# Key Distribution

Problem of Symmetric Cryptography Algorithm

# Key Distribution

- Symmetric schemes require both parties to share a common/same secret key.
- Issue is how to securely distribute this key.
- So some mechanism is required for secure transmission of key is known as *key distribution*.
- often *secure system fails due to a break* in the key distribution scheme.

# Key Management

1. Authentication of the users of the key.
2. Generation of key.
3. Distribution of key.
4. Storage of key.

# Key Distribution

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

# Key Distribution

- **Session key:**
  - Data encrypted with a one-time session key. At the conclusion of the session the key is destroyed.
- **Permanent key:**
  - Used between entities for the purpose of *distributing session keys.*

# Automatic Key Distribution

- Session Key
  - Used for duration of one logical connection
  - Destroyed at end of session
  - Used for user data
- Permanent key
  - Used for distribution of keys
- Key distribution center
  - Determines which systems may communicate
  - Provides one session key for that connection
- Front end processor
  - Performs end to end encryption
  - Obtains keys for host

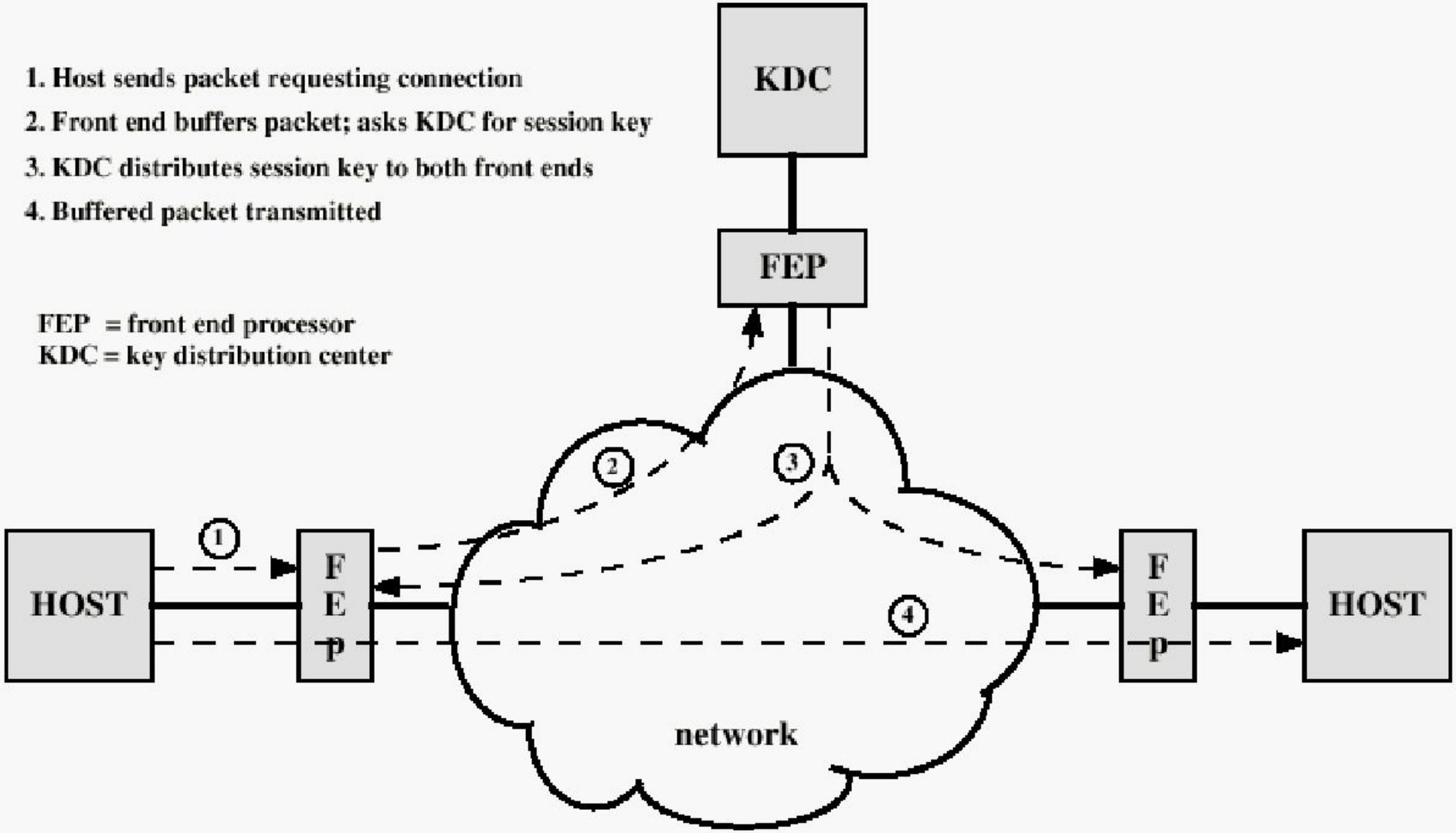



**Figure 2.10 Automatic Key Distribution for Connection-Oriented Protocol**

# Key Distribution in Public key Crypto

- Following are the 4 ways

1. Public Announcement
2. Publicly available directory
3. Public key Authority
4. Public key Certificate

# 1. Public Announcement

- Broadcasted by the owner of the key.
- Limitation:=
    1. Forge key
    2. Misuse it
    3. No Control on accessing of the key

