

Chapter 2

Conventional Encryption Message Confidentiality

Henric Johnson

Blekinge Institute of Technology, Sweden

<http://www.its.bth.se/staff/hjo/>

henric.johnson@bth.se



Outline

- *Conventional Encryption Principles*
- *Conventional Encryption Algorithms*
- *Cipher Block Modes of Operation*
- *Location of Encryption Devices*
- *Key Distribution*

Conventional Encryption Principles

- *An encryption scheme has five ingredients:*
 - *Plaintext*
 - *Encryption algorithm*
 - *Secret Key*
 - *Ciphertext*
 - *Decryption algorithm*
- *Security depends on the secrecy of the key, not the secrecy of the algorithm*

Conventional Encryption Principles

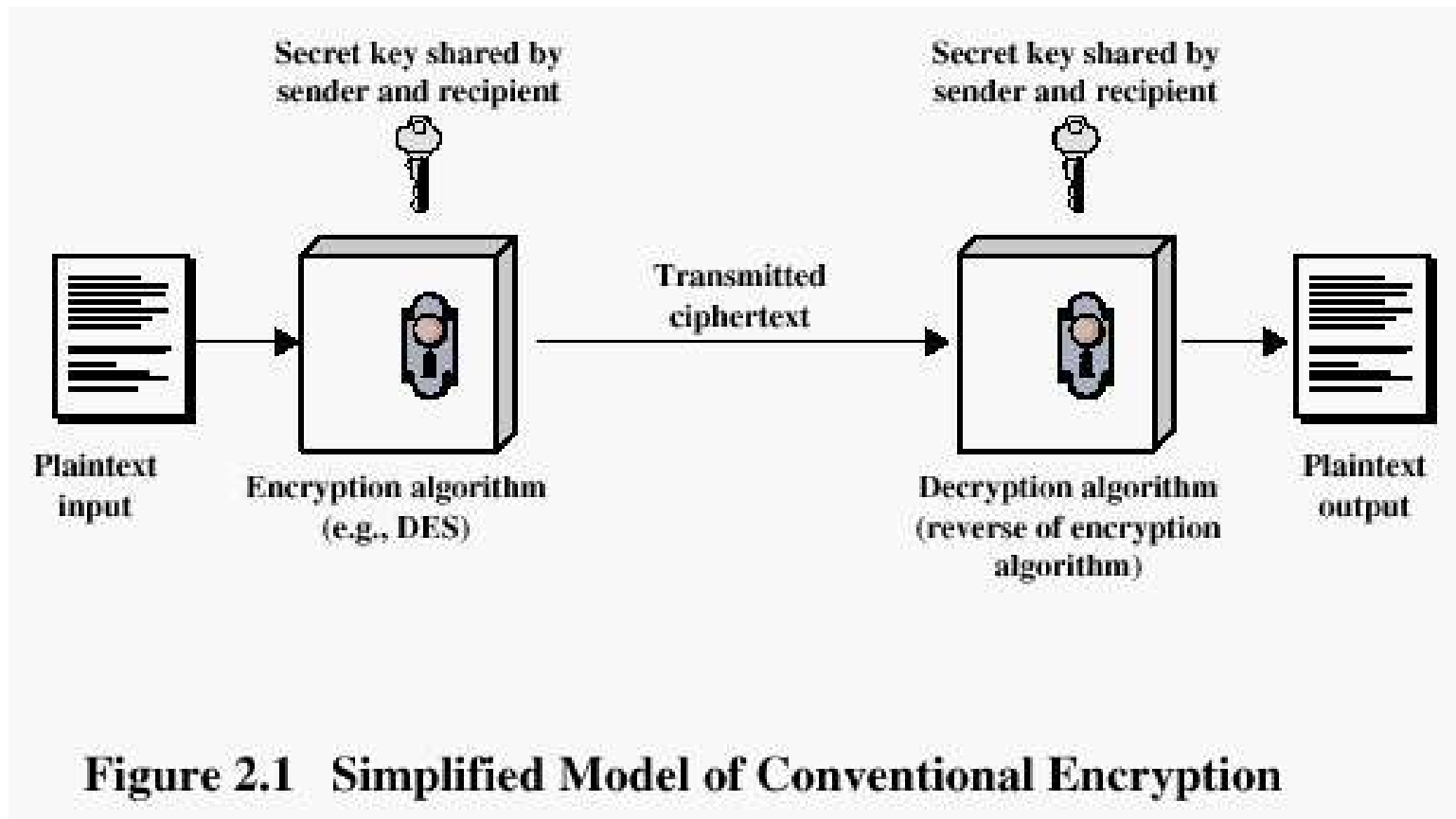


Figure 2.1 Simplified Model of Conventional Encryption

Cryptography

- *Classified along three independent dimensions:*
 - *The type of operations used for transforming plaintext to ciphertext*
 - *The number of keys used*
 - *symmetric (single key)*
 - *asymmetric (two-keys, or public-key encryption)*
 - *The way in which the plaintext is processed*

