Network Security

Dr. Qazi Ejaz Ali

Assistant Professor

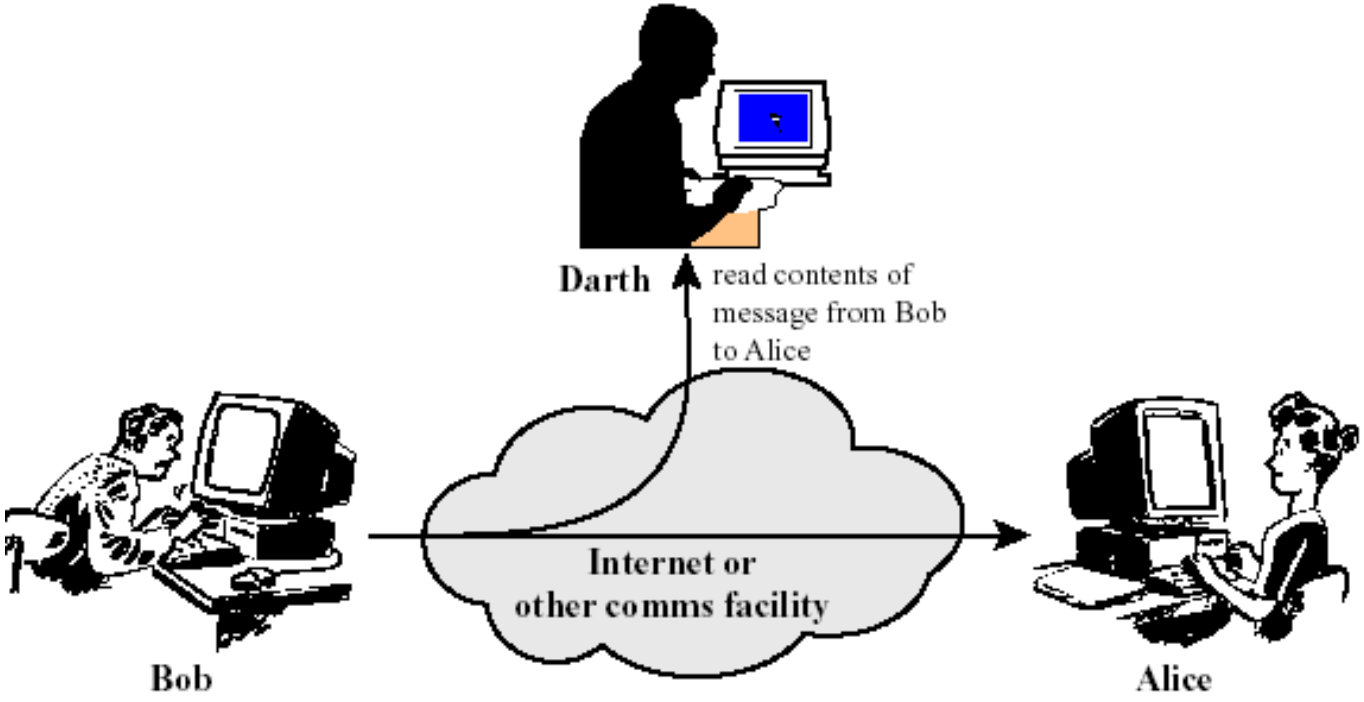
Department of computer Science

University of Peshawar

Passive and active attacks

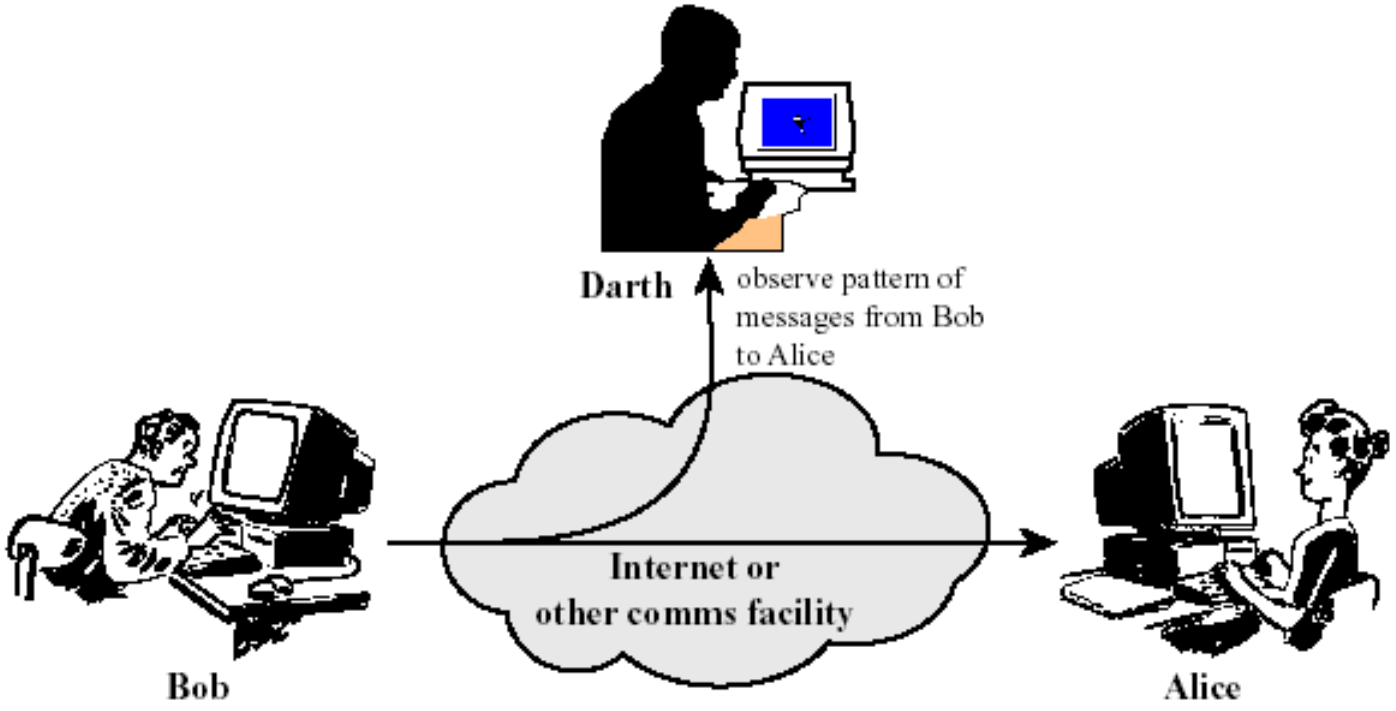
- **Passive attacks**
  - No modification of content or fabrication
  - Eavesdropping to learn contents or other information (transfer patterns, traffic flows etc.)
- **Active attacks**
  - Modification of content and/or participation in communication to
    - Impersonate legitimate parties
    - Modify the content in transit
    - Launch denial of service attacks