# 2. Publicly Available Directory

- Directory of Keys is maintained by third party
- Directory is Password protected
- Only Registered User can access it

| Name | Public Key |
|---|---|
| A | 115 |
| B | 215 |

- Hacking:=
  1. Password of the Directory being steal

# 3. Public Key Authority(PKA)

- Public key of the user can only be accessed by decrypting reply message of PKA.

- Private key of PKA used for encryption purpose & vice-versa.

- Limitation:=
  I. Reuse of public key by either party in future.
  II. System slow down due too overhead.

- T1 & T2 – time of request
- N1 & N2 – random number called as nounce.
- $ID_A$ – network address of Initiator A for communication
- Step 7- Initiator A confirm the Request by replying back.

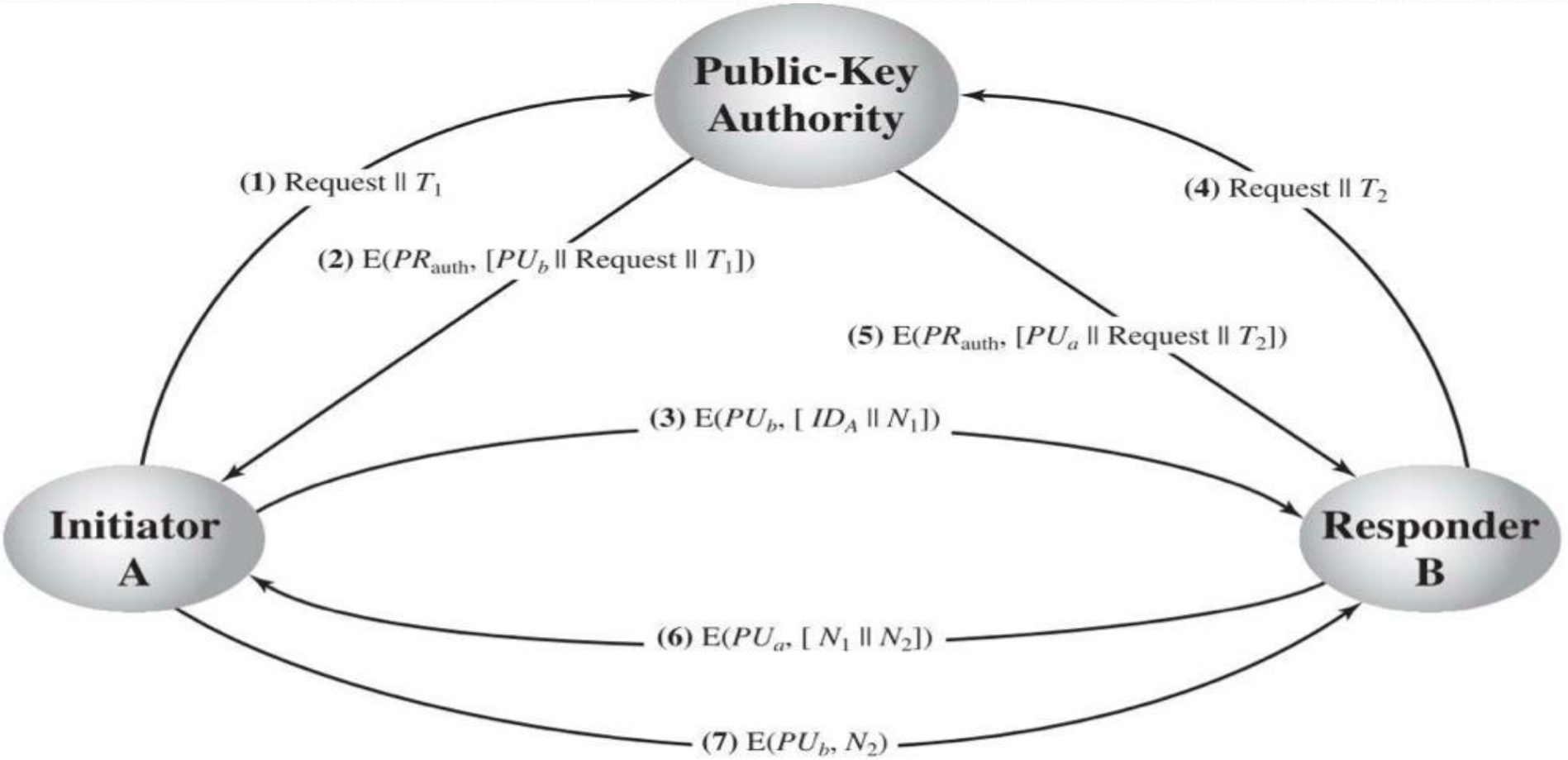
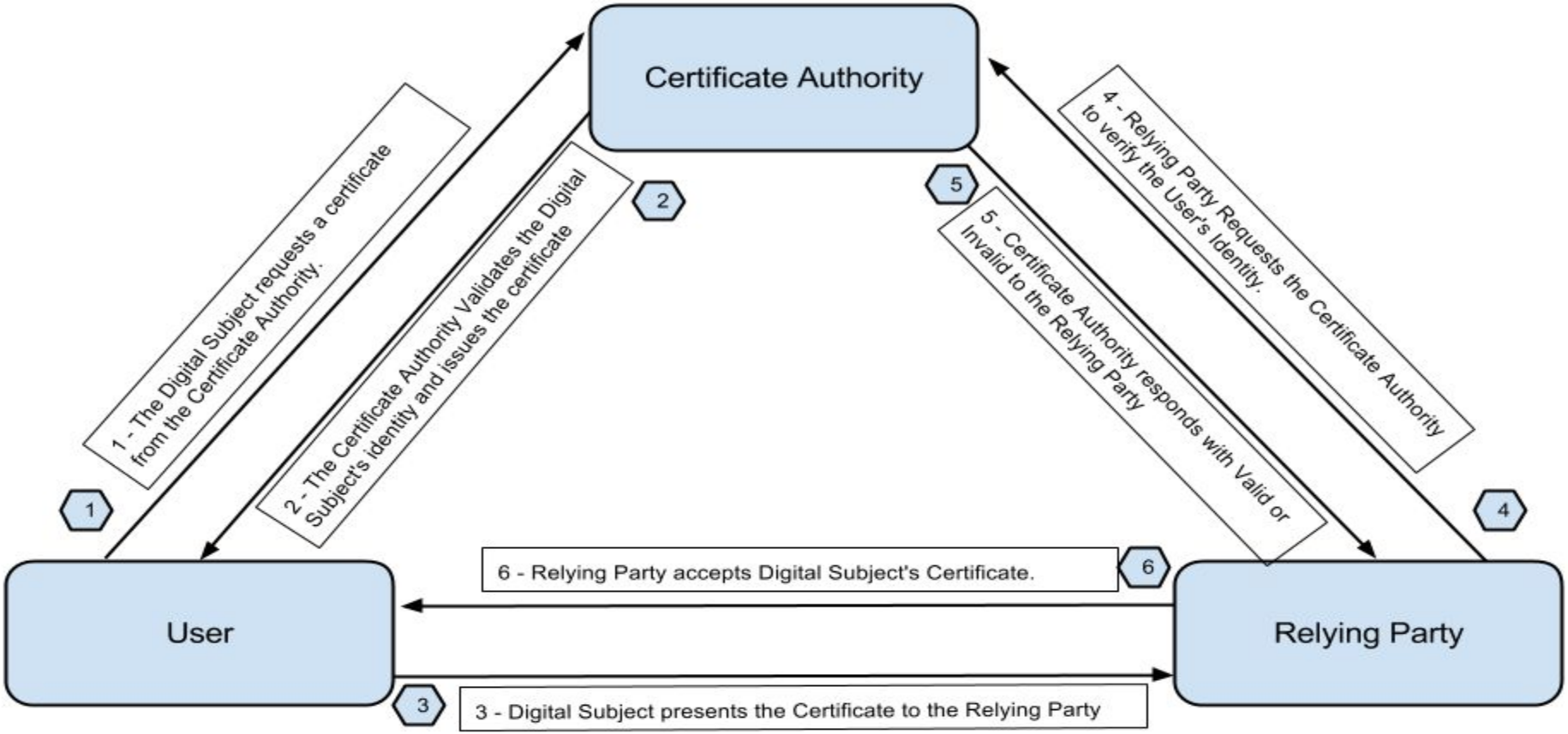



Figure 14.11 Public-Key Distribution Scenario

# 3. Public Key Certificate(PKC)

- Suggested by Kohnfelder.
- Initiator sends name & his public key.
- Public keys are exchanged by means of certificates.
- Private key of PKC used for encryption purpose & vice-versa.
- Certificate contains information such as *time of the request, network address & public key* of the user who made the request.