Average time required for exhaustive key search

<i>Key Size (bits)</i>	<i>Number of Alternative Keys</i>	<i>Time required at 10^6 Decryption/μs</i>
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

Feistel Cipher Structure

- *Virtually all conventional block encryption algorithms, including DES have a structure first described by Horst Feistel of IBM in 1973*
- *The realisation of a Feistel Network depends on the choice of the following parameters and design features (see next slide):*

Feistel Cipher Structure

- *Block size: larger block sizes mean greater security*
- *Key Size: larger key size means greater security*
- *Number of rounds: multiple rounds offer increasing security*
- *Subkey generation algorithm: greater complexity will lead to greater difficulty of cryptanalysis.*
- *Fast software encryption/decryption: the speed of execution of the algorithm becomes a concern*

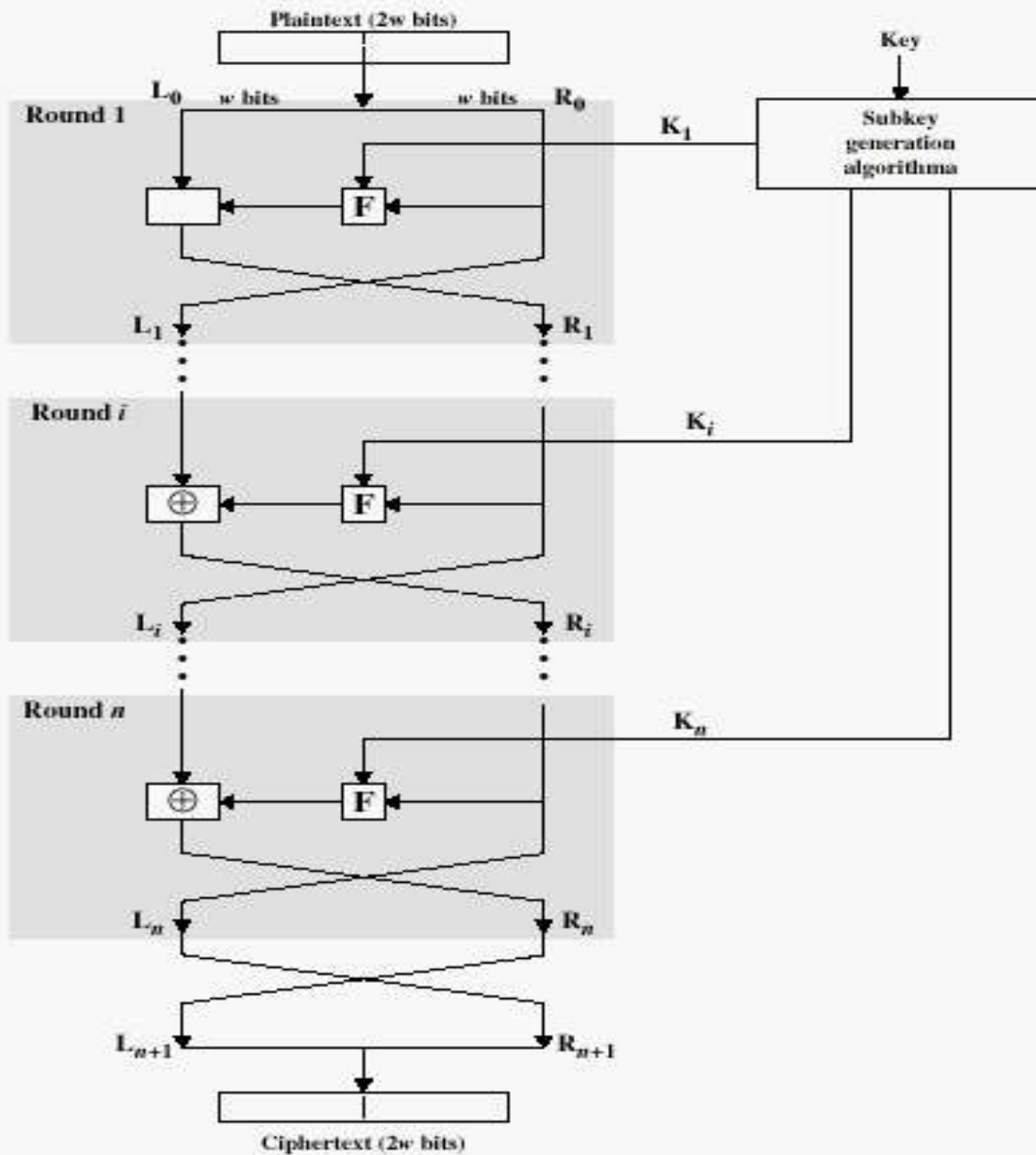


Figure 2.2 Classical Feistel Network

Conventional Encryption Algorithms

- *Data Encryption Standard (DES)*
 - *The most widely used encryption scheme*
 - *The algorithm is referred 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*

