

GLOBAL
EDITION



Cryptography and Network Security

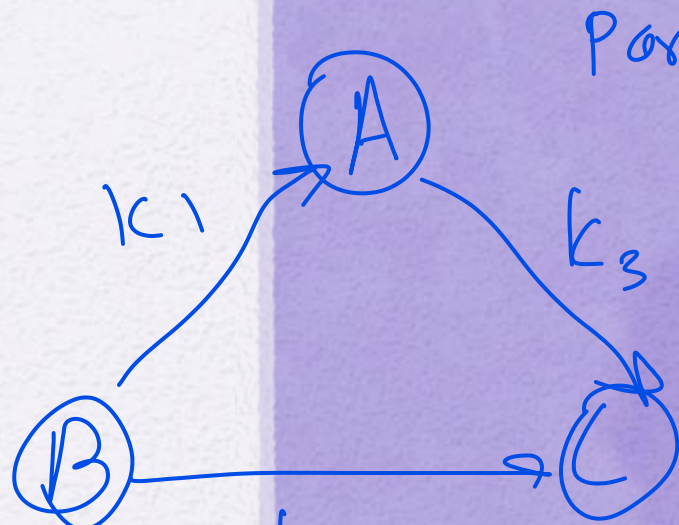
Principles and Practice

SEVENTH EDITION

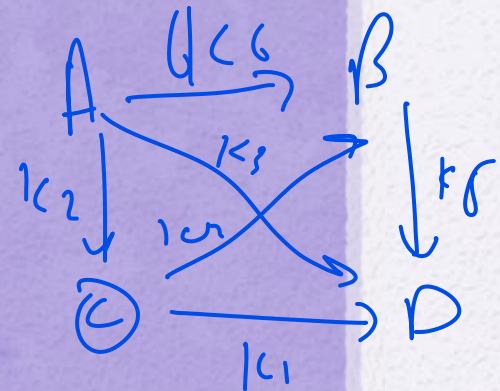
William Stallings



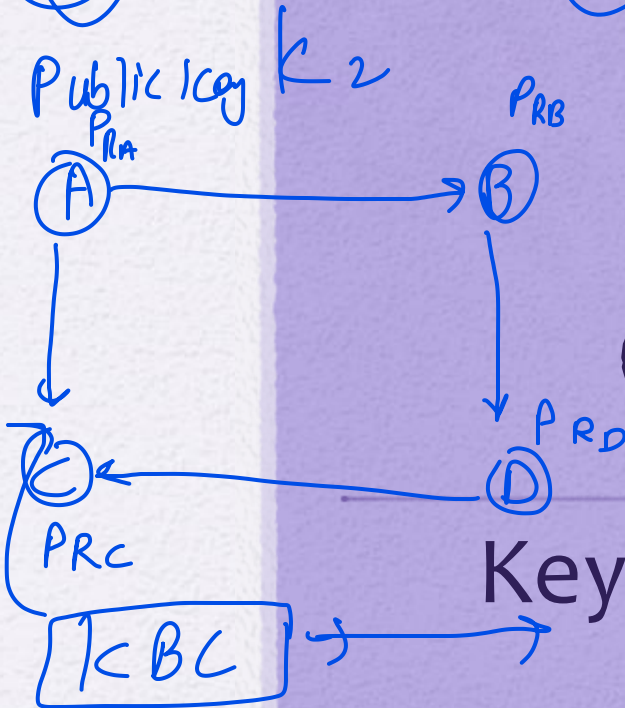
Pearson



Parties common
Key=3



Key=6



$$n = \frac{n(n-1)}{2}$$

Number of key

Chapter 14

Key Management and Distribution

$$\frac{5 \times 4}{2} = 10$$

$$N = 100 \quad \text{key } p = 100$$

$$\text{key}_s = \frac{100 \times 99}{2} = 4950$$

Check both key
Required in
Symmetric and
asymmetric

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

Session keys
 ↳ Session in web
 ↳ available for specific time

for example
 1 key is used
 for one day,

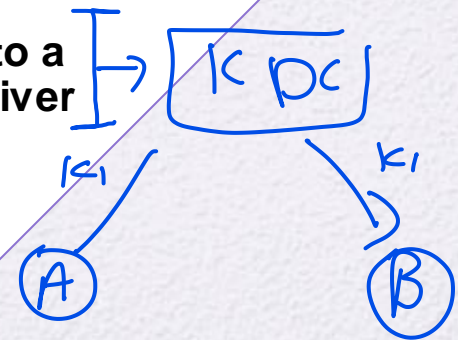
Symmetric Key Distribution

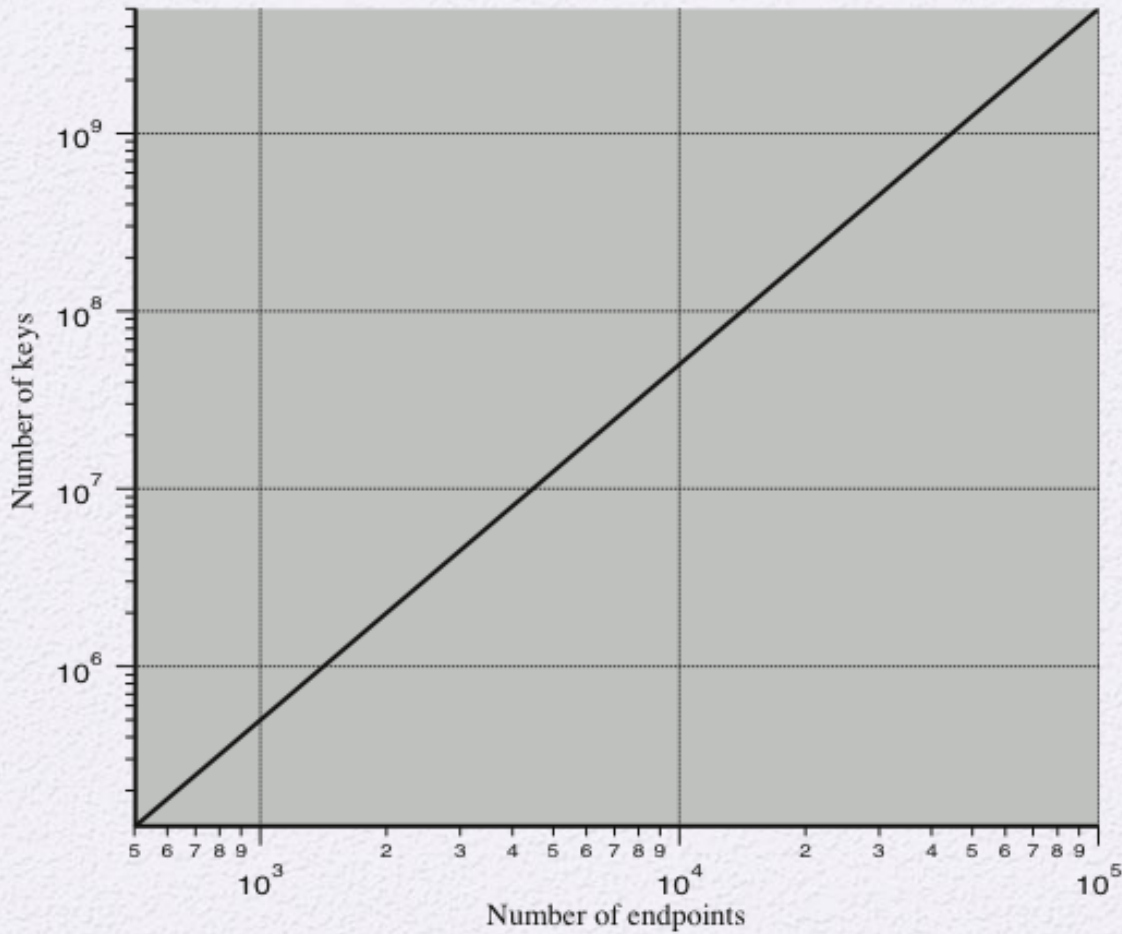
A k_1 B
Session expired
 $A^{k_2} \xrightarrow{E(k_1, k_2)} B$