Passive Attacks



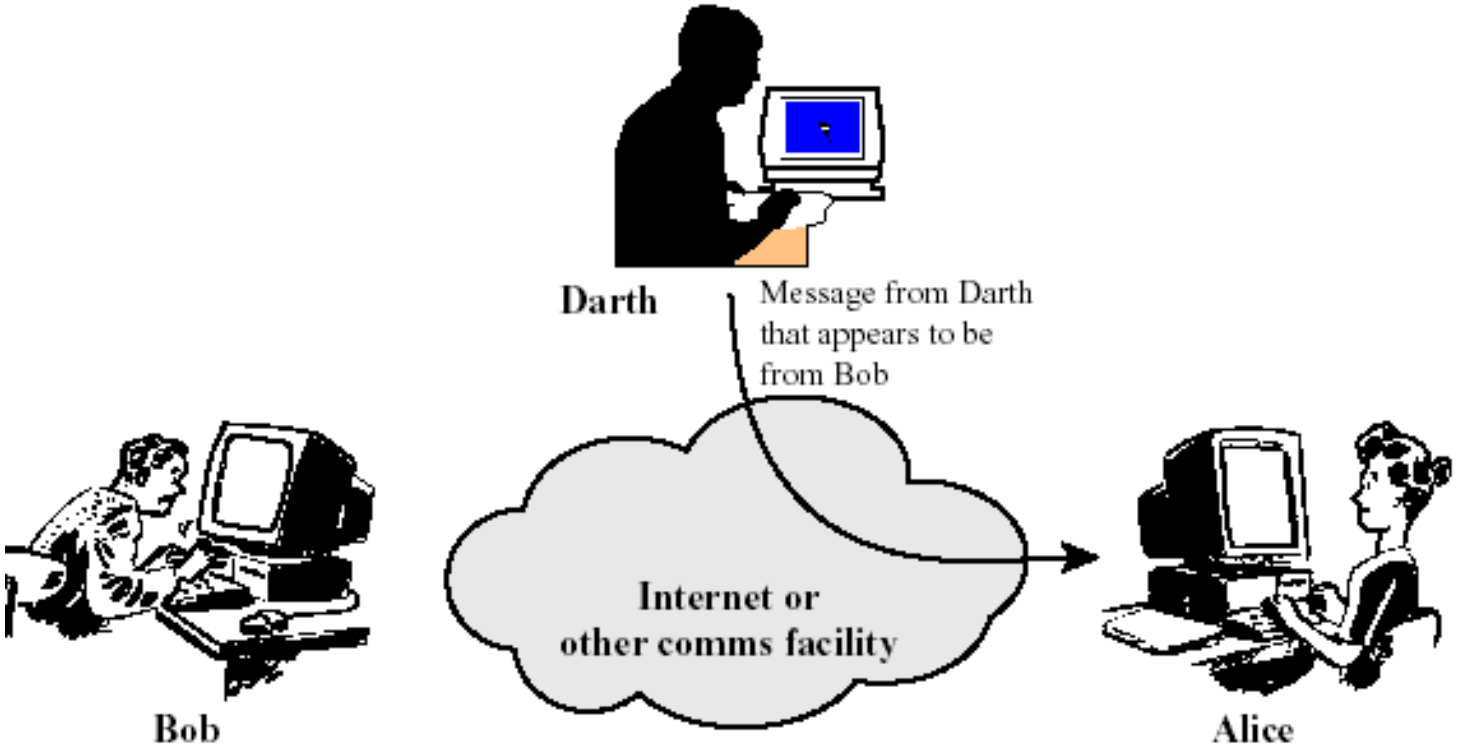
(a) Release of message contents

Passive Attacks



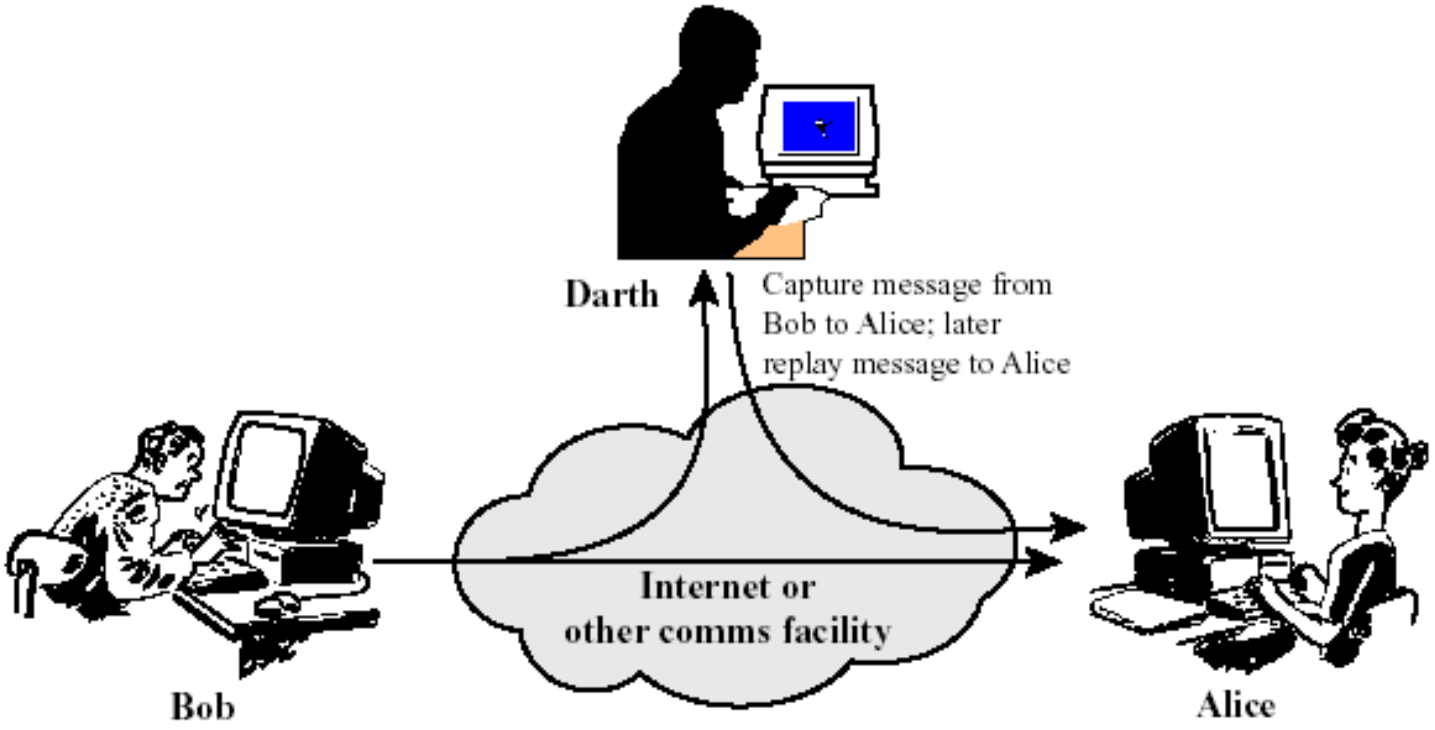
(b) Traffic analysis

Active Attacks



(a) Masquerade

Active Attacks



(b) Replay

Common Attacks on Encrypted Schemes

- cipher text only
-known plain text
-chosen plain text

Types of Cryptography

1. Secret key cryptography
2. public key cryptography
3. Hash Algorithm

Conventional Encryption Message Confidentiality

Conventional Encryption Principles

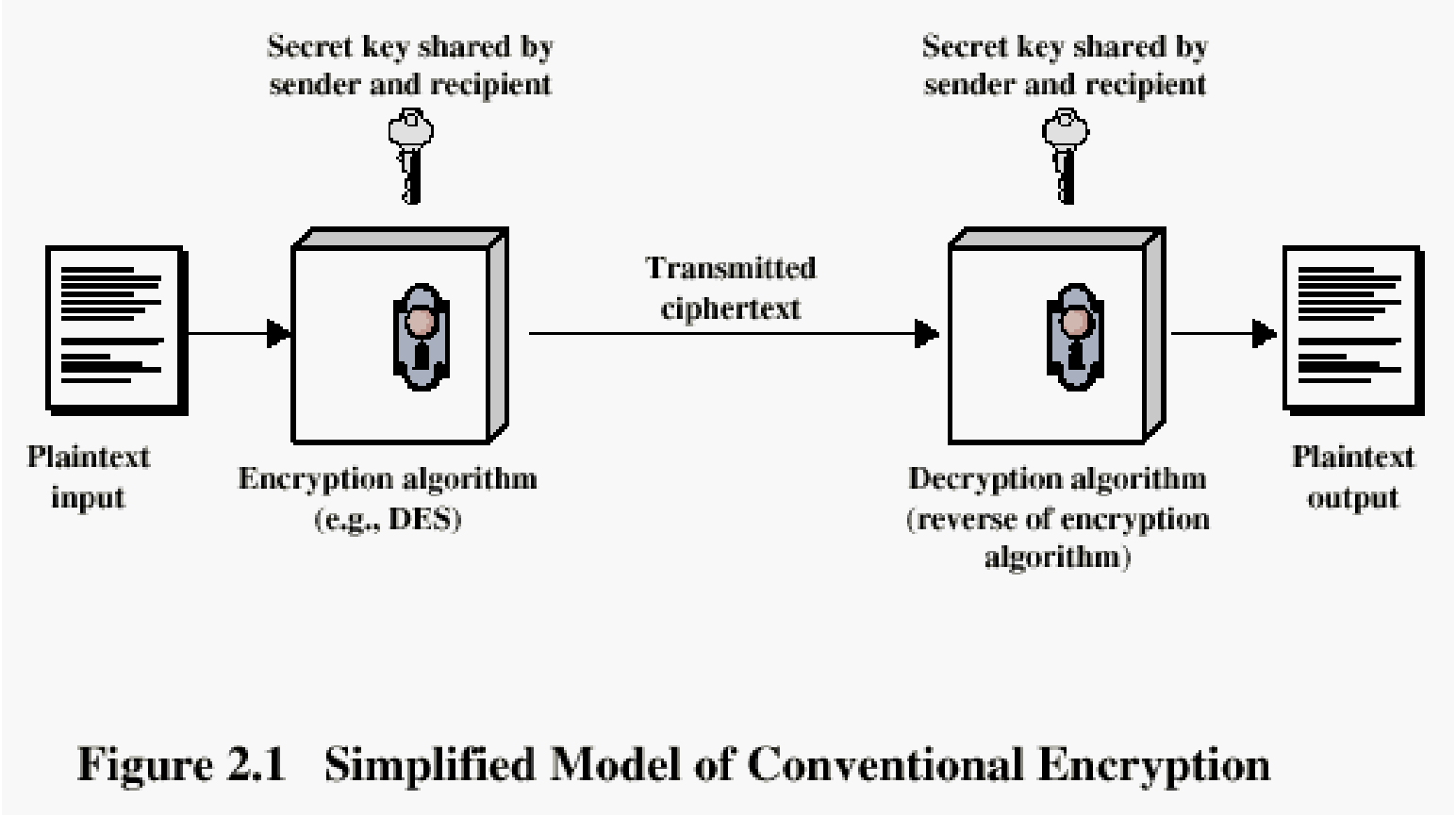


Figure 2.1 Simplified Model of Conventional Encryption

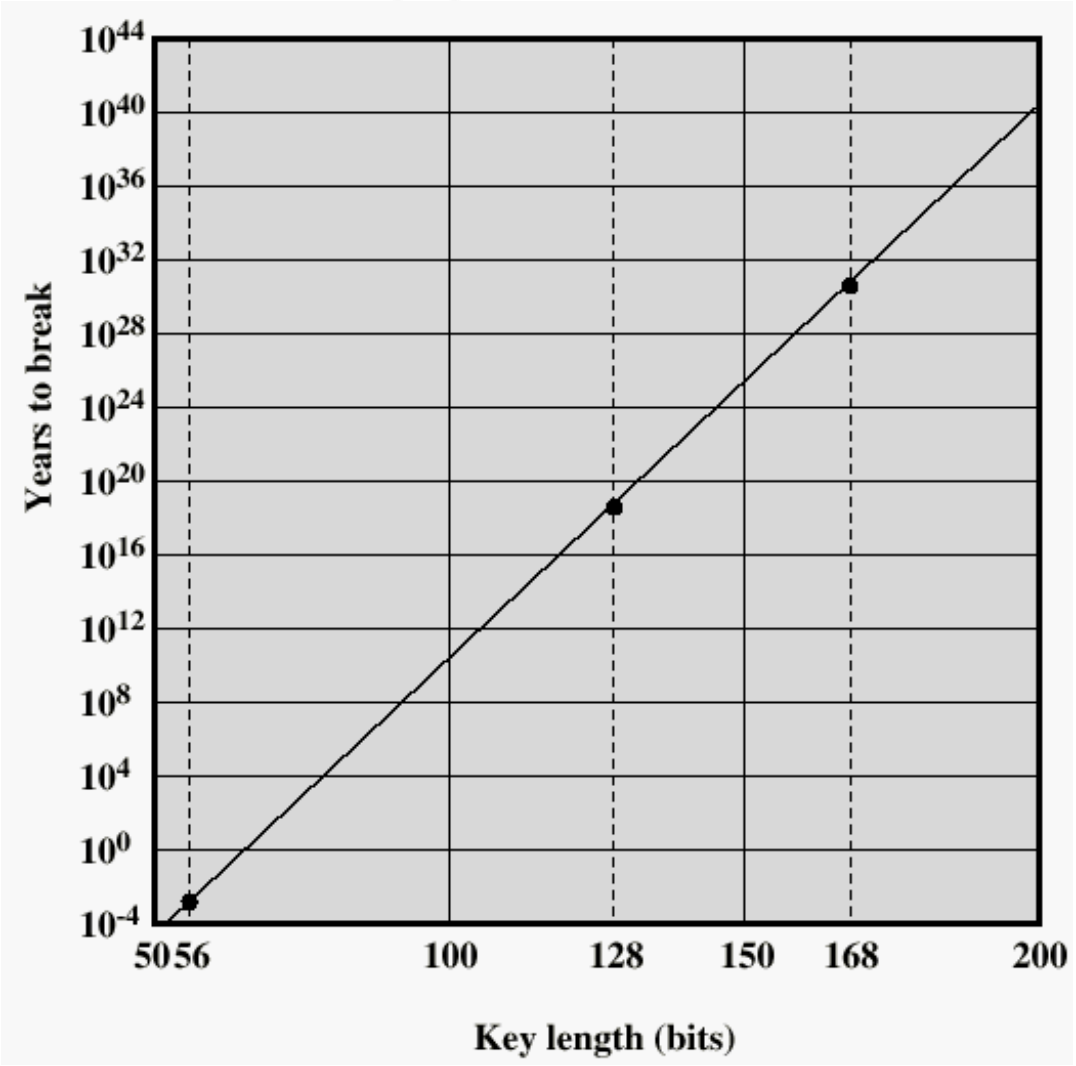
Average time required for exhaustive key search

Key Size (bits)	Number of Alternative Keys	Time required at 10^6 Decryption/μs
32	$2^{32} = 4.3 \times 10^9$	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	10 hours
128	$2^{128} = 3.4 \times 10^{38}$	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	5.9×10^{30} years

Conventional Encryption Algorithms

- Data Encryption Standard (DES)
  - The most widely used encryption scheme
  - The algorithm is reffered to the Data Encryption Algorithm (DEA)
  - DES is a block cipher
  - The plaintext is processed in 64-bit blocks
  - The key is 56-bits in length

Time to break a code (10^6 decryptions/μs)



Other Symmetric Block Ciphers

- **International Data Encryption Algorithm (IDEA)**
  - 128-bit key
  - Used in PGP
- **Blowfish**
  - Easy to implement
  - High execution speed
  - Run in less than 5K of memory

Other Symmetric Block Ciphers

- **RC5**
  - Suitable for hardware and software
  - Fast, simple
  - Adaptable to processors of different word lengths
  - Variable number of rounds
  - Variable-length key
  - Low memory requirement
  - High security
  - Data-dependent rotations
- **Cast-128**
  - Key size from 40 to 128 bits
  - The round function differs from round to round

Location of Encryption Device

- **Link encryption:**
  - A lot of encryption devices
  - High level of security
  - Decrypt each packet at every switch
- **End-to-end encryption**
  - The source encrypt and the receiver decrypts
  - Payload encrypted
  - Header in the clear
- **High Security:** Both link and end-to-end encryption are needed (see Figure 2.9)

