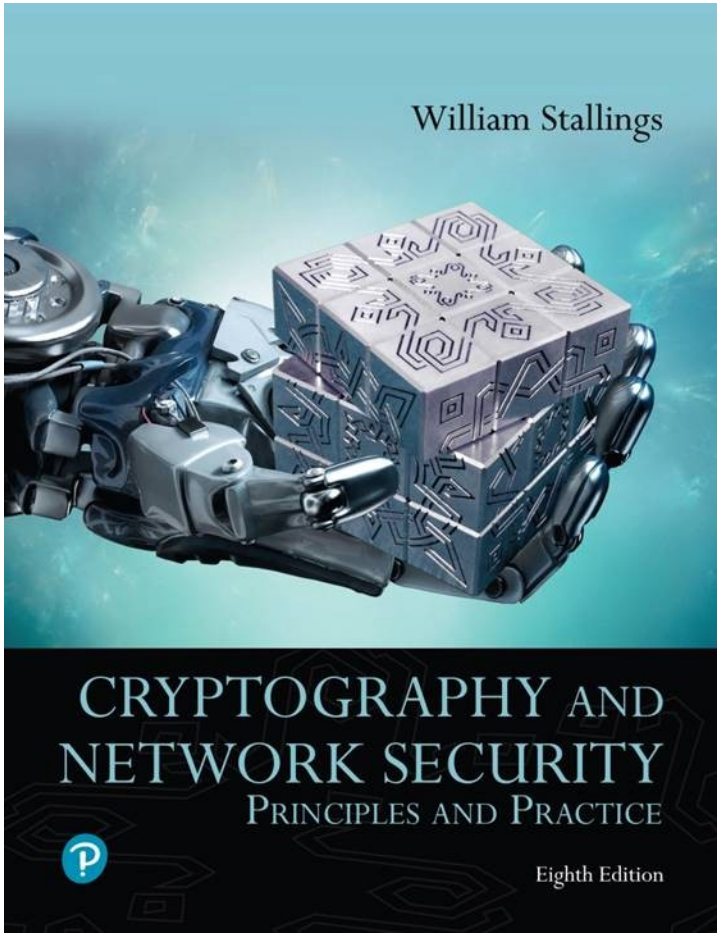
Cryptography and Network Security: Principles and Practice

Eighth Edition



Chapter 4

Block Ciphers and the Data Encryption Standard

Stream Cipher (1 of 2)

- Encrypts a digital data stream one bit or one byte at a time.
  - Examples:
    - Autokeyed Vigenère cipher
    - Vernam cipher
- In the ideal case, a one-time pad version of the Vernam cipher would be used, in which the key stream is as long as the plaintext bit stream.
  - If the cryptographic keystream is random, then this cipher is unbreakable by any means other than acquiring the key stream.
    - Key stream must be provided to both users in advance via some independent and secure channel
    - This introduces insurmountable logistical problems if the intended data traffic is very large

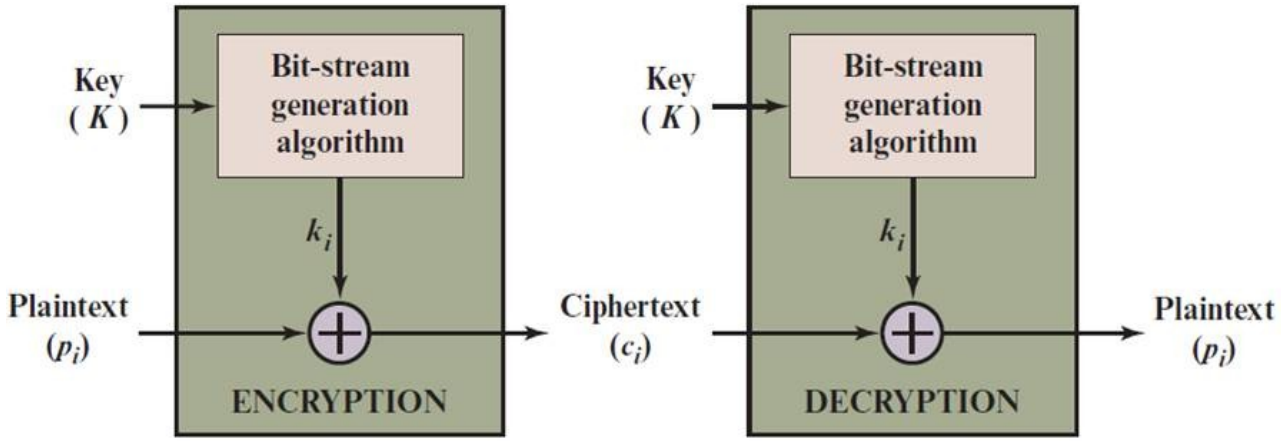
Stream Cipher (2 of 2)

- For practical reasons, the bit-stream generator must be implemented as an algorithmic procedure so that the cryptographic bit stream can be produced by both users.
  - It must be computationally impractical to predict future portions of the bit stream based on previous portions of the bit stream.
  - The two users need only share the generating key and each can produce the key stream..

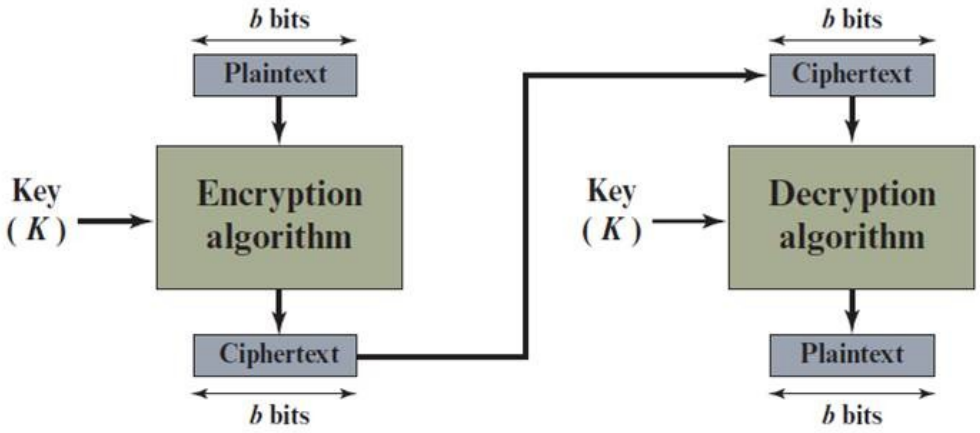
Block Cipher

- A block of plaintext is treated as a whole and used to produce a ciphertext block of equal length
- Typically, a block size of 64 or 128 bits is used
- As with a stream cipher, the two users share a symmetric encryption key.
- Most network-based symmetric cryptographic applications make use of block ciphers.

Figure 4.1 Stream Cipher and Block Cipher



(a) Stream cipher using algorithmic bit-stream generator



(b) Block cipher

Note

A full-size key *n*-bit transposition cipher or a substitution block cipher can be modeled as a permutation, but their key sizes are different:

- **Transposition: the key is $\lceil \log_2 n! \rceil$ bits long.**
- **Substitution: the key is $\lceil \log_2 (2n)! \rceil$ bits long.**

Note

A partial-key cipher is a group under the composition operation if it is a subgroup of the corresponding full-size key cipher.

5.1.1 Substitution or Transposition

A modern block cipher can be designed to act as a substitution cipher or a transposition cipher.

Note

To be resistant to exhaustive-search attack, a modern block cipher needs to be designed as a substitution cipher.