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

- A can select a key and physically deliver it 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

No third party:





$$\frac{n(n-1)}{2}$$

host

↳ Node;

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

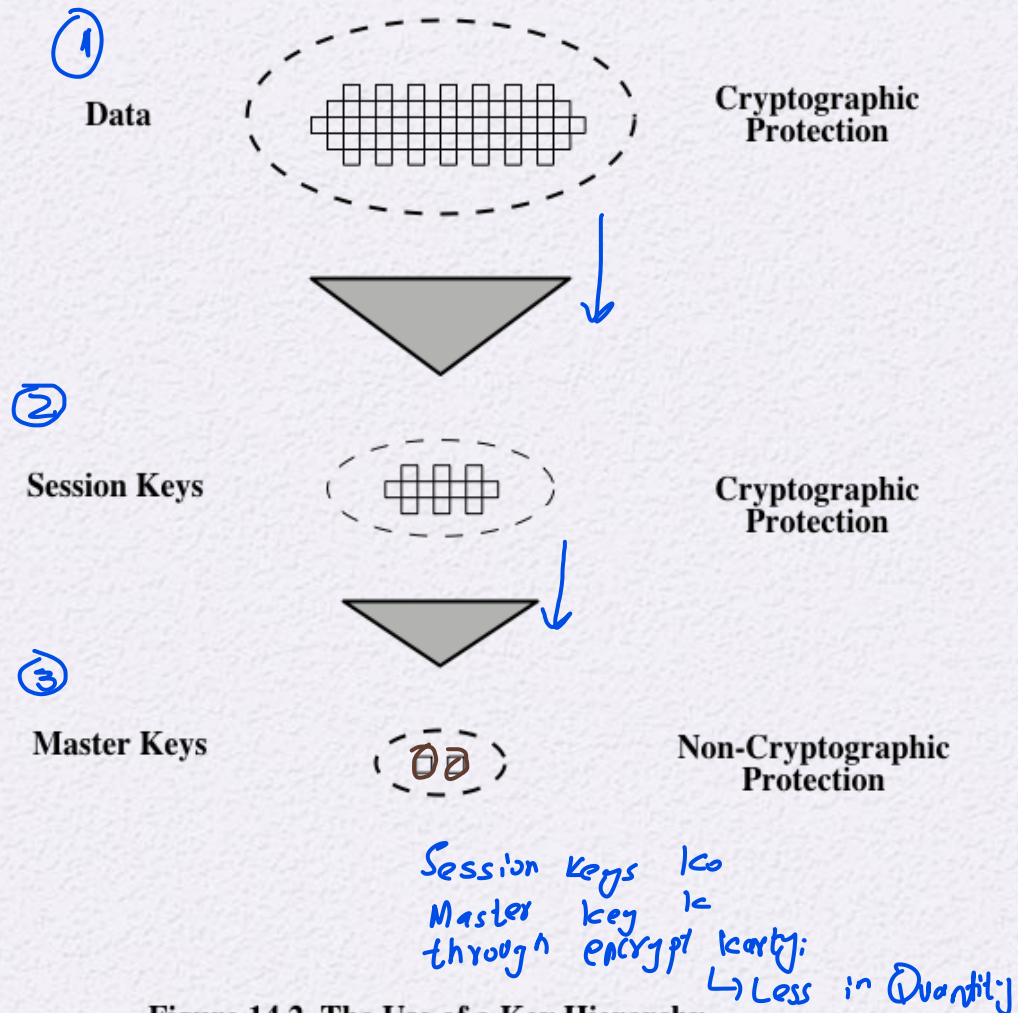


Figure 14.2 The Use of a Key Hierarchy

When Session over the
Some process again
do the same functions
→ This is Actually
handshake
between 2
Parties