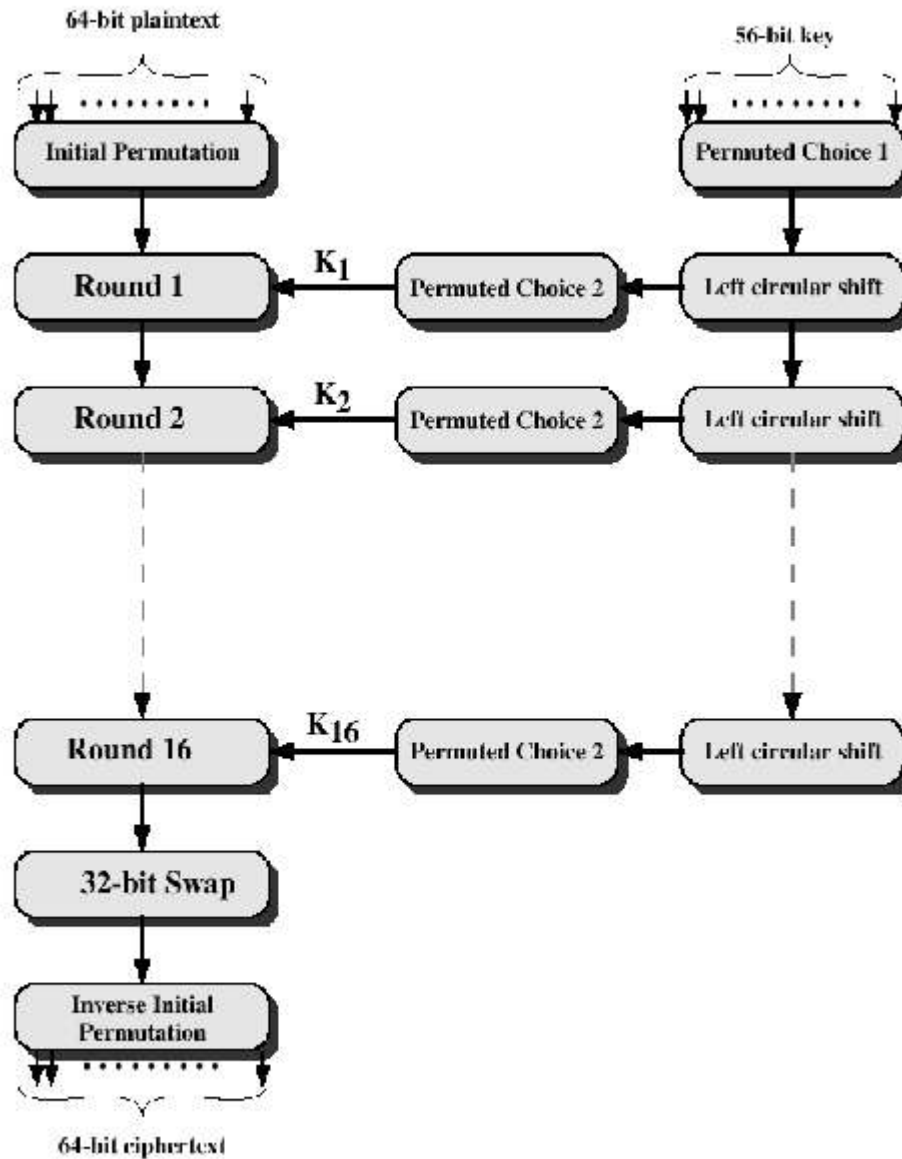


Figure 2.3 General Depiction of DES Encryption Algorithm