Feistel Cipher

- Feistel proposed the use of a cipher that alternates substitutions and permutations
- Substitutions
  - Each plaintext element or group of elements is uniquely replaced by a corresponding ciphertext element or group of elements
- Permutation
  - No elements are added or deleted or replaced in the sequence, rather the order in which the elements appear in the sequence is changed
- Is a practical application of a proposal by Claude Shannon to develop a product cipher that alternates confusion and diffusion functions
- Is the structure used by many significant symmetric block ciphers currently in use

Diffusion and Confusion

- Terms introduced by Claude Shannon to capture the two basic building blocks for any cryptographic system
  - Shannon's concern was to thwart cryptanalysis based on statistical analysis
- **Diffusion**
  - The statistical structure of the plaintext is dissipated into long-range statistics of the ciphertext
  - This is achieved by having each plaintext digit affect the value of many ciphertext digits
- **Confusion**
  - Seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible
  - Even if the attacker can get some handle on the statistics of the ciphertext, the way in which the key was used to produce that ciphertext is so complex as to make it difficult to deduce the key

5.1.4 Continued

Diffusion

The idea of diffusion is to hide the relationship between the ciphertext and the plaintext.

Note

Diffusion hides the relationship between the ciphertext and the plaintext.

5.1.4 Continued

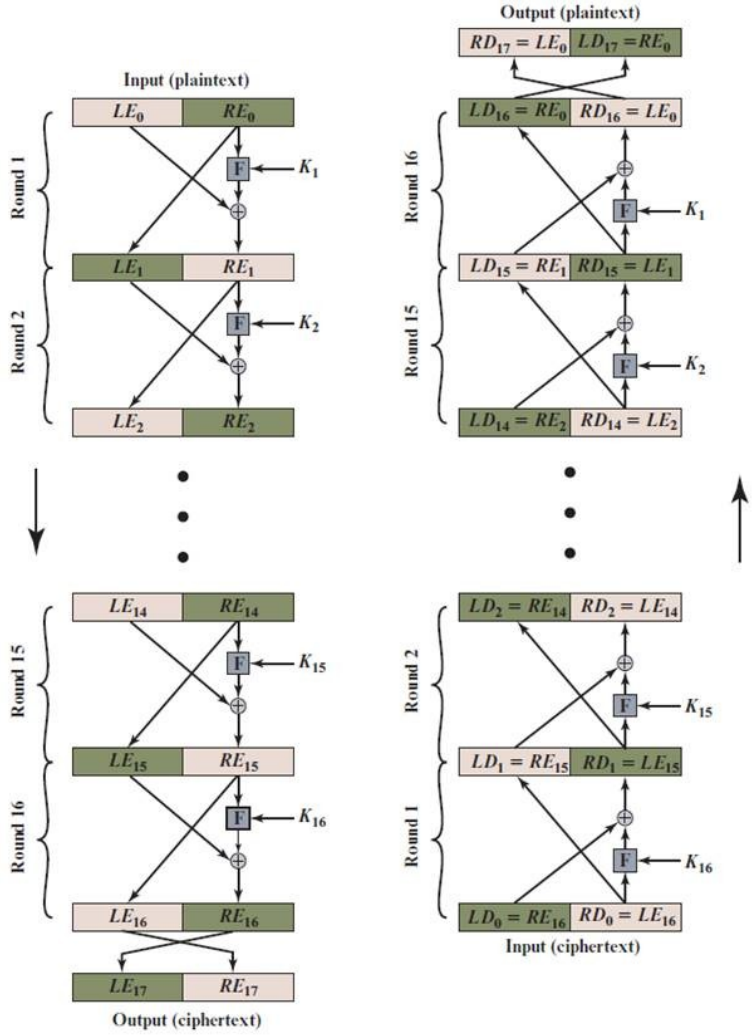
Confusion

The idea of confusion is to hide the relationship between the ciphertext and the key.

Note

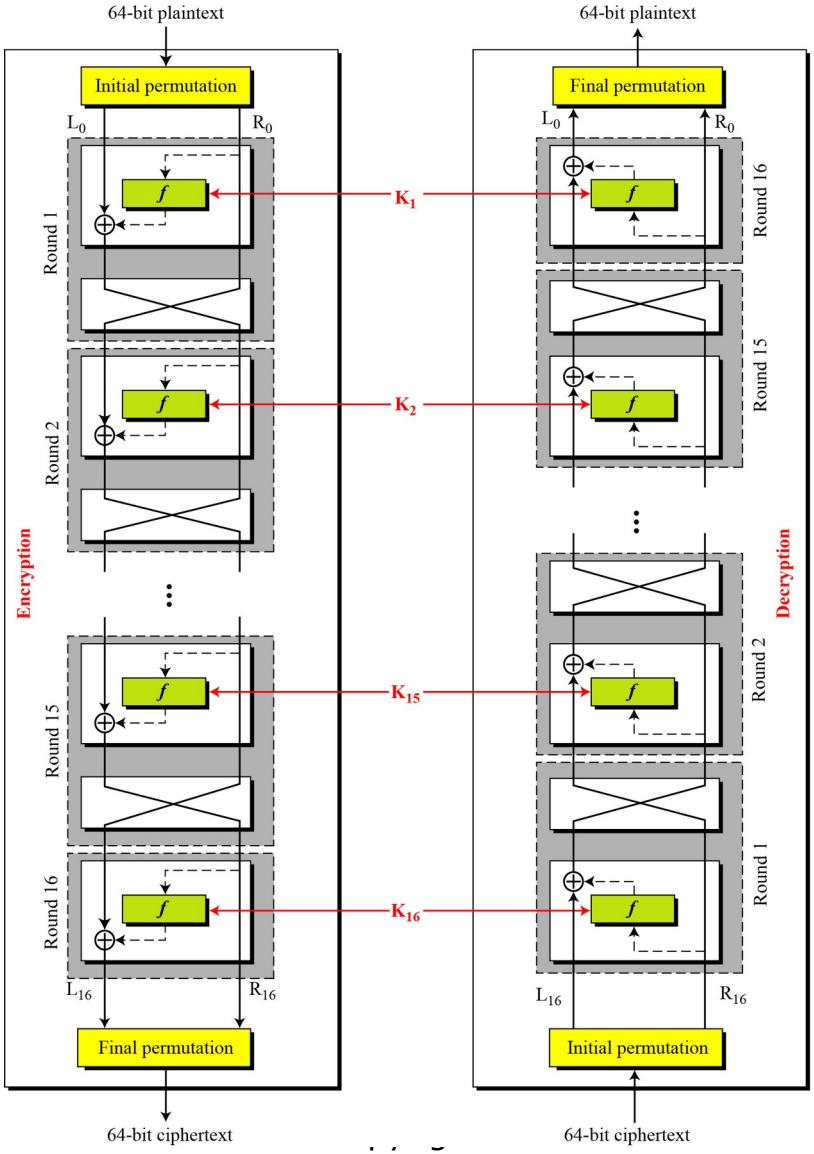
Confusion hides the relationship between the ciphertext and the key.

Figure 4.3 Feistel Encryption and Decryption (16 rounds)



6.2.3 Continued

Figure 6.9 *DES cipher and reverse cipher for the first approach*



6.2.2 Rounds

DES uses 16 rounds. Each round of DES is a Feistel cipher.