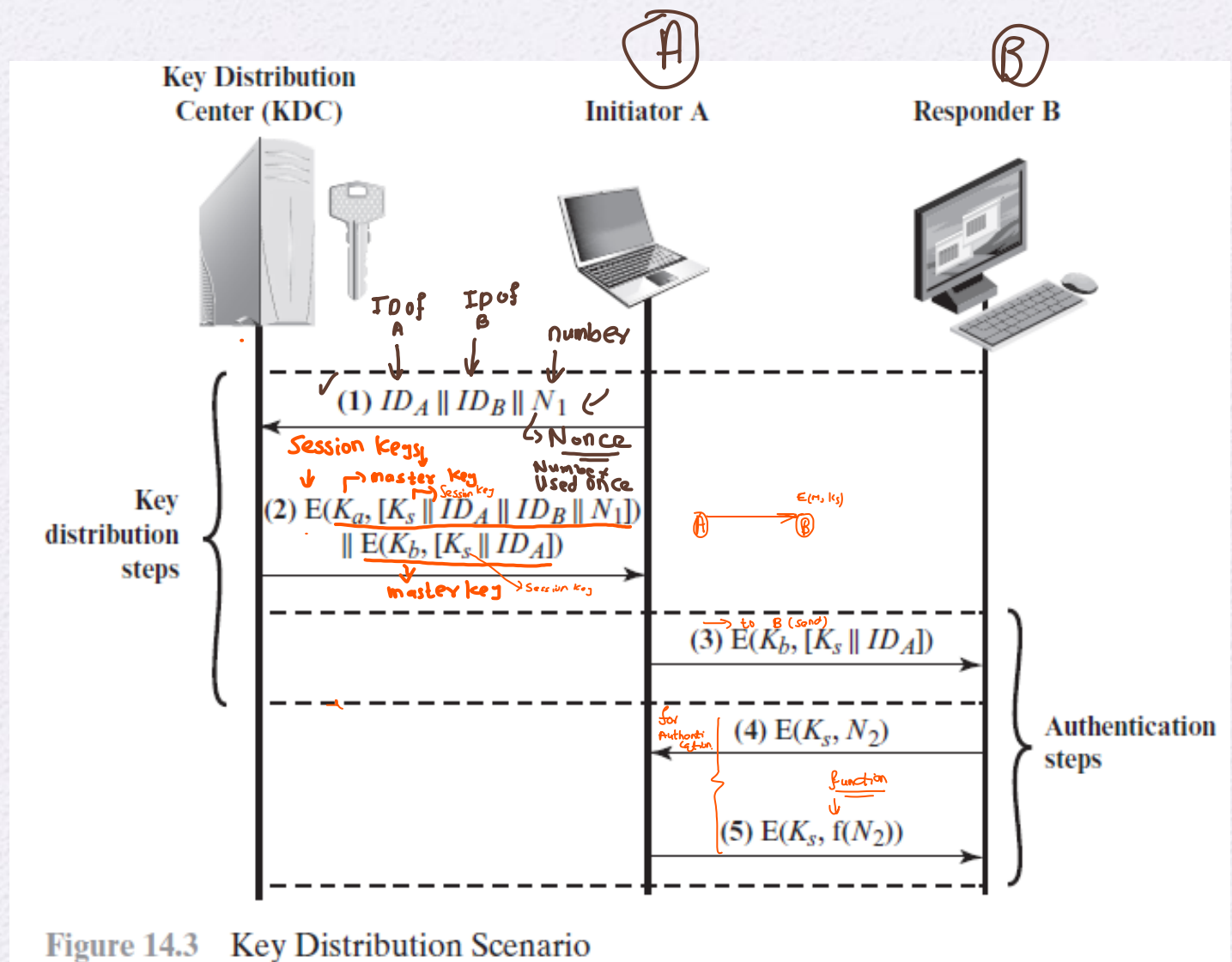


Figure 14.3 Key Distribution Scenario

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

For connection-oriented protocols one choice is to use the same session key for the length of time that the connection is open, using a new session key for each new session

A security manager must balance competing considerations:

For a connectionless protocol there is no explicit connection initiation or termination, thus it is not obvious how often one needs to change the session key

The more frequently session keys are exchanged, the more secure they are

The distribution of session keys delays the start of any exchange and places a burden on network capacity

