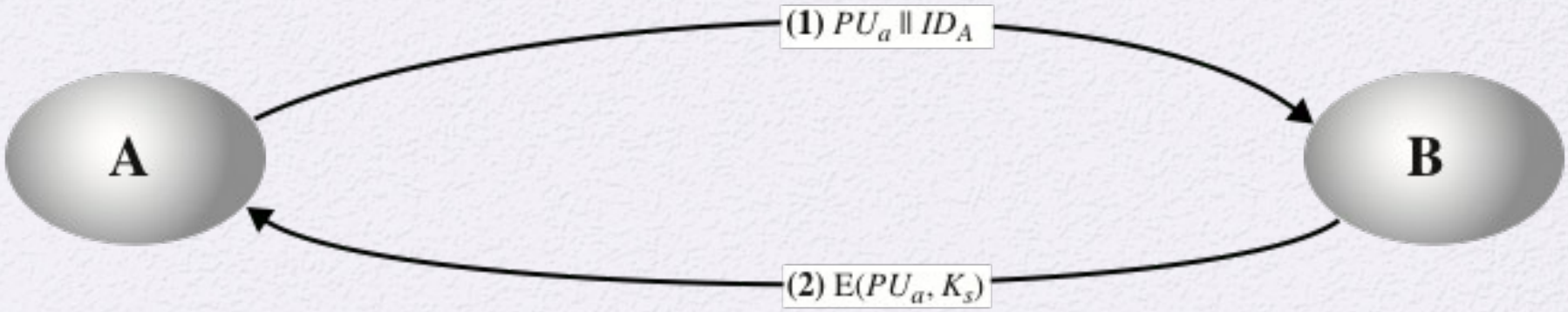


Figure 14.7 Simple Use of Public-Key Encryption to Establish a Session Key

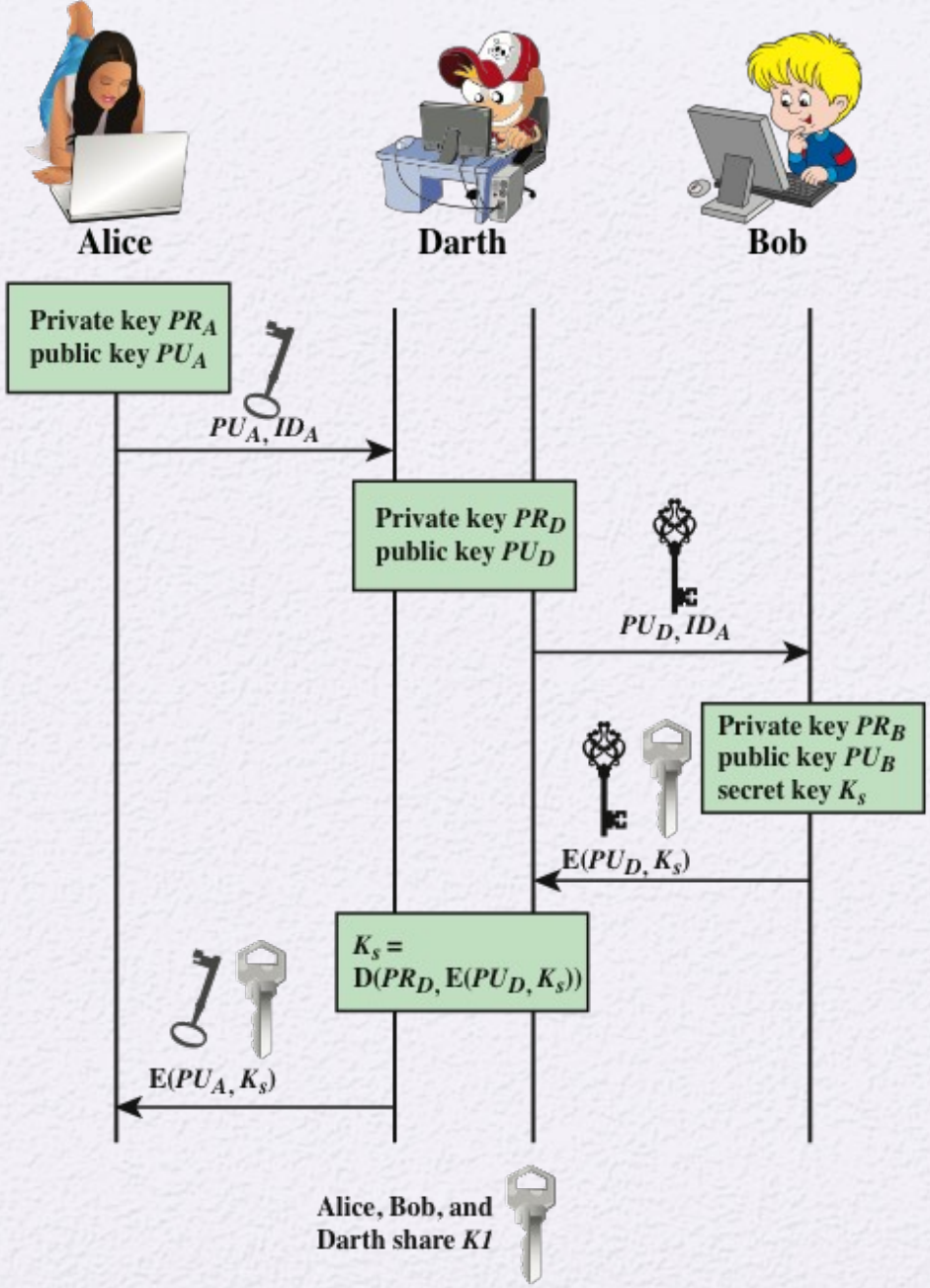


Figure 14.8 Another Man-in-the-Middle Attack

Confidentiality and Authentication

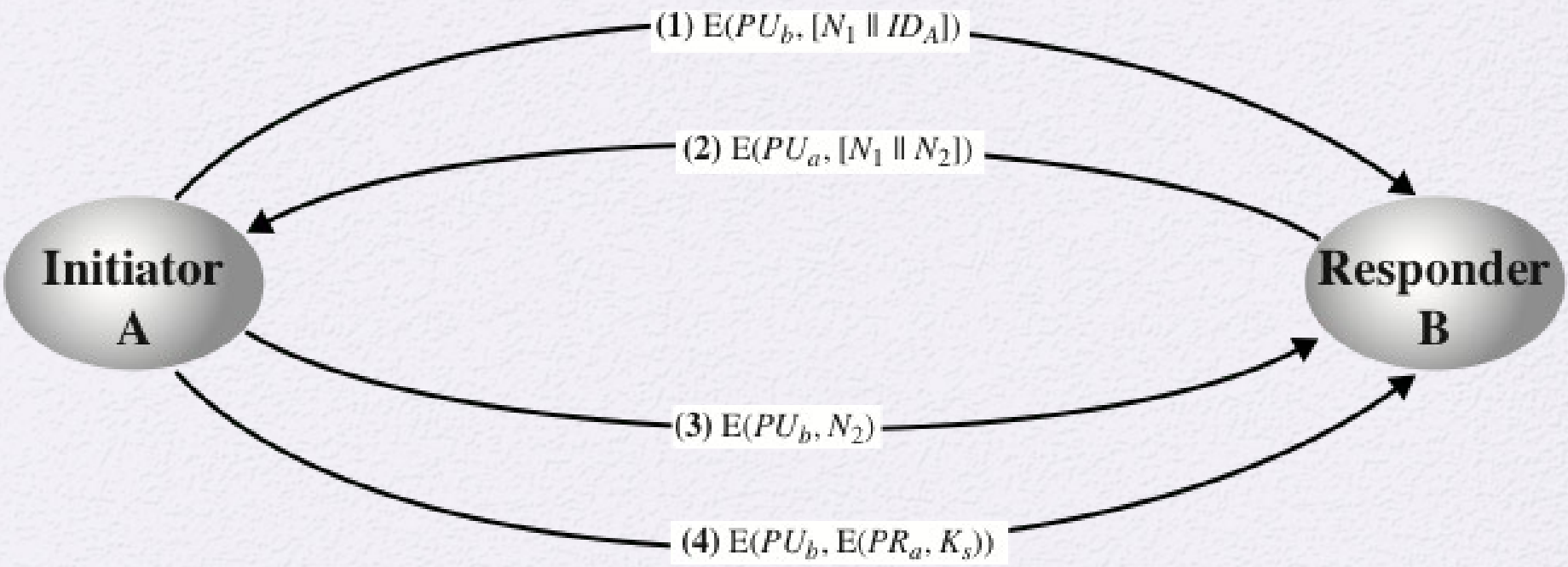


Figure 14.9 Public-Key Distribution of Secret Keys

A Hybrid Scheme

- In use on IBM mainframes
- Retains the use of a key distribution center (KDC) that shares a secret master key with each user and distributes secret session keys encrypted with the master key
- A public-key scheme is used to distribute the master keys

Rationale:

- Performance
- Backward compatibility

Distribution of Public Keys

- Several techniques have been proposed for the distribution of public keys. Virtually all these proposals can be grouped into the following general schemes:

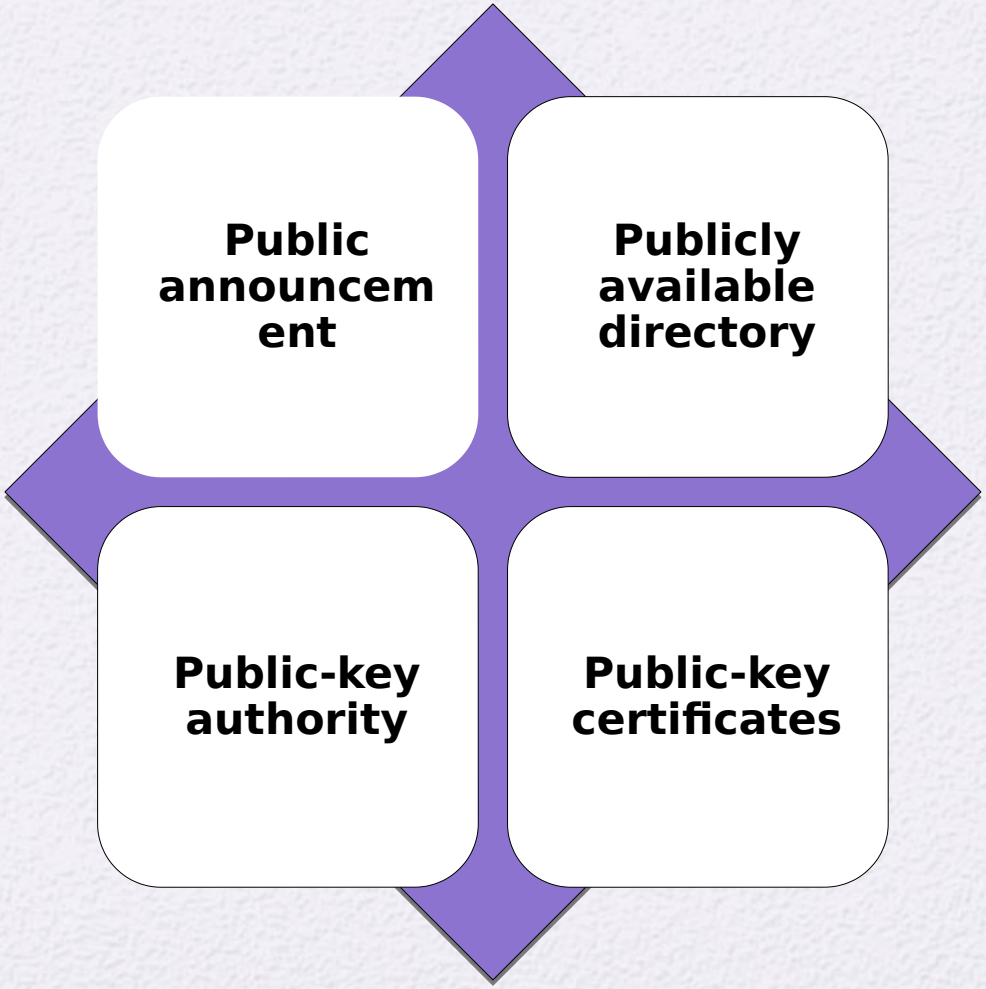


Figure 14.10 Uncontrolled Public Key Distribution

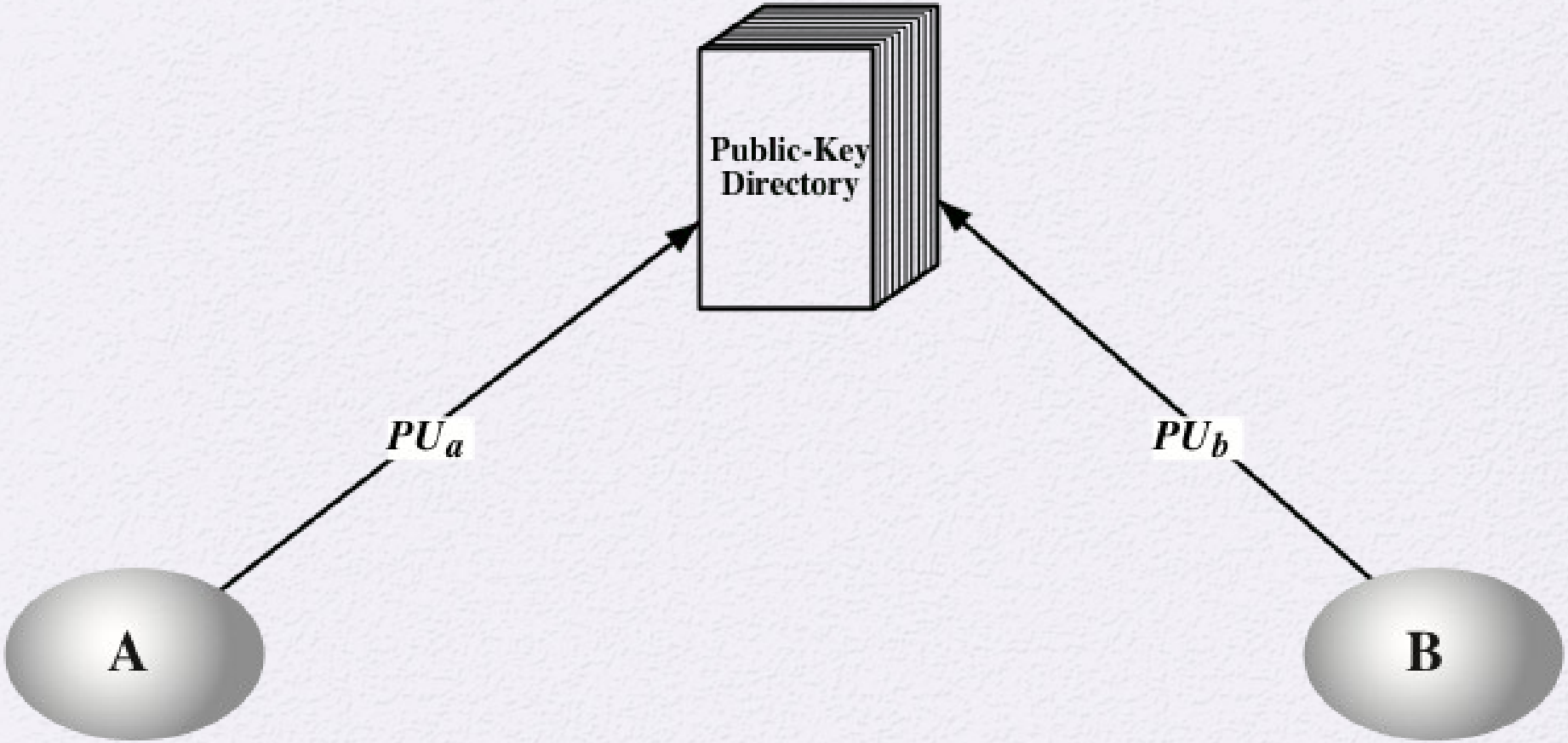


Figure 14.11 Public Key Publication

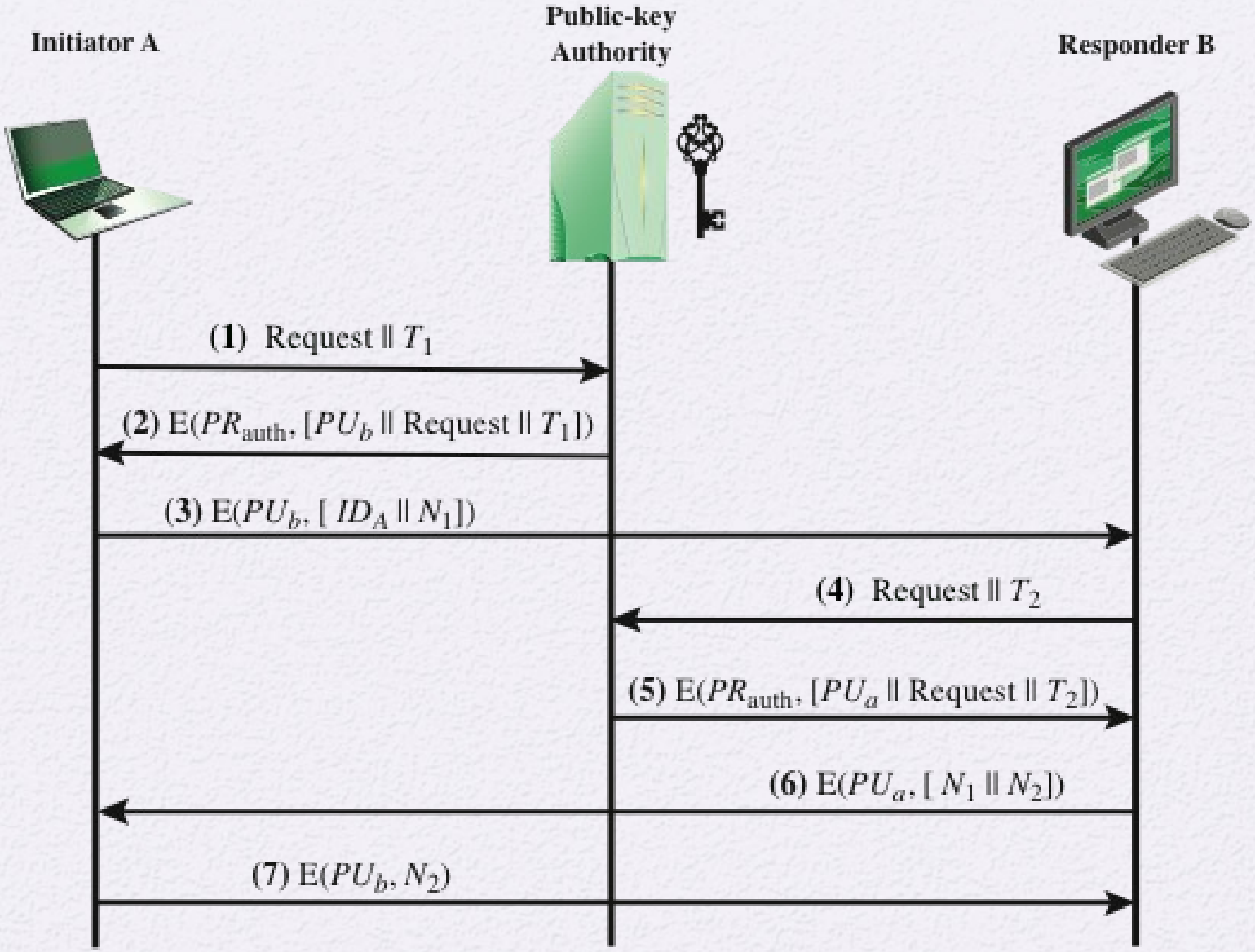


Figure 14.12 Public-Key Distribution Scenario