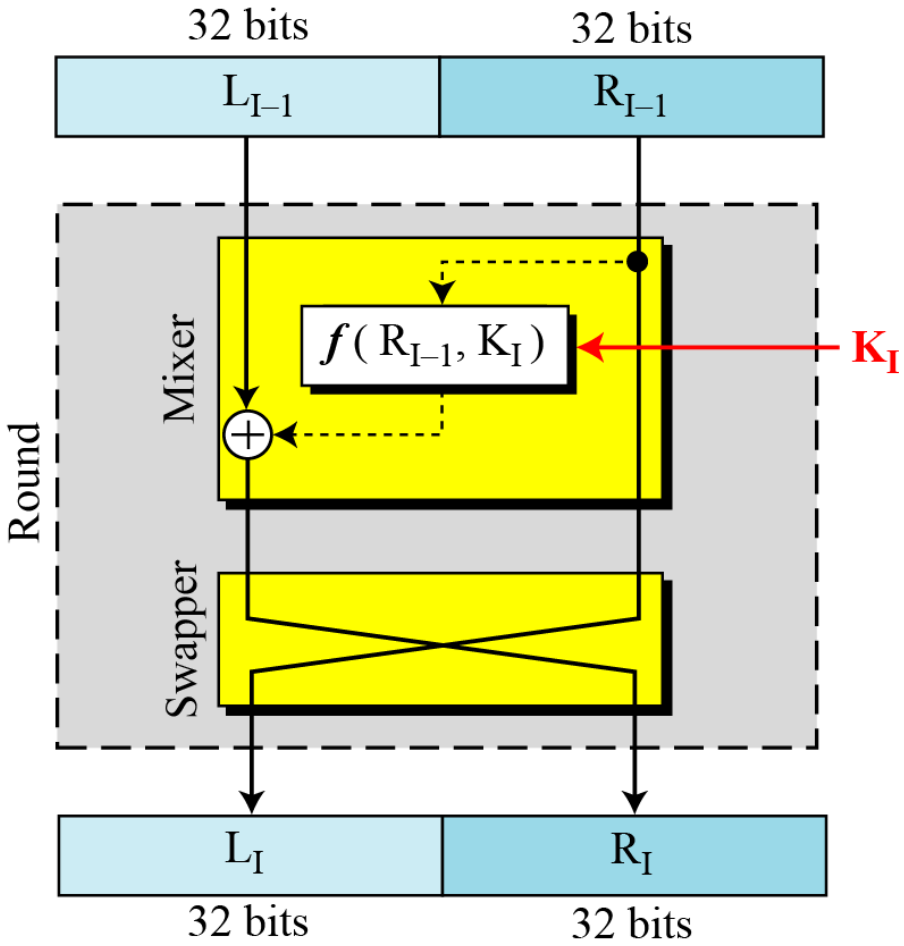
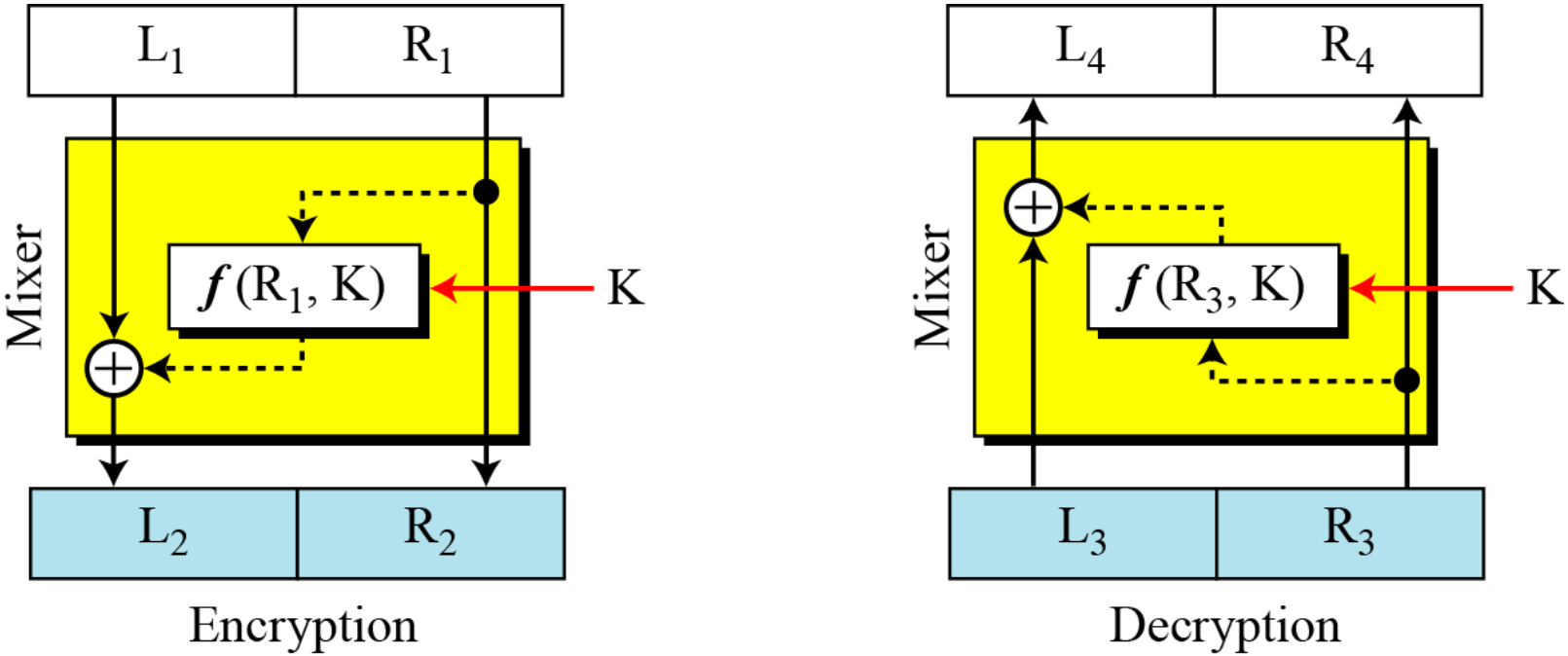


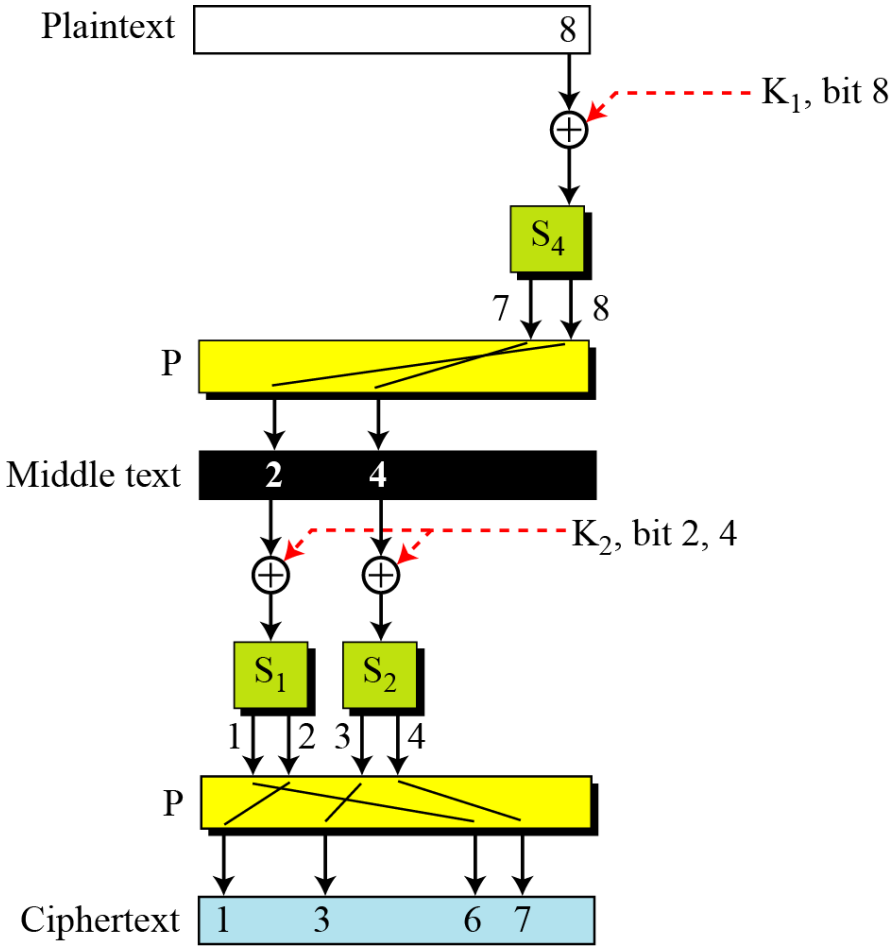
Figure 6.4
A round in DES (encryption site)