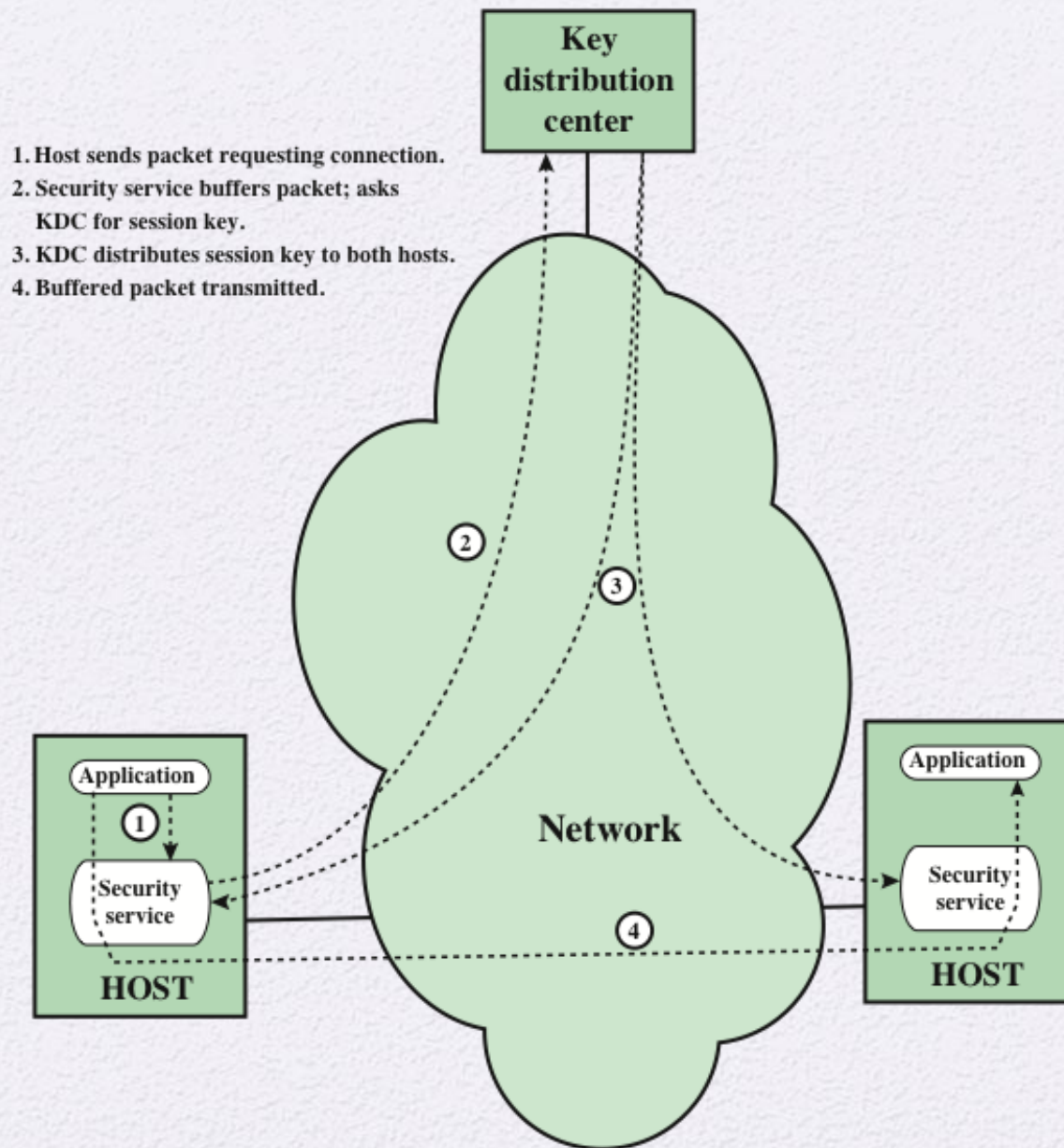


Figure 14.4 Automatic Key Distribution for Connection-Oriented Protocol

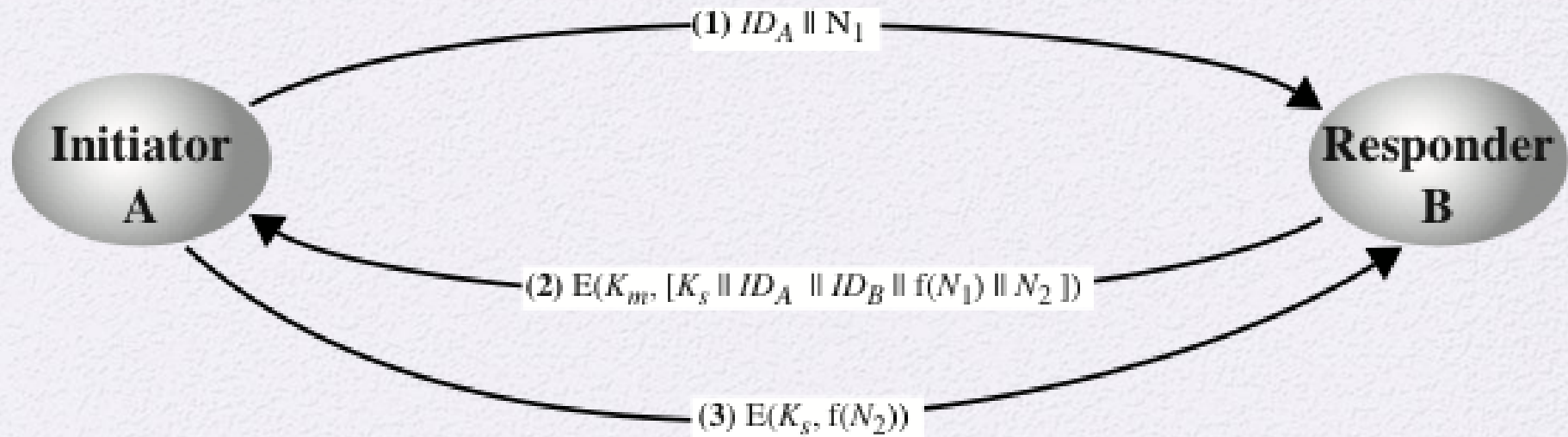
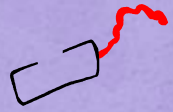


Figure 14.5 Decentralized Key Distribution

https://www.youtube.com/watch?v=lvXhyUG50xk&ab_channel=SAVI

Controlling Key Usage

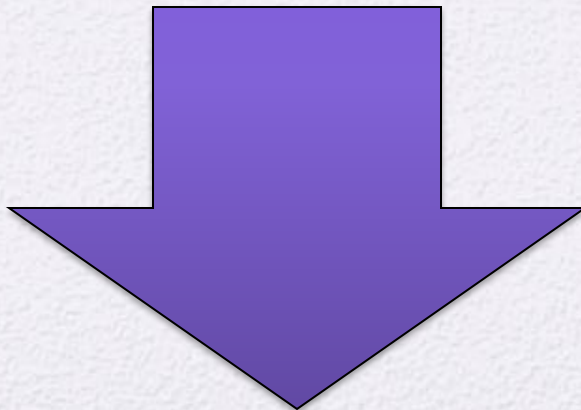


- The concept of a key hierarchy and the use of automated key distribution techniques greatly reduce the number of keys that must be manually managed and distributed
- It also may be desirable to impose some control on the way in which automatically distributed keys are used
 - For example, in addition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