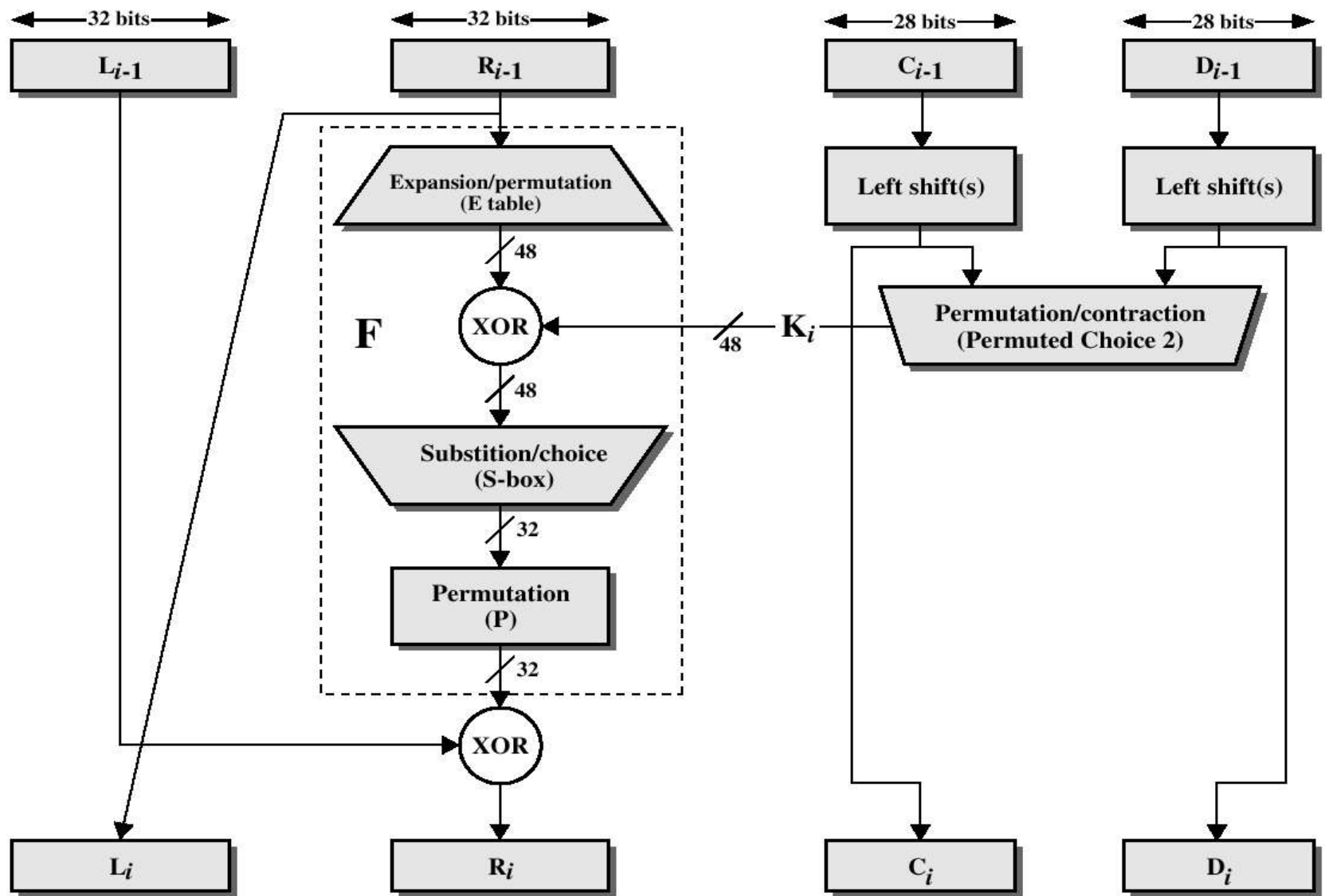
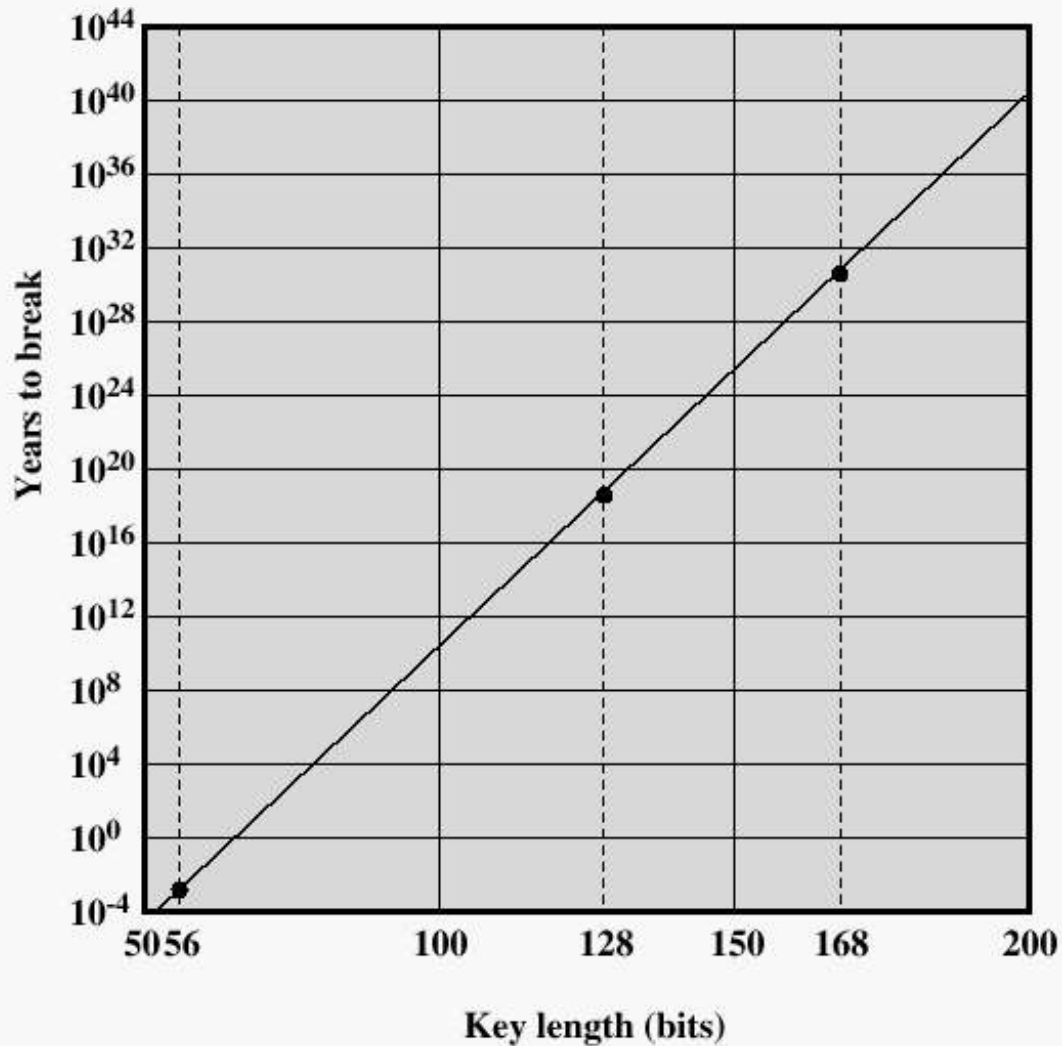