Figure *Improvement of the previous Feistel design*



Continued

Figure *Diffusion and confusion in a block cipher*



Feistel Cipher Design Features (1 of 2)

- Block size
  - Larger block sizes mean greater security but reduced encryption/decryption speed for a given algorithm
- Key size
  - Larger key size means greater security but may decrease encryption/decryption speeds
- Number of rounds
  - The essence of the Feistel cipher is that a single round offers inadequate security but that multiple rounds offer increasing security
- Subkey generation algorithm
  - Greater complexity in this algorithm should lead to greater difficulty of cryptanalysis

Feistel Cipher Design Features (2 of 2)

- Round function F
  - Greater complexity generally means greater resistance to cryptanalysis
- Fast software encryption/decryption
  - In many cases, encrypting is embedded in applications or utility functions in such a way as to preclude a hardware implementation; accordingly, the speed of execution of the algorithm becomes a concern
- Ease of analysis
  - If the algorithm can be concisely and clearly explained, it is easier to analyze that algorithm for cryptanalytic vulnerabilities and therefore develop a higher level of assurance as to its strength

Data Encryption Standard (DES)

- Issued in 1977 by the National Bureau of Standards (now NIST) as Federal Information Processing Standard 46
- Was the most widely used encryption scheme until the introduction of the Advanced Encryption Standard (AES) in 2001
- Algorithm itself is referred to as the Data Encryption Algorithm (DEA)
  - Data are encrypted in 64-bit blocks using a 56-bit key
  - The algorithm transforms 64-bit input in a series of steps into a 64-bit output
  - The same steps, with the same key, are used to reverse the encryption

Figure 4.5 General Depiction of DES Encryption Algorithm

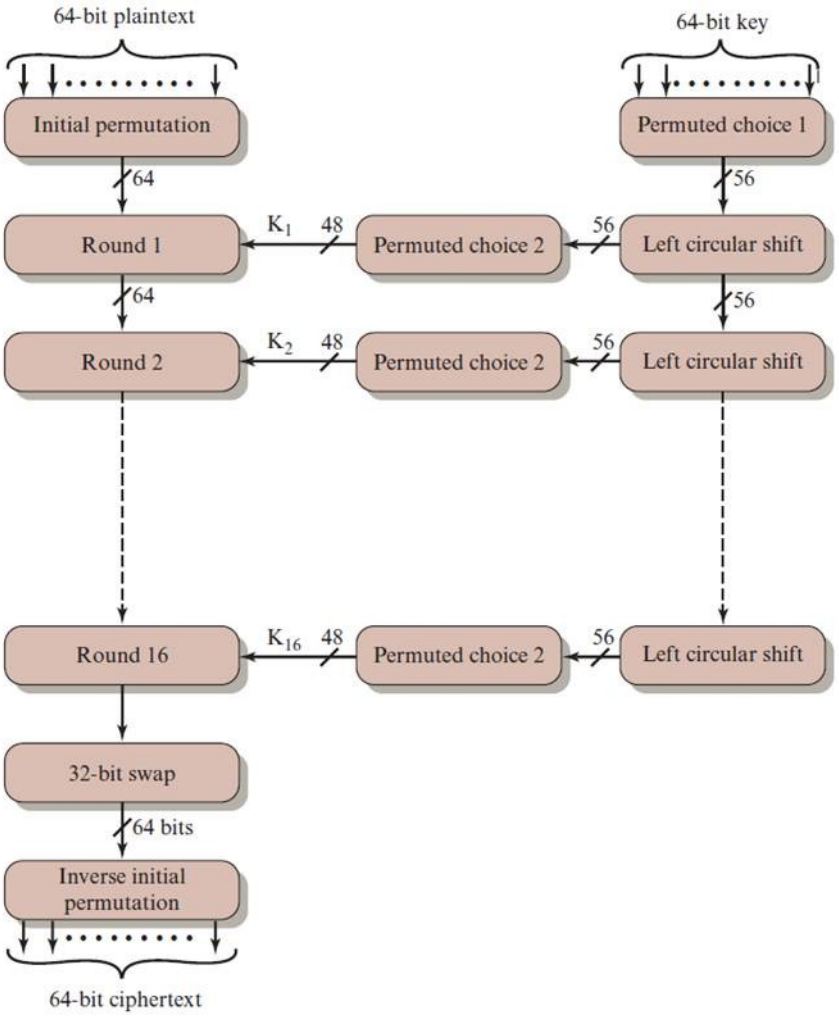
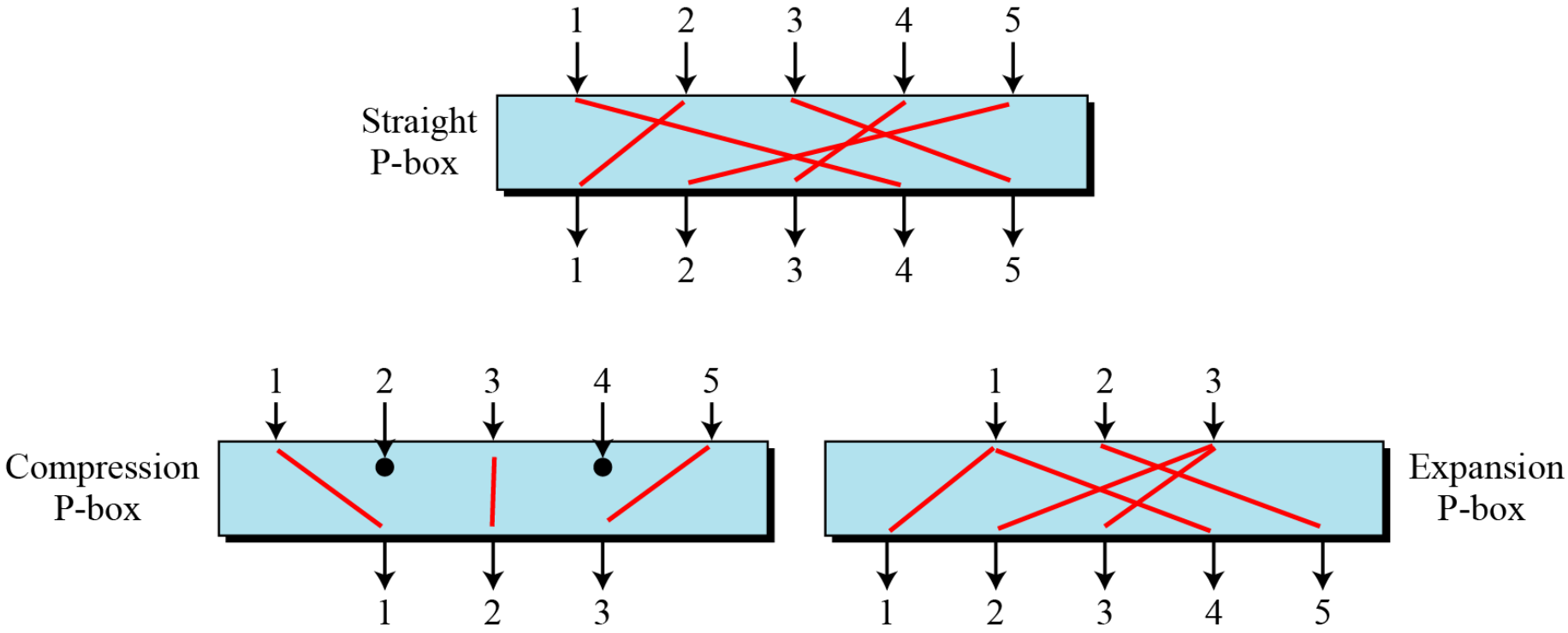


Figure 5.4 *Three types of P-boxes*



5.1.3 Continued

P-Boxes: Invertibility

Note

A straight P-box is invertible, but compression and expansion P-boxes are not.