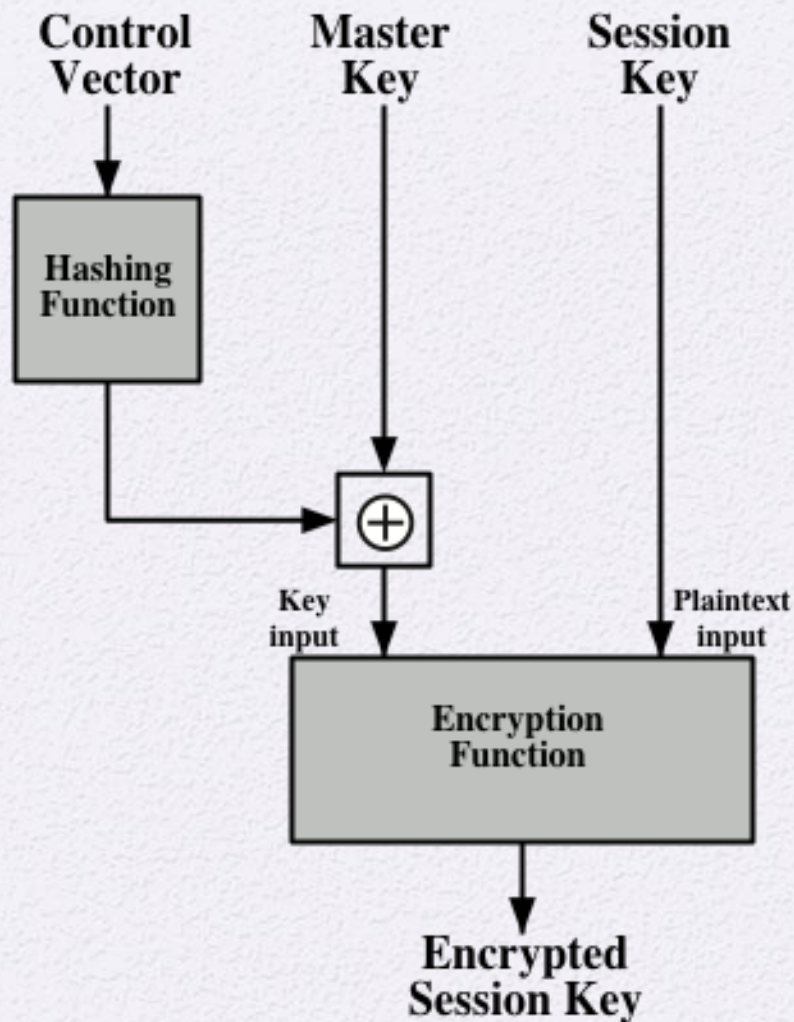
Key Controls

- 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

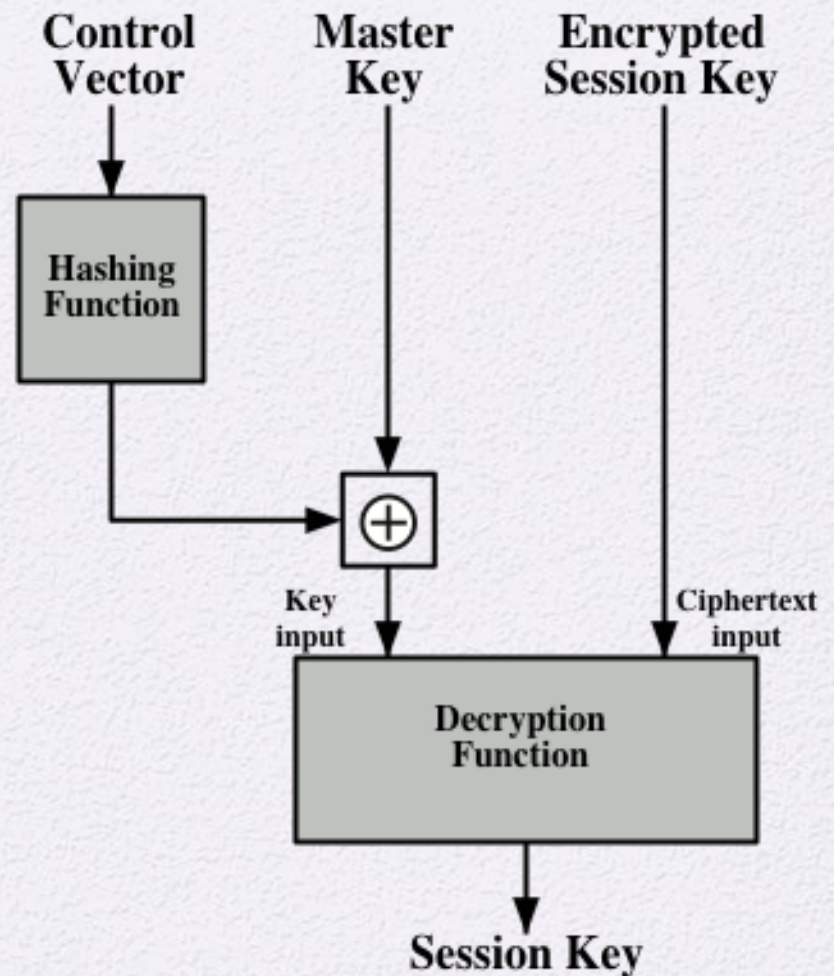


Drawbacks:

- 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



(a) Control Vector Encryption



(b) Control Vector Decryption

Figure 14.6 Control Vector Encryption and Decryption

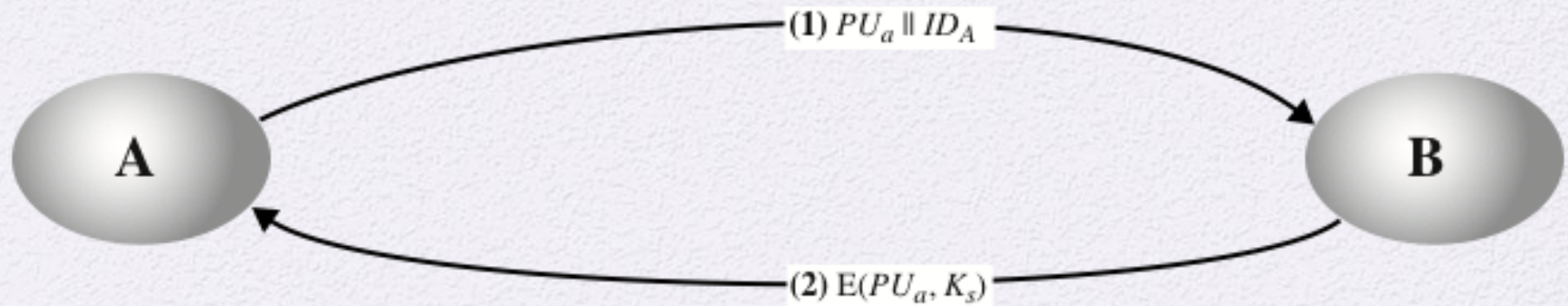


Figure 14.7 Simple Use of Public-Key Encryption to Establish a Session Key

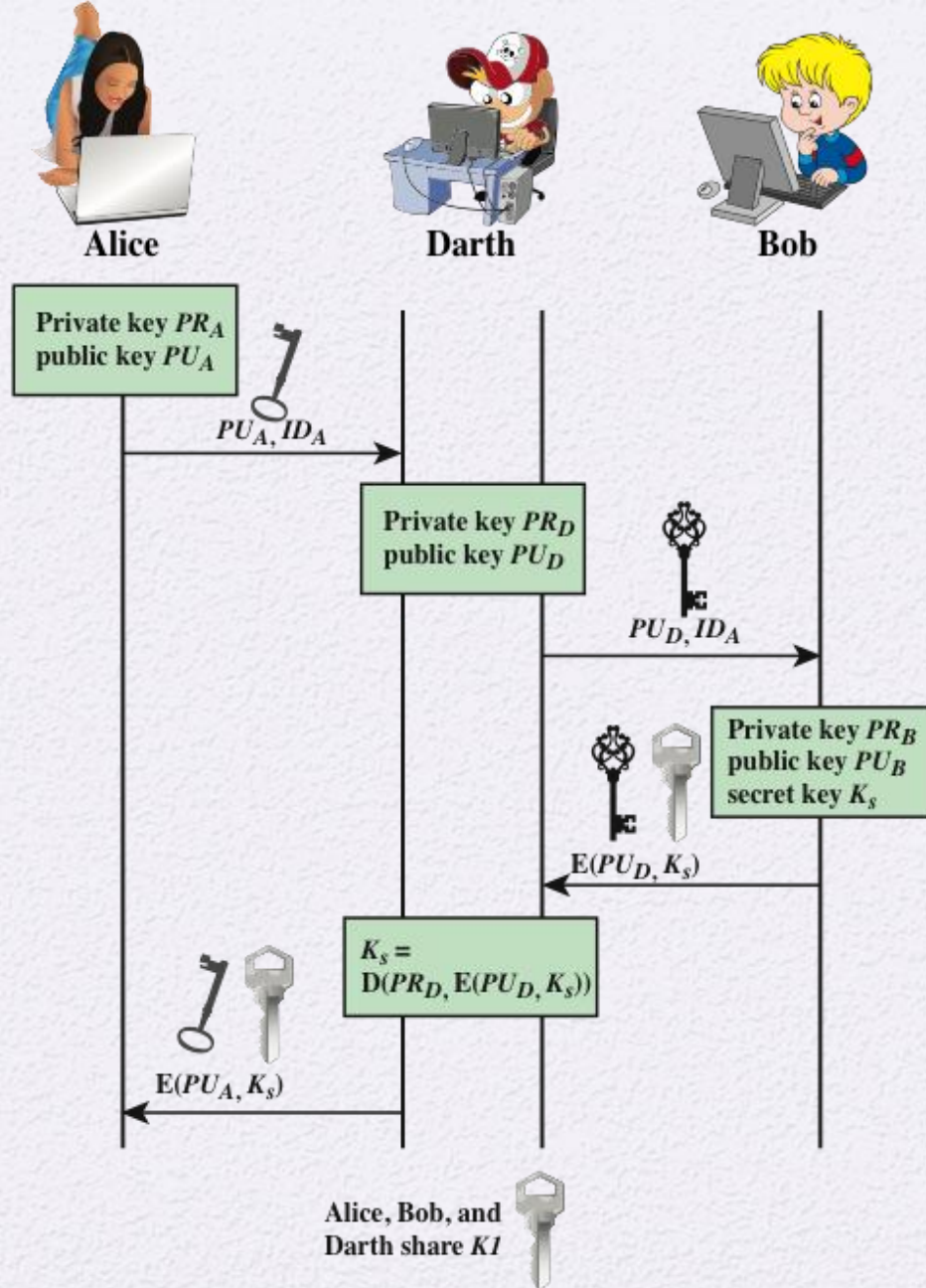


Figure 14.8 Another Man-in-the-Middle Attack

Confidentiality and Authentication

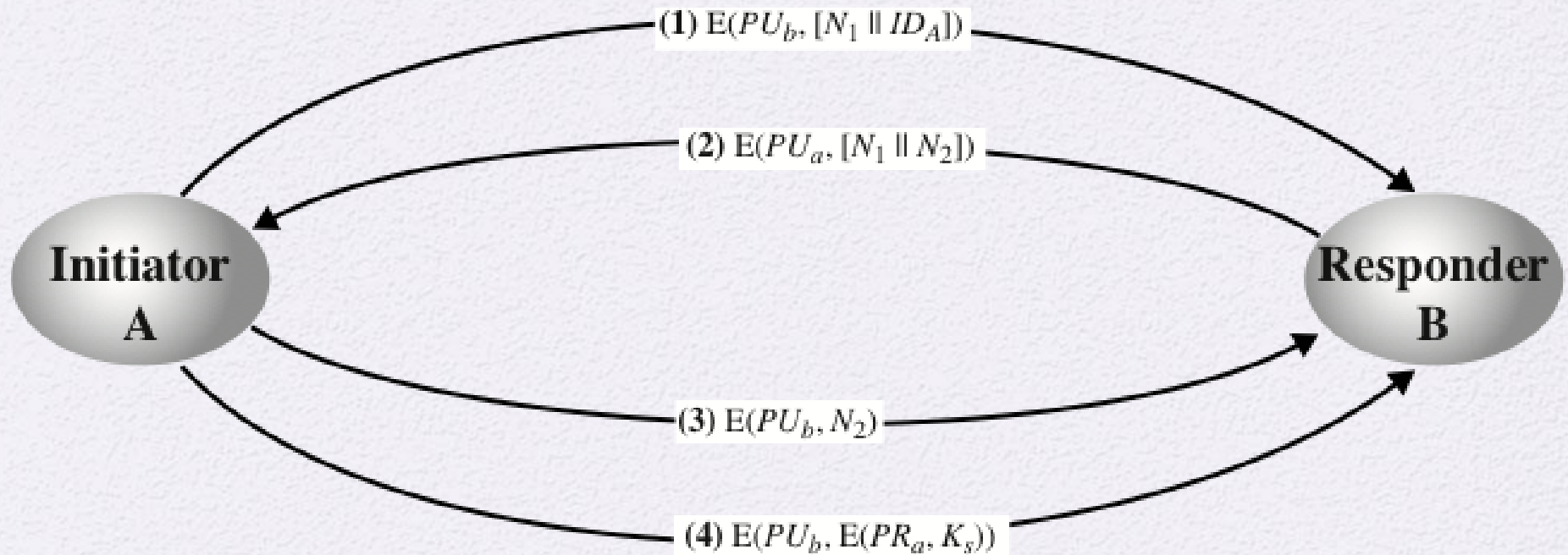


Figure 14.9 Public-Key Distribution of Secret Keys

A Hybrid Scheme

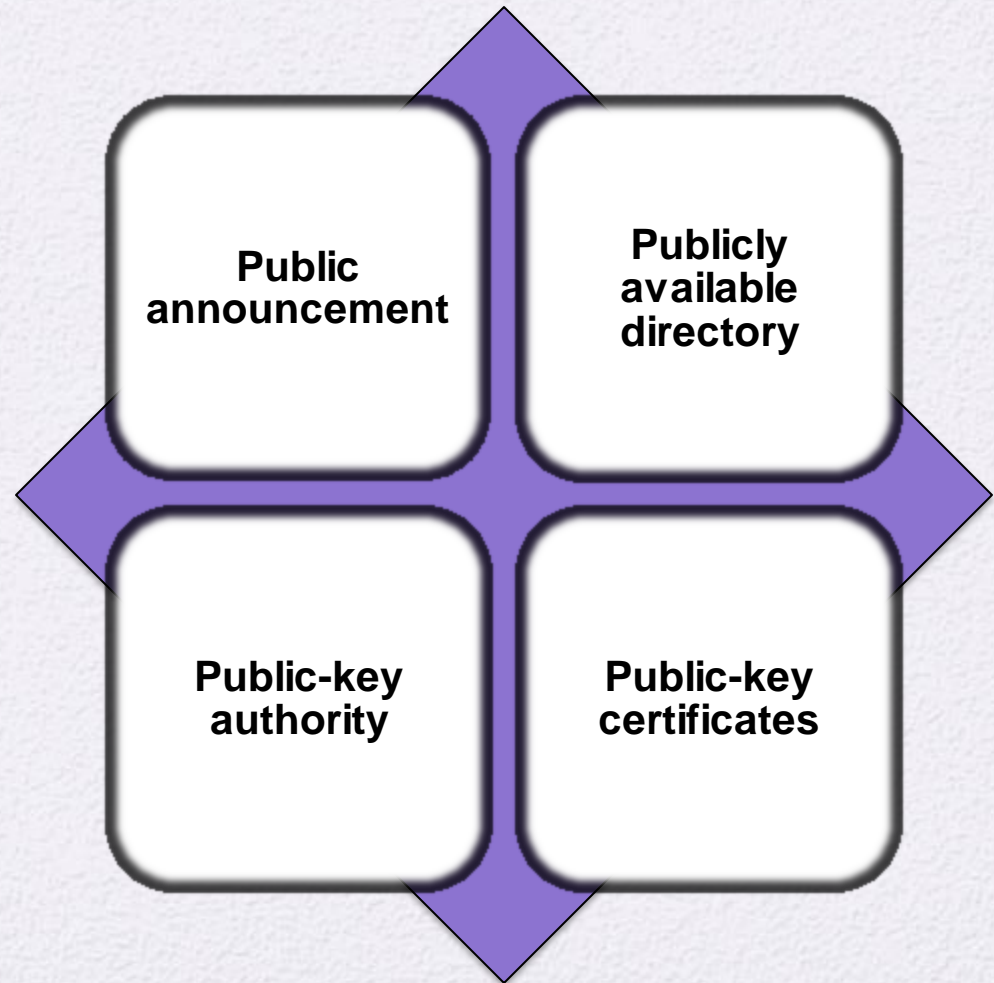
- In use on IBM mainframes
- Retains the use of a key distribution center (KDC) that shares a secret master key with each user and distributes secret session keys encrypted with the master key
- A public-key scheme is used to distribute the master keys

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:



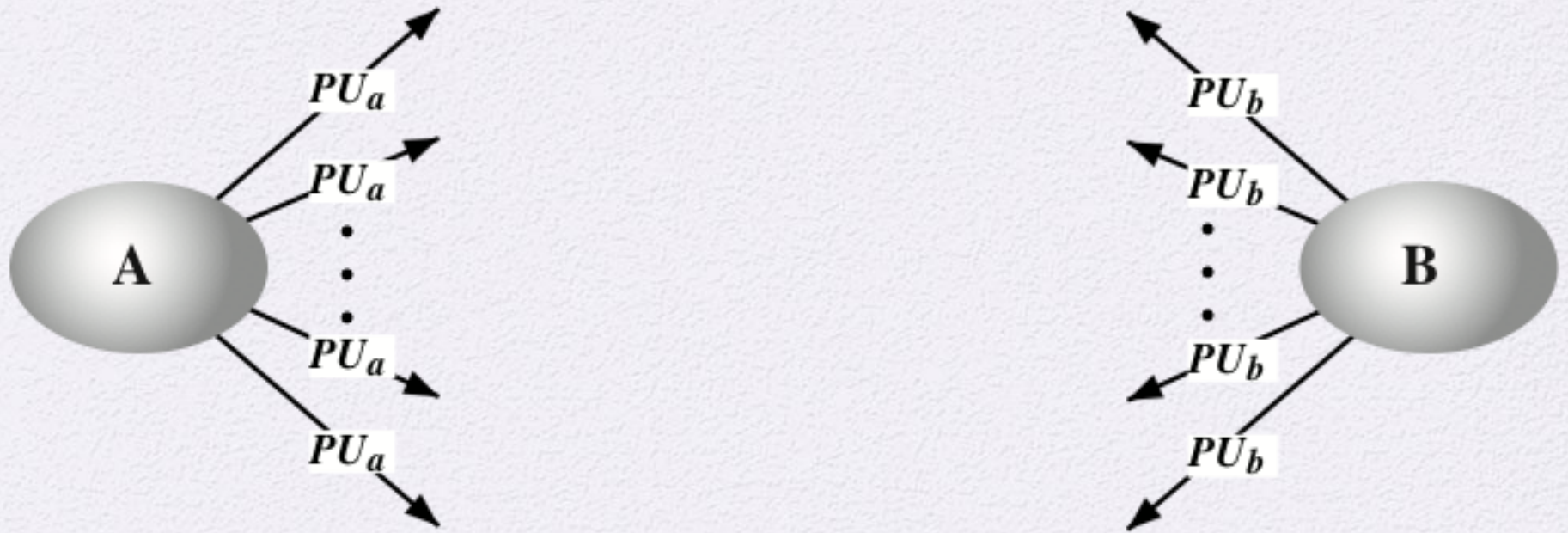


Figure 14.10 Uncontrolled Public Key Distribution

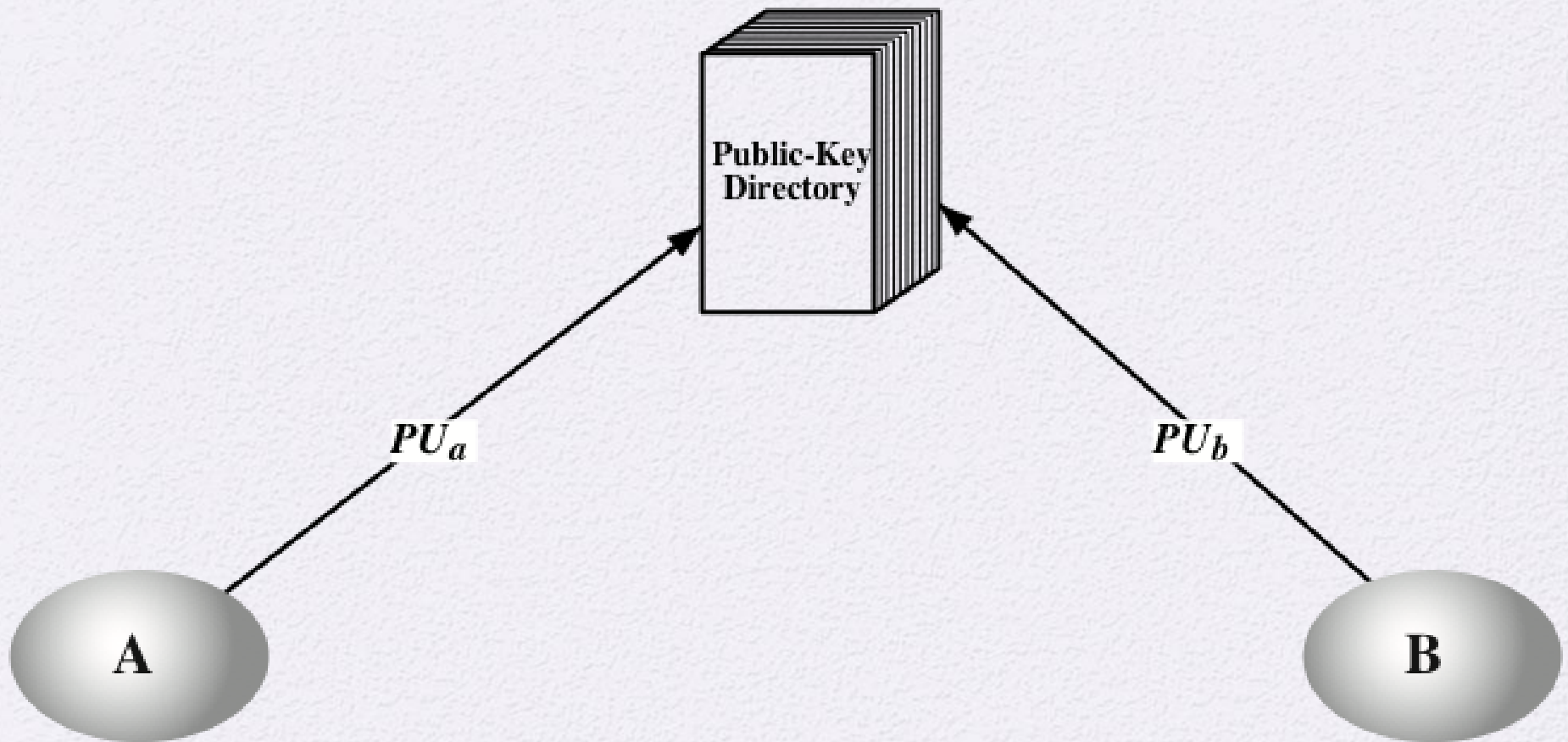


Figure 14.11 Public Key Publication

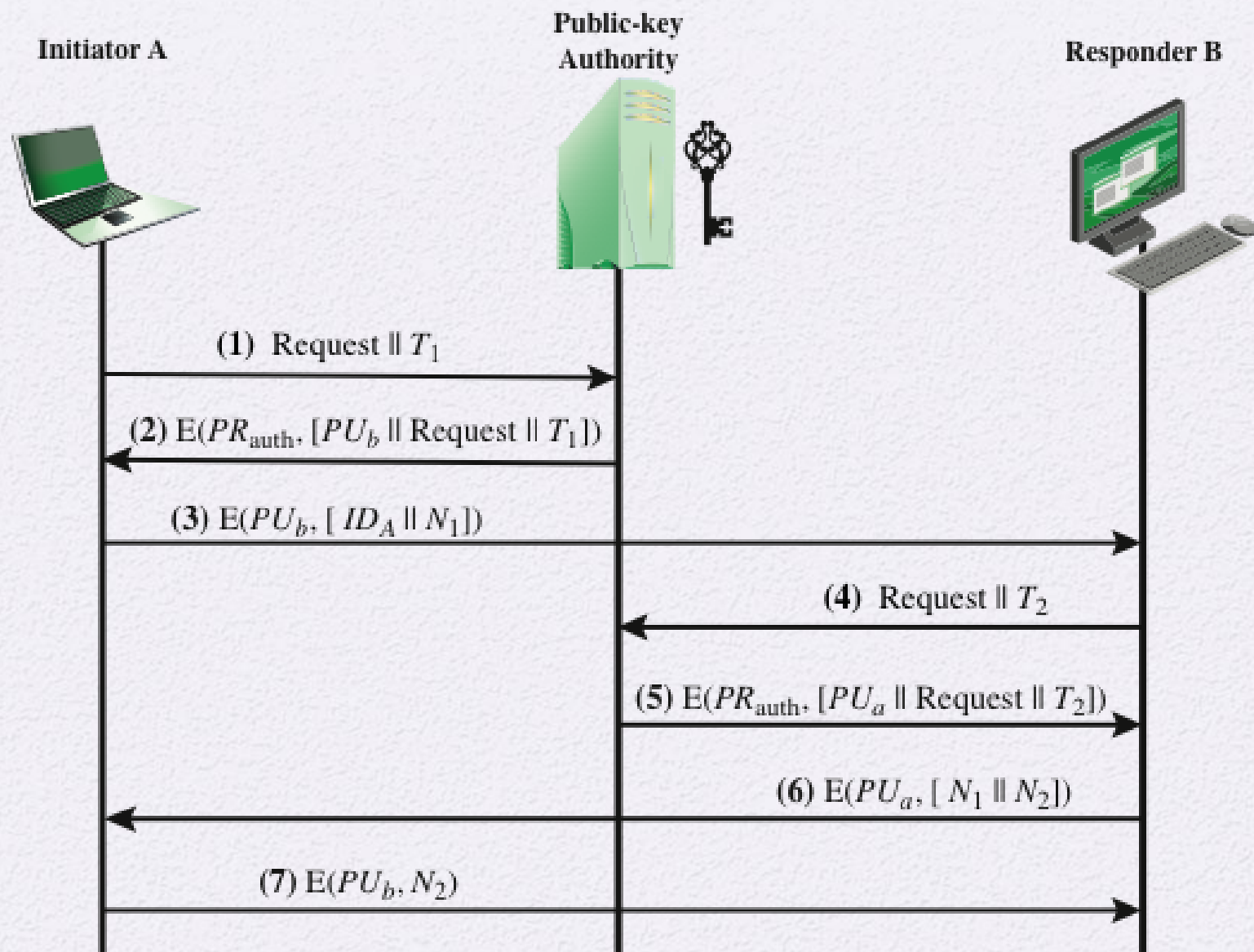