Figure 2.4 Single Round of DES Algorithm

DES

- *The overall processing at each iteration:*
 - $L_i = R_{i-1}$
 - $R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$
- *Concerns about:*
 - *The algorithm and the key length (56-bits)*

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



Triple DEA

- Use three keys and three executions of the DES algorithm (encrypt-decrypt-encrypt)

$$C = E_{K_3}[D_{K_2}[E_{K_1}[P]]]$$

- C = ciphertext
 - P = Plaintext
 - $E_{K}[X]$ = encryption of X using key K
 - $D_{K}[Y]$ = decryption of Y using key K
- Effective key length of 168 bits

Triple DEA

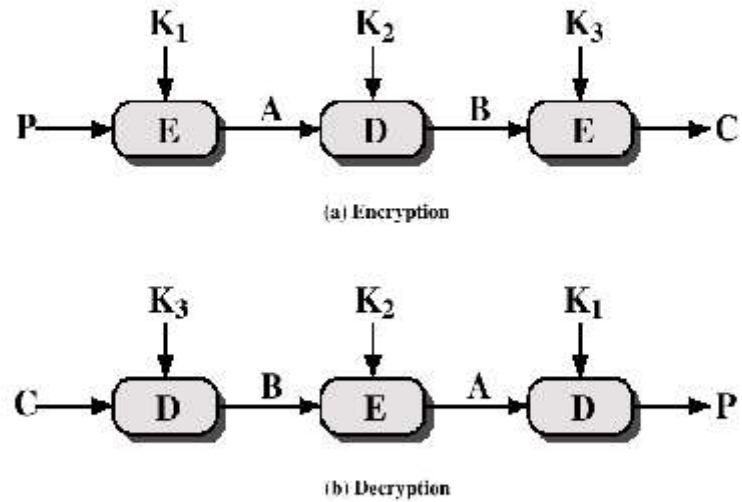


Figure 2.6 Triple DEA

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*

Cipher Block Modes of Operation

- *Cipher Block Chaining Mode (CBC)*
 - *The input to the encryption algorithm is the XOR of the current plaintext block and the preceding ciphertext block.*
 - *Repeating pattern of 64-bits are not exposed*