5.1.3 Continued

Example 5.7

Figure 5.6 shows how to invert a permutation table represented as a one-dimensional table.

Figure 5.6 *Inverting a permutation table*

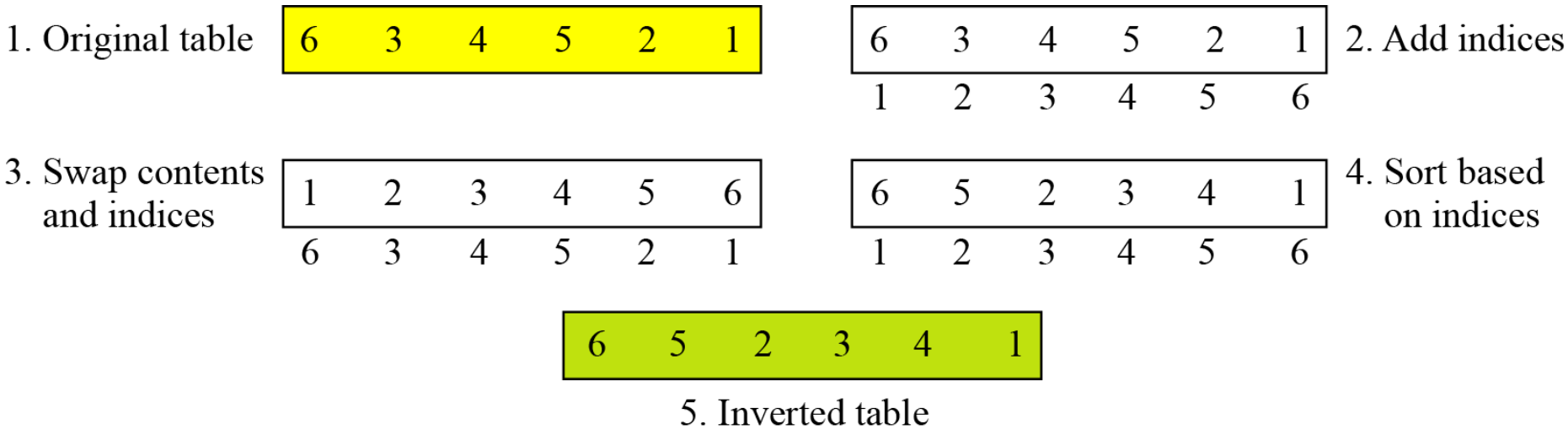
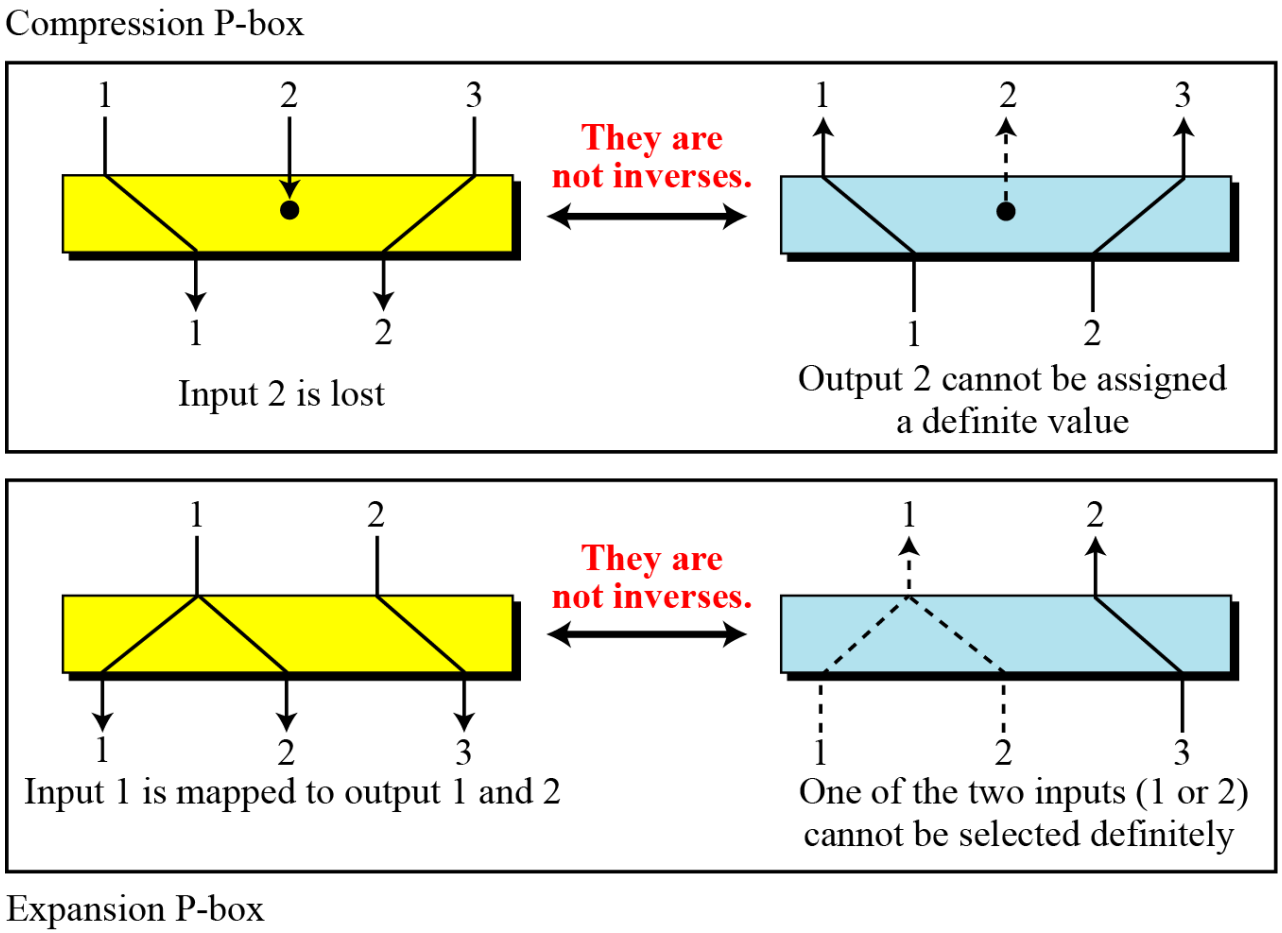


Figure 5.7 *Compression and expansion P-boxes are non-invertible*



5.1.3 Continued

S-Box

An S-box (substitution box) can be thought of as a miniature substitution cipher.

Note

An S-box is an $m \times n$ substitution unit, where m and n are not necessarily the same.

5.1.4 Product Ciphers

Shannon introduced the concept of a product cipher. A product cipher is a complex cipher combining substitution, permutation, and other components discussed in previous sections.

Table 4.5 Average Time Required for Exhaustive Key Search

Key Size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 Decryptions/s	Time Required at 10^{13} Decryptions/s
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	2^{55} ns = 1.125 years	1 hour
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	2^{127} ns = 5.3×10^{21} years	5.3×10^{17} years
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	2^{167} ns = 5.8×10^{33} years	5.8×10^{29} years
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	2^{191} ns = 9.8×10^{40} years	9.8×10^{36} years
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	2^{255} ns = 1.8×10^{60} years	1.8×10^{56} years
26 characters (permutation)	Monoalphabetic	$2! = 4 \times 10^{26}$	2×10^{26} ns = 6.3×10^{9} years	6.3×10^{6} years

5.1.5 Two Classes of Product Ciphers

Modern block ciphers are all product ciphers, but they are divided into two classes.