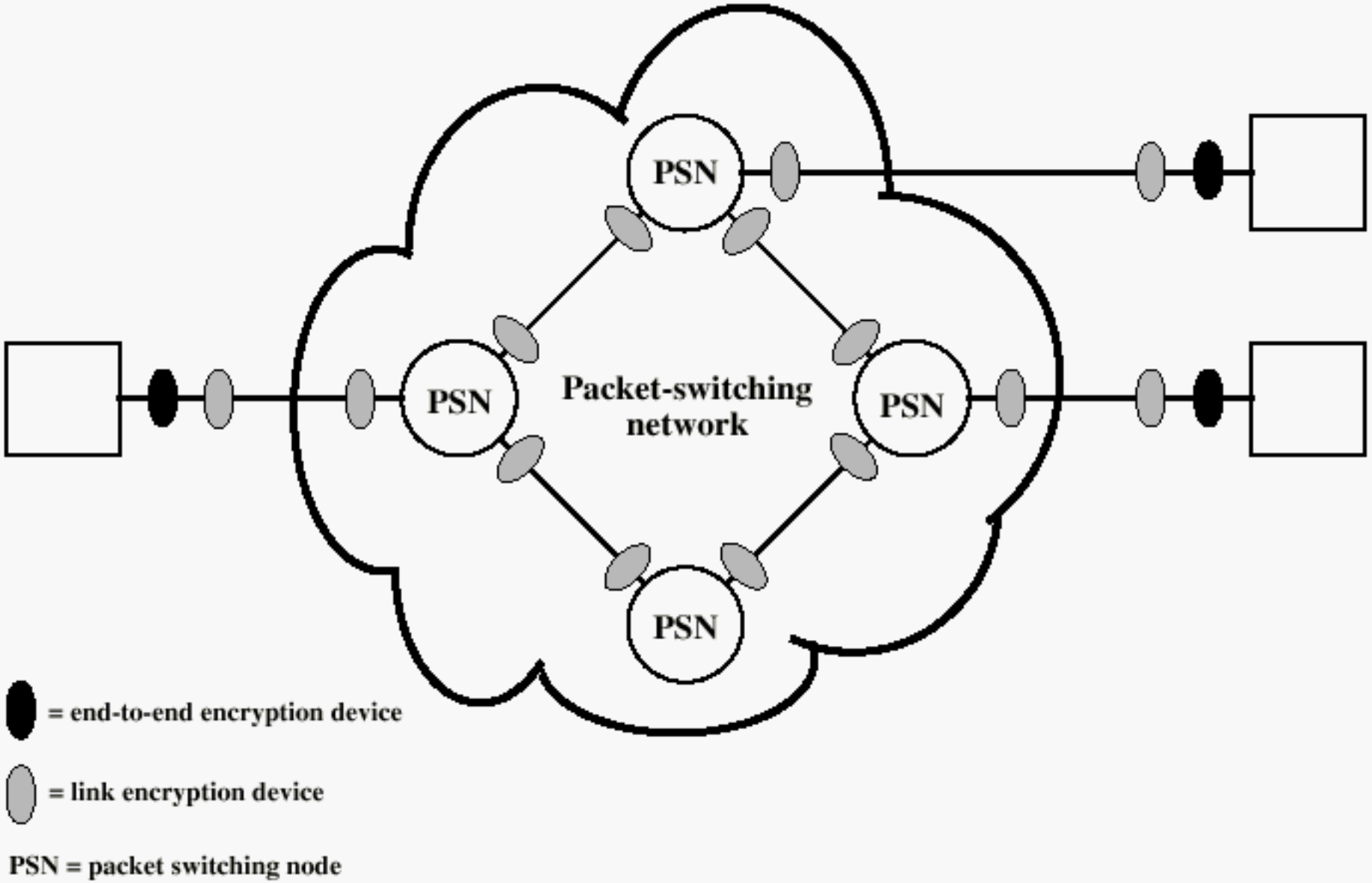


Figure 2.9 Encryption Across a Packet-Switching Network

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