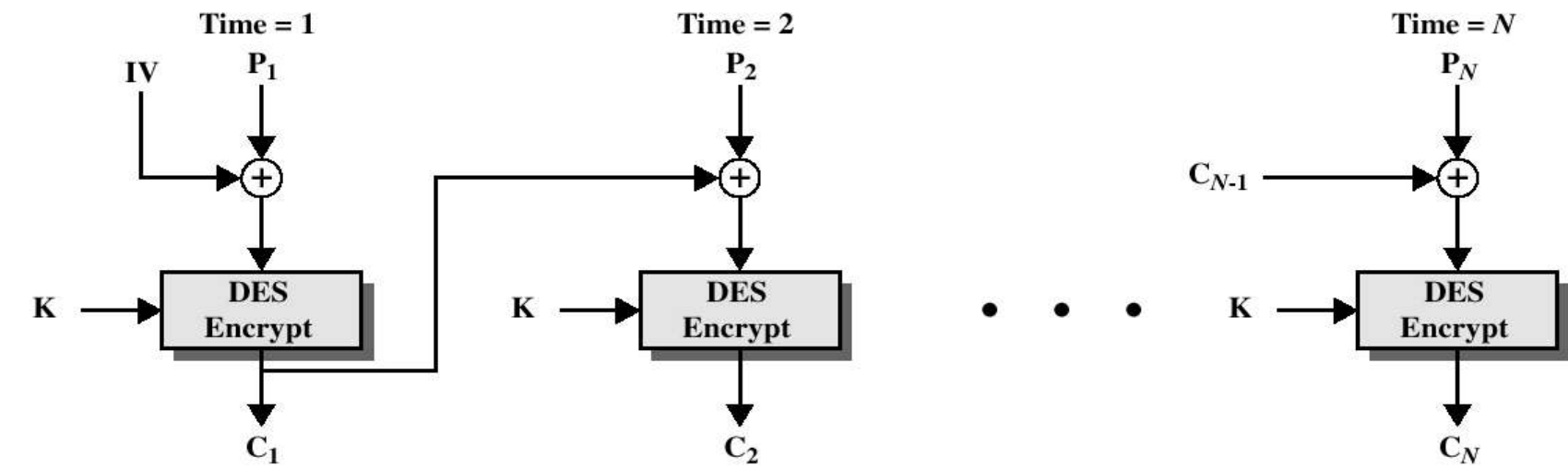
$$C_i = E_k [C_{i-1} \oplus P_i]$$

$$D_K [C_i] = D_K [E_K (C_{i-1} \oplus P_i)]$$

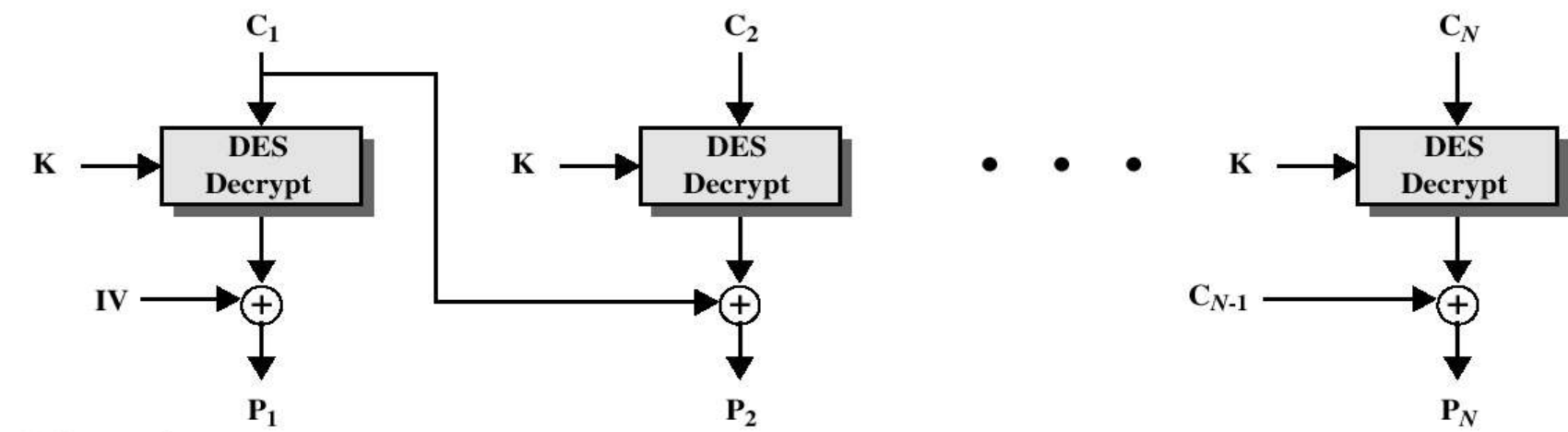
$$D_K [C_i] = (C_{i-1} \oplus P_i)$$

$$C_{i-1} \oplus D_K [C_i] = C_{i-1} \oplus (C_{i-1} \oplus P_i) = P_i$$

Henric Johnson



(a) Encryption