1. ***Feistel ciphers***

2. ***Non-Feistel ciphers***

5.1.5 Continued

Feistel Ciphers

Feistel designed a very intelligent and interesting cipher that has been used for decades. A Feistel cipher can have three types of components: self-invertible, invertible, and noninvertible.

Self-invertible Feistel cipher.
Example: 1010⊕1100 = 0110 and 0110⊕1100 = 1010.
Invertible Feistel cipher.
Example: product cipher.

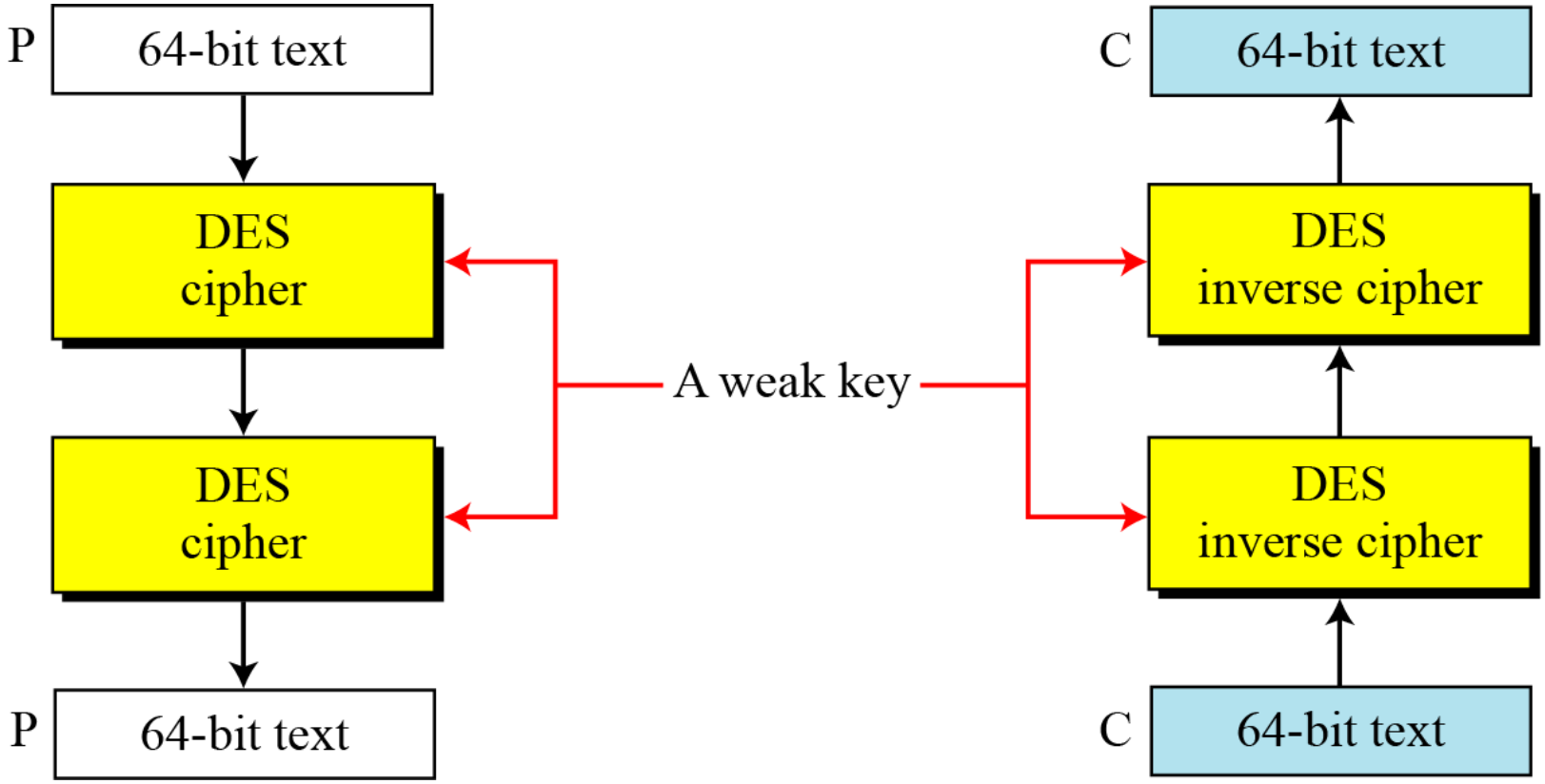
5.1.5 Continued

Non-Feistel Ciphers

A non-Feistel cipher uses only invertible components. A component in the encryption cipher has the corresponding component in the decryption cipher.

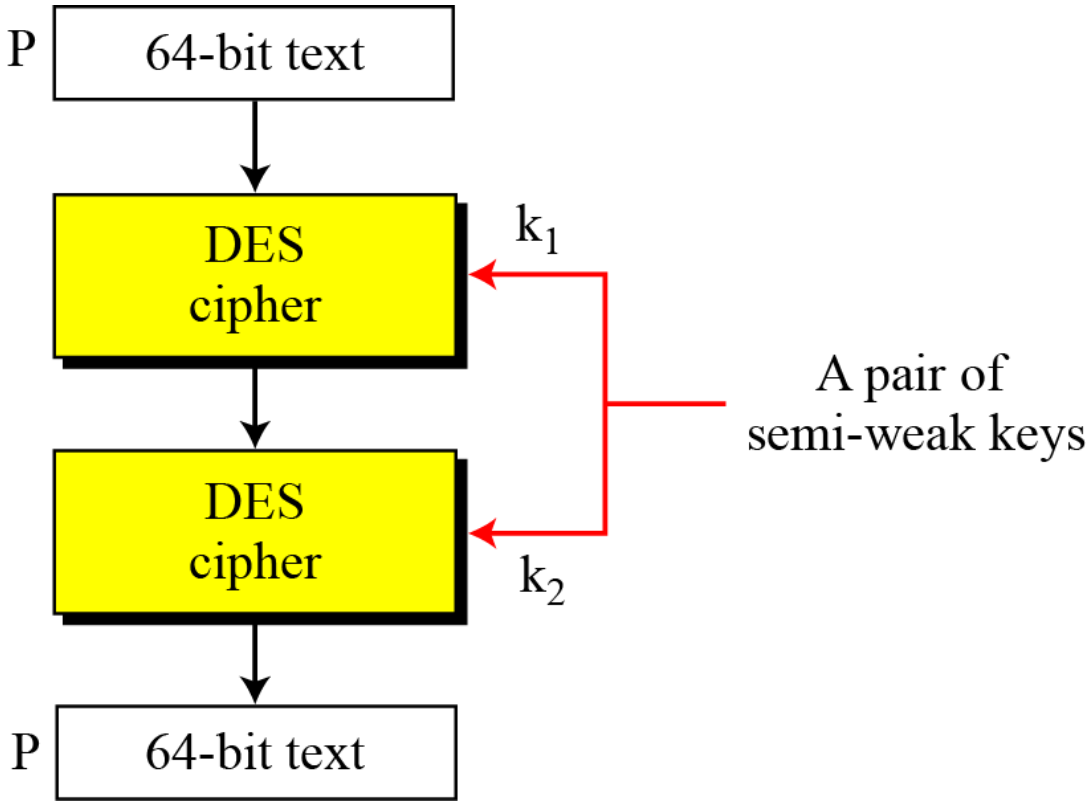
6.3.3 Continued

Figure 6.11 *Double encryption and decryption with a weak key*



6.3.3 Continued

Figure 6.12 *A pair of semi-weak keys in encryption and decryption*



6-4 Multiple DES

The major criticism of DES regards its key length. Fortunately DES is not a group. This means that we can use double or triple DES to increase the key size.