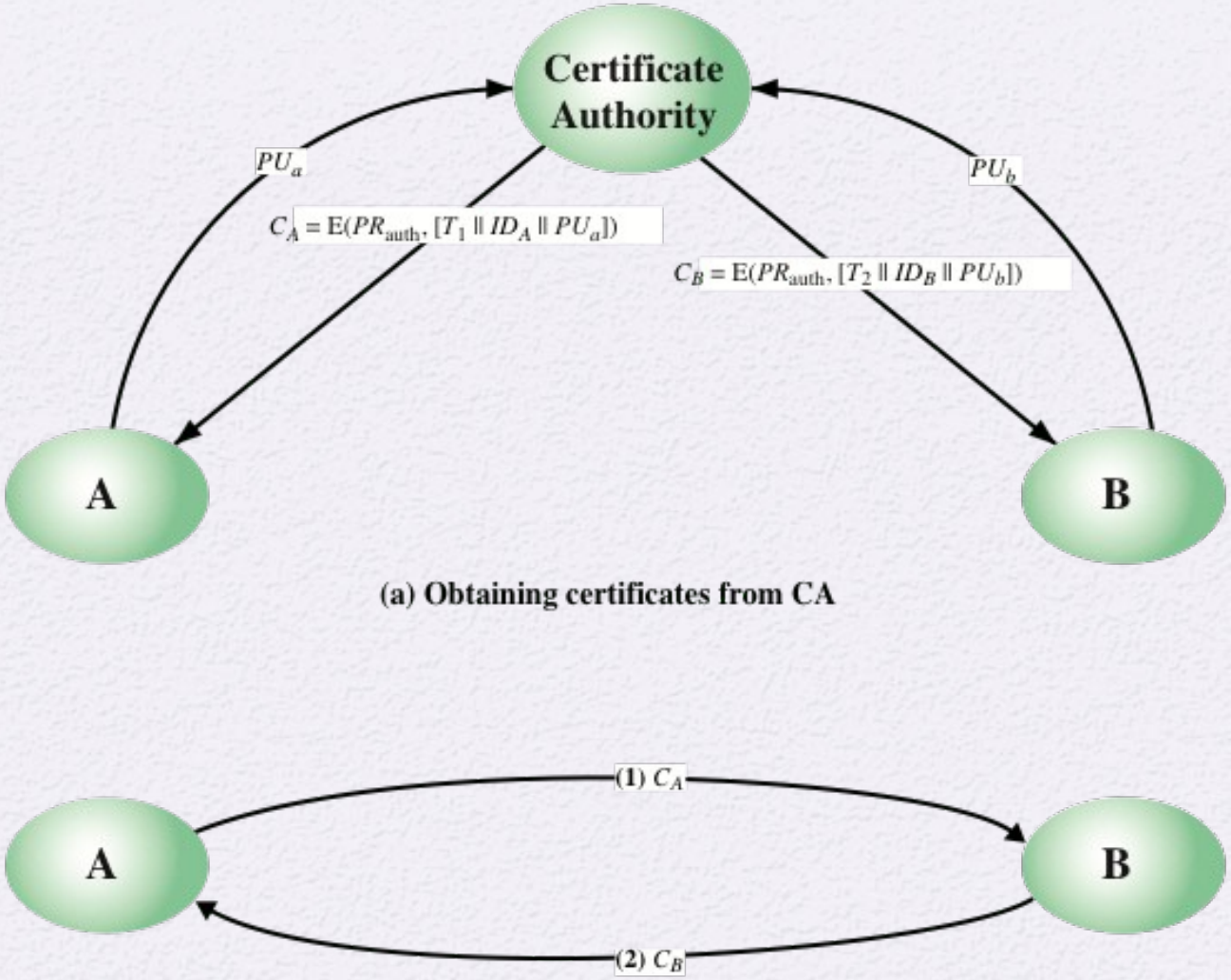
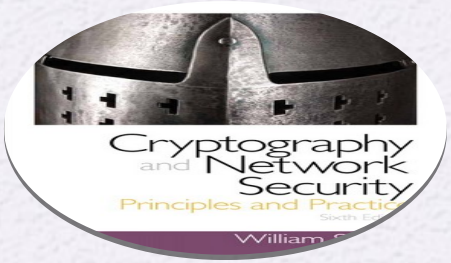


Figure 14.13 Exchange of Public-Key Certificates

Summary

- Symmetric key distribution using symmetric encryption
  - Key distribution scenario
  - Hierarchical key control
  - Session key lifetime
  - Transparent key control scheme
  - Decentralized key control
  - Controlling key usage
- Symmetric key distribution using asymmetric encryption
  - Simple secret key distribution
  - Secret key distribution with confidentiality and authentication
  - Hybrid scheme



- Distribution of public keys
  - Public announcement of public keys
  - Publicly available directory
  - Public-key authority
  - Public-key certificates