Chapter 5

Introduction to Modern Symmetric-key Ciphers

Chapter 5
Objectives

- ❑ To distinguish between traditional and modern symmetric-key ciphers.
- ❑ To introduce modern block ciphers and discuss their characteristics.
- ❑ To explain why modern block ciphers need to be designed as substitution ciphers.
- ❑ To introduce components of block ciphers such as P-boxes and S-boxes.

Chapter 5
Objectives (Continued)

- ❑ To discuss product ciphers and distinguish between two classes of product ciphers: Feistel and non-Feistel ciphers.
- ❑ To discuss two kinds of attacks particularly designed for modern block ciphers: differential and linear cryptanalysis.
- ❑ To introduce stream ciphers and to distinguish between synchronous and nonsynchronous stream ciphers.
- ❑ To discuss linear and nonlinear feedback shift registers for implementing stream ciphers.