(b) Decryption

Figure 2.7 Cipher Block Chaining (CBC) Mode

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)*

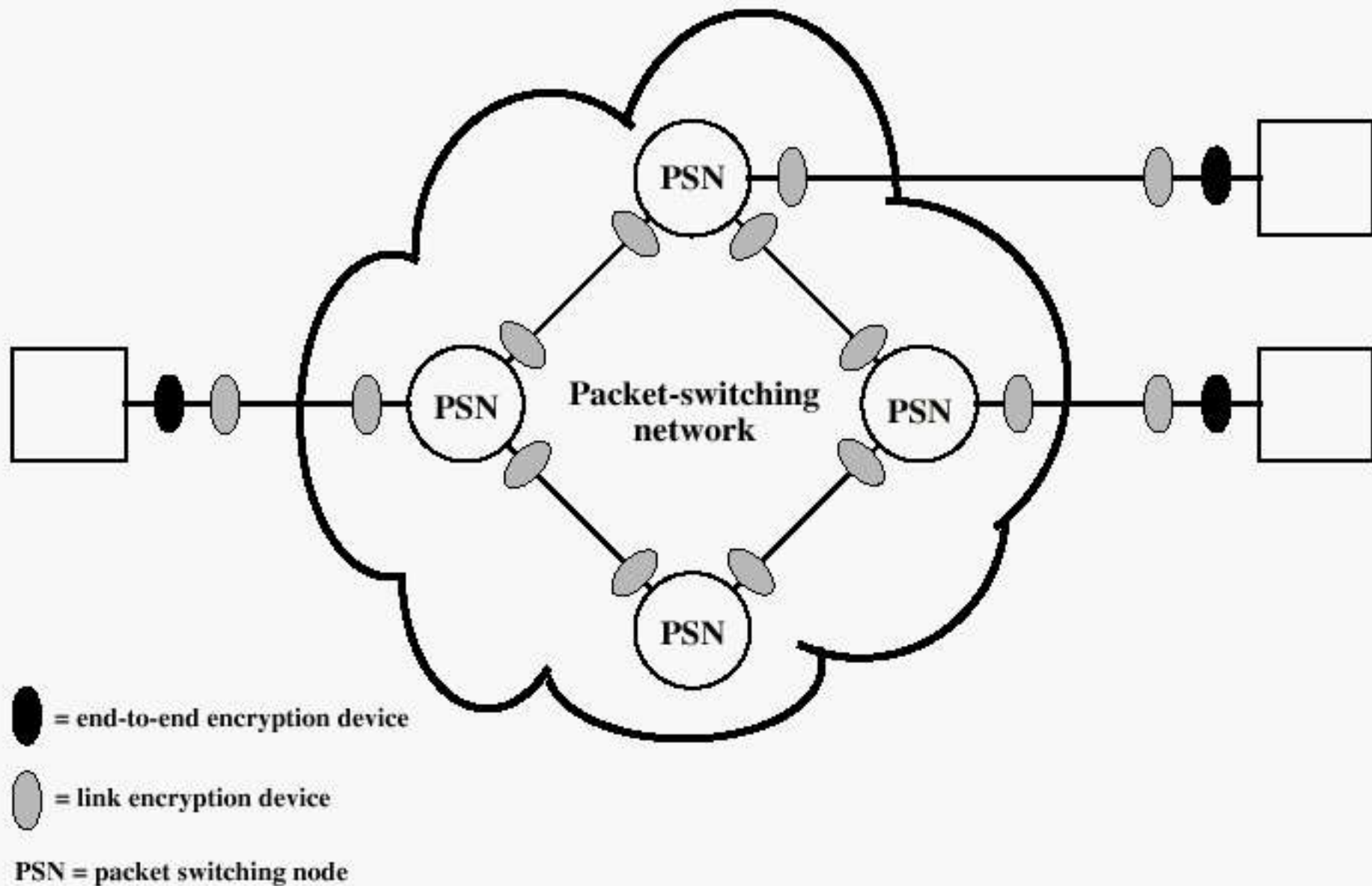


Figure 2.9 Encryption Across a Packet-Switching Network

Key Distribution

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

Key Distribution (See Figure 2.10)

- *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*

1. Host sends packet requesting connection
2. Front end buffers packet; asks KDC for session key
3. KDC distributes session key to both front ends
4. Buffered packet transmitted

FEP = front end processor
KDC = key distribution center

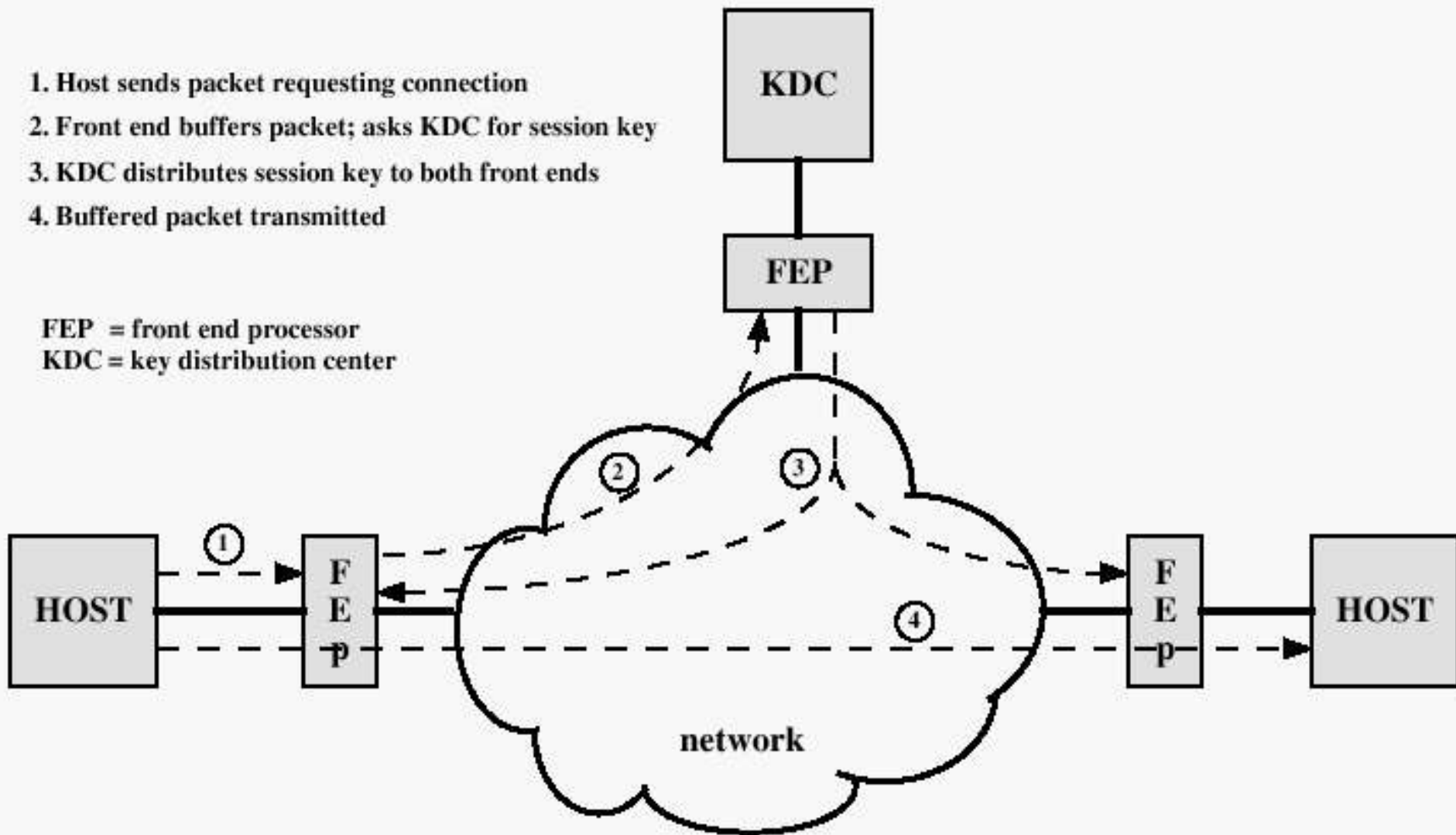


Figure 2.10 Automatic Key Distribution for Connection-Oriented Protocol

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*