Topics discussed in this section:

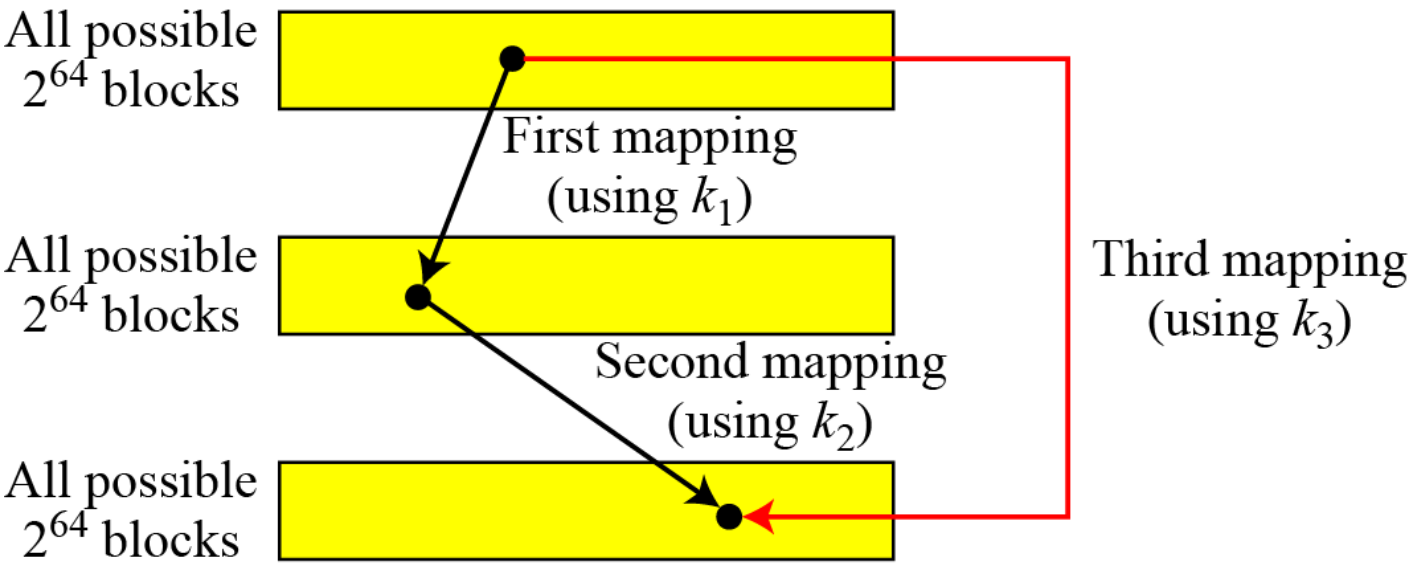
6.4.1 Double DES

6.4.4 Triple DES

6-4 Continued

A substitution that maps every possible input to every possible output is a group.

Figure 6.13 *Composition of mapping*



6.4.1 Double DES

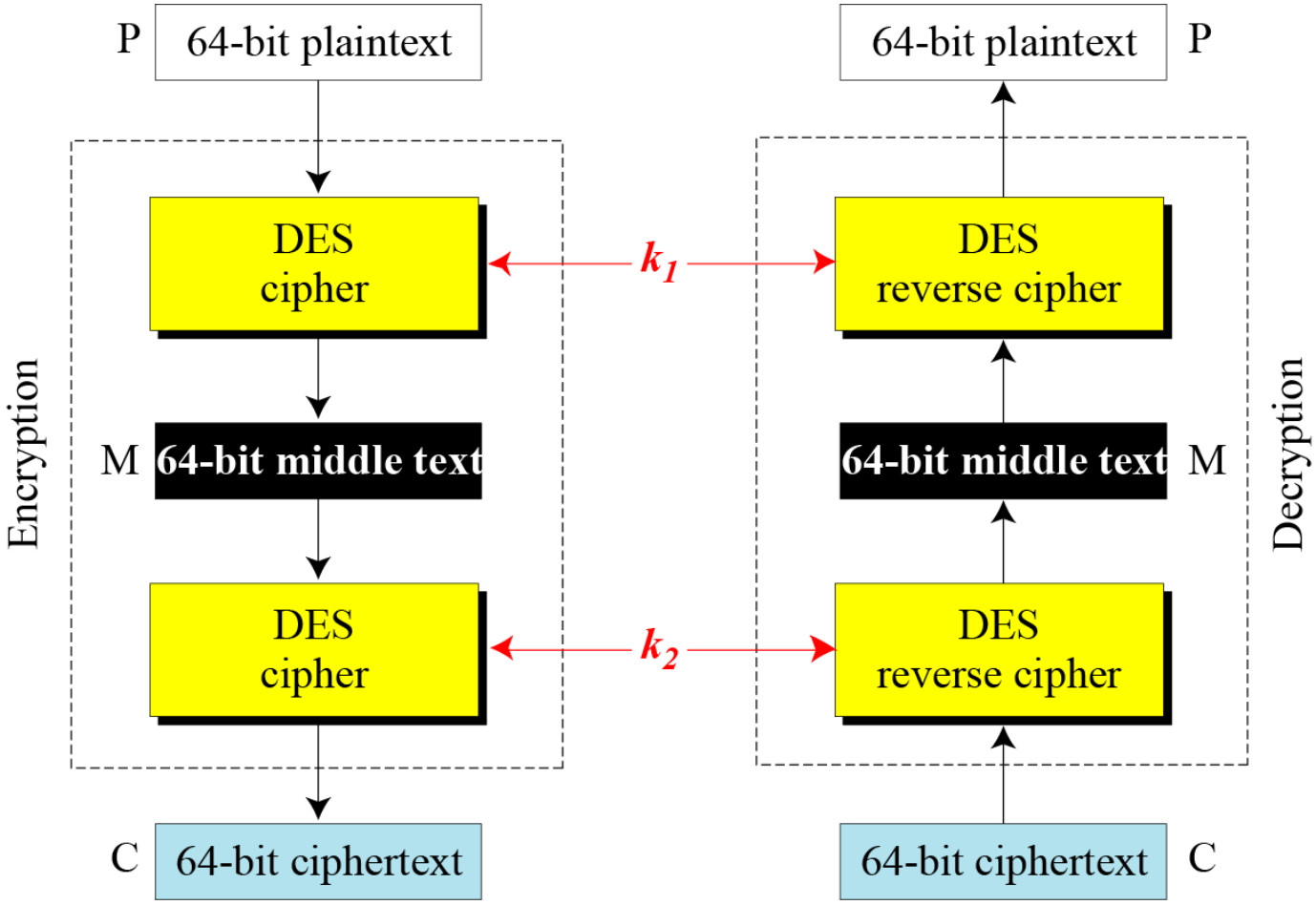
The first approach is to use double DES (2DES).

Meet-in-the-Middle Attack

However, using a known-plaintext attack called meet-in-the-middle attack proves that double DES improves this vulnerability slightly (to 2^{57} tests), but not tremendously (to 2^{112}).