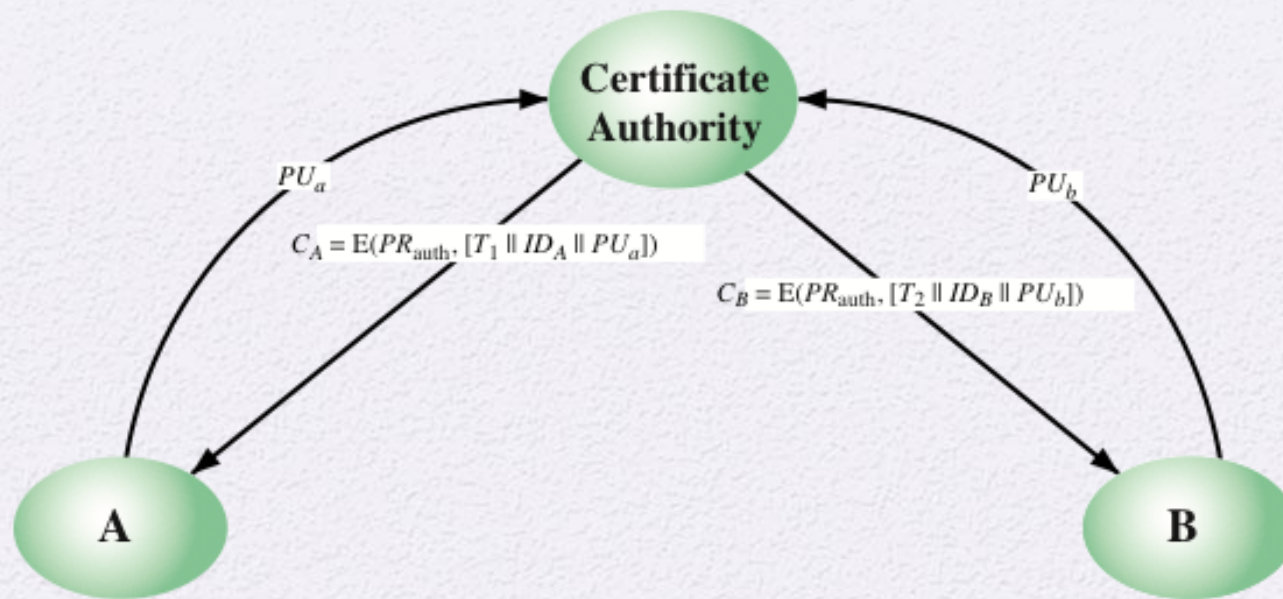
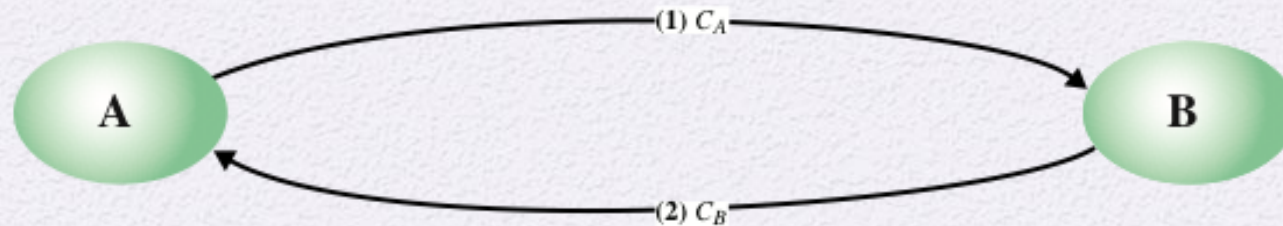


Figure 14.12 Public-Key Distribution Scenario



(a) Obtaining certificates from CA



(b) Exchanging certificates

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