# PKC Overview



# 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 purposes keys are used for

# Summary

- have considered:
  - use of symmetric encryption to protect confidentiality
  - need for good key distribution
  - use of trusted third party KDC's

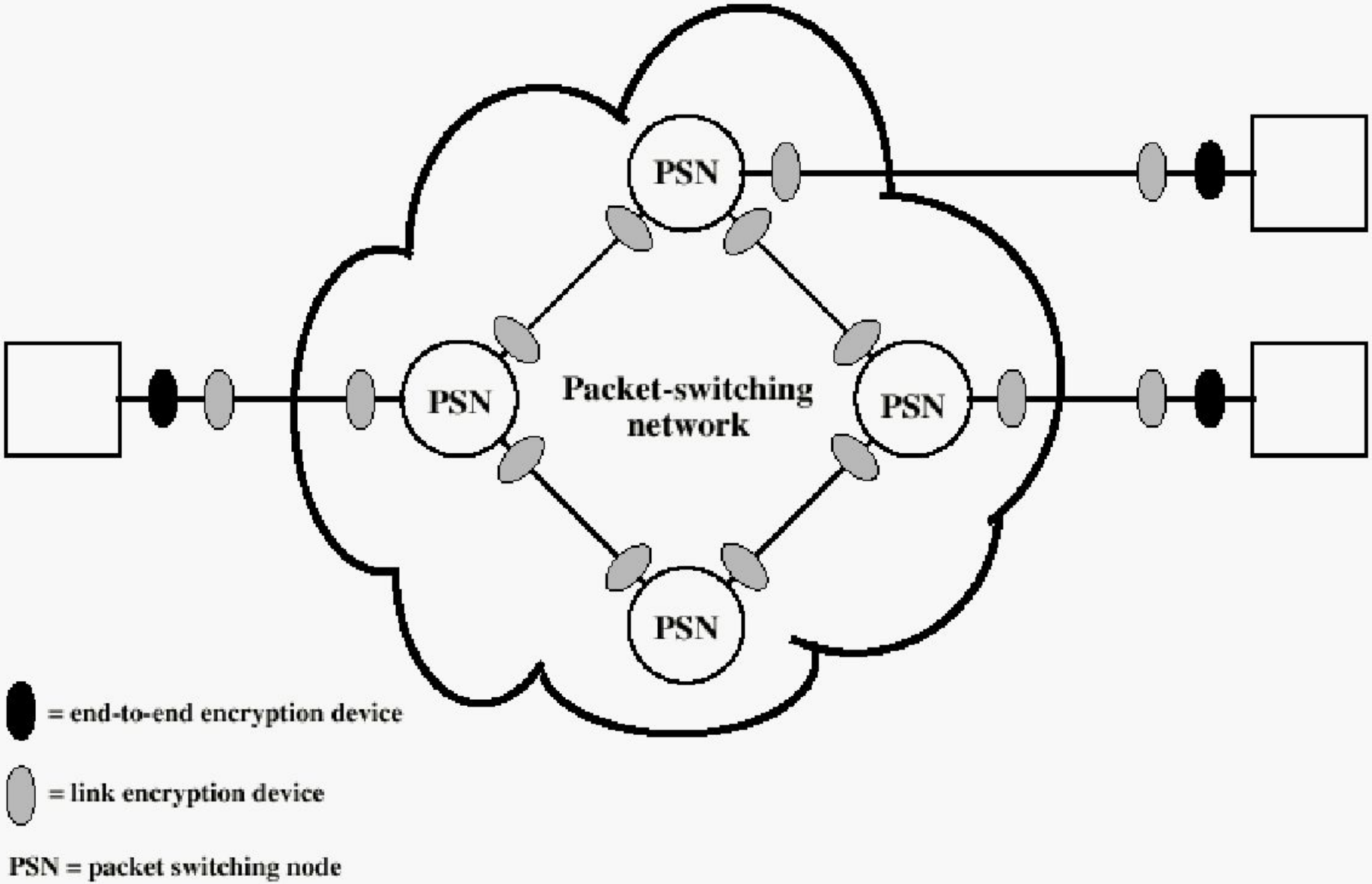



**Figure 2.9 Encryption Across a Packet-Switching Network**

# Recommended Reading

- Stallings, W. *Cryptography and Network Security: Principles and Practice, 2nd edition*. Prentice Hall, 1999
- Scneier, B. *Applied Cryptography*, New York: Wiley, 1996
- Mel, H.X. Baker, D. *Cryptography Decrypted*. Addison Wesley, 2001