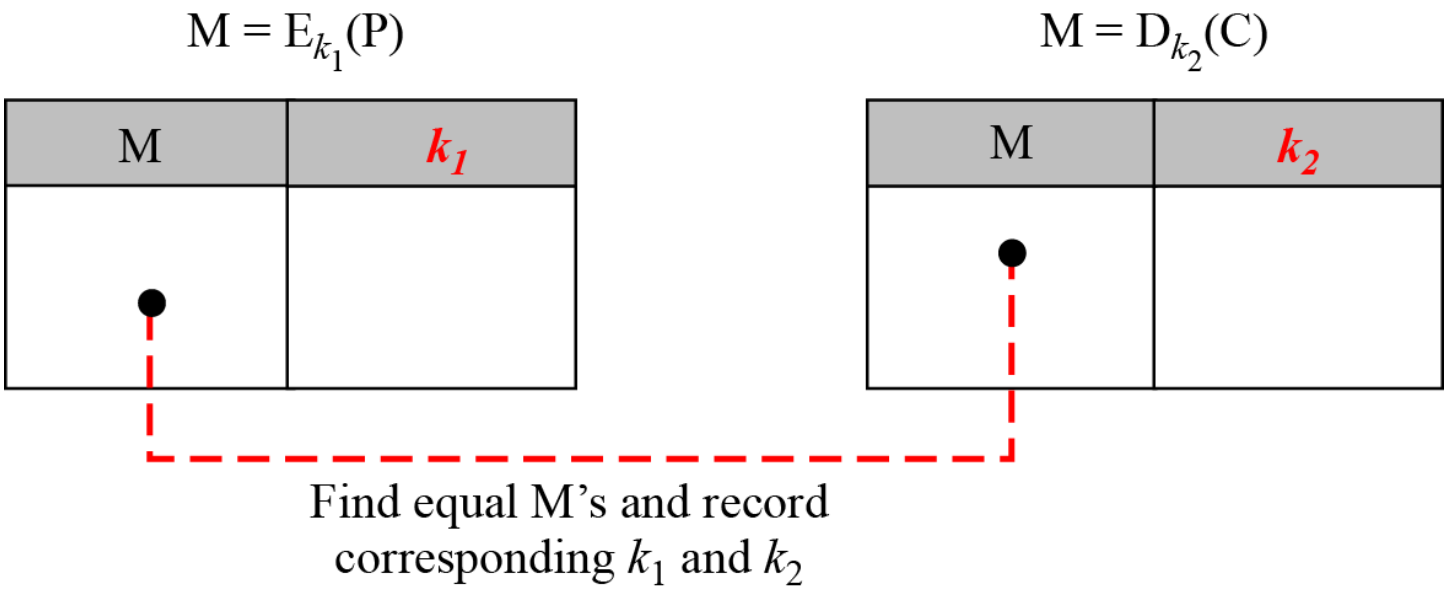
6.4.1 Continued

Figure 6.14 *Meet-in-the-middle attack for double DES*



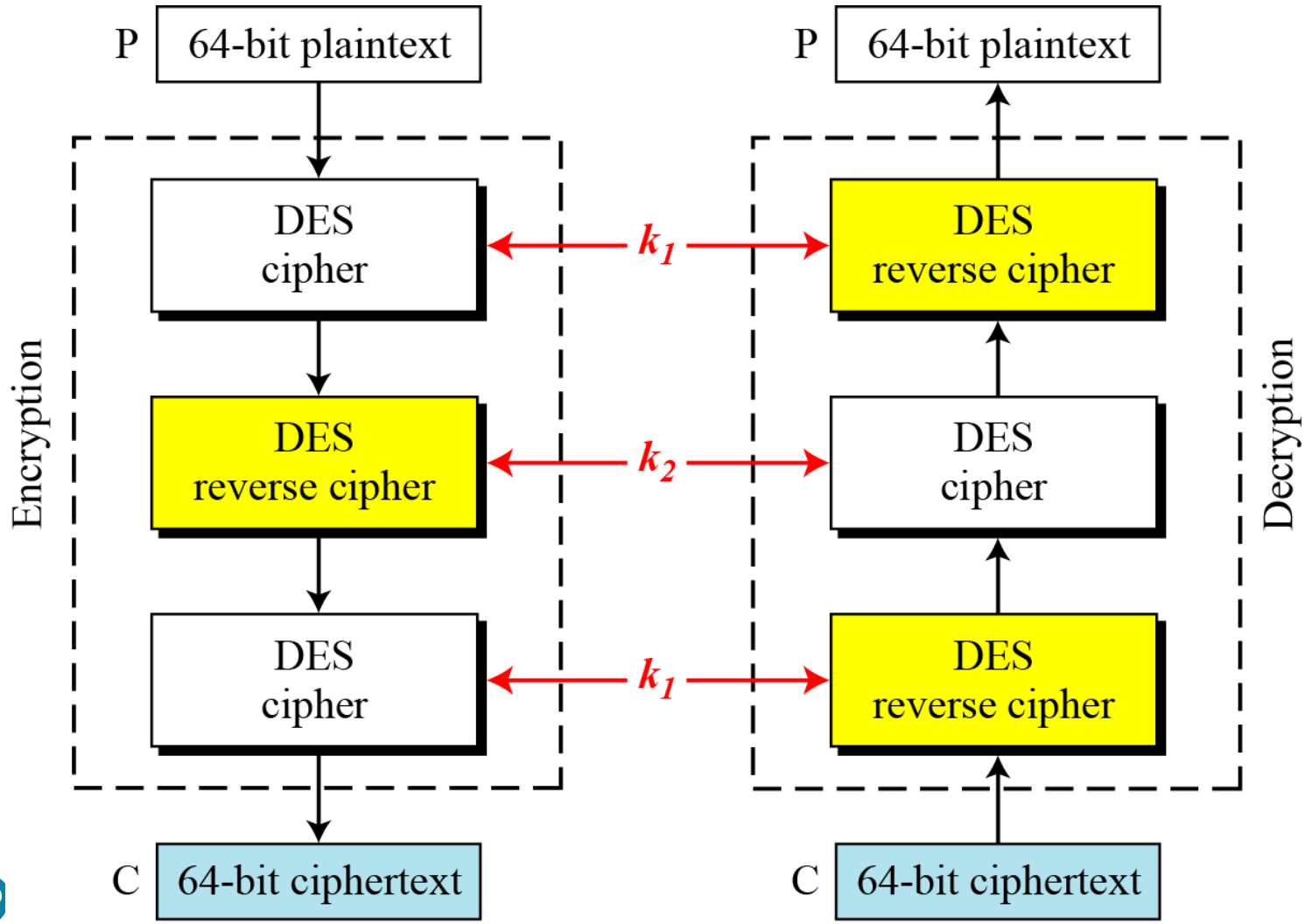
6.4.1 Continued

Figure 6.15 *Tables for meet-in-the-middle attack*



6.4.2 Triple DES

Figure 6.16 *Triple DES with two keys*



6.4.2 Continuous

Triple DES with Three Keys

The possibility of known-plaintext attacks on triple DES with two keys has enticed some applications to use triple DES with three keys. Triple DES with three keys is used by many applications such as PGP (See Chapter 16).

6-5 Security of DES

DES, as the first important block cipher, has gone through much scrutiny. Among the attempted attacks, three are of interest: brute-force, differential cryptanalysis, and linear cryptanalysis.

Topics discussed in this section:

6.5.1 Brute-Force Attack

We have discussed the weakness of short cipher key in DES. Combining this weakness with the key complement weakness, it is clear that DES can be broken using 2^{55} encryptions.

6.5.2 Differential Cryptanalysis

It has been revealed that the designers of DES already knew about this type of attack and designed S-boxes and chose 16 as the number of rounds to make DES specifically resistant to this type of attack.

Note

We show an example of DES differential cryptanalysis in Appendix N.

6.5.3 Linear Cryptanalysis

Linear cryptanalysis is newer than differential cryptanalysis. DES is more vulnerable to linear cryptanalysis than to differential cryptanalysis. S-boxes are not very resistant to linear cryptanalysis. It has been shown that DES can be broken using 2^{43} pairs of known plaintexts. However, from the practical point of view, finding so many pairs is very unlikely.

Note

We show an example of DES linear cryptanalysis in Appendix N.

Summary

- Explain the concept of the avalanche effect
- Discuss the cryptographic strength of DES
- Summarize the principal block cipher design principles
- Understand the distinction between stream ciphers and block ciphers
- Present an overview of the Feistel cipher and explain how decryption is the inverse of encryption
- Present an overview of Data Encryption Standard (DES)

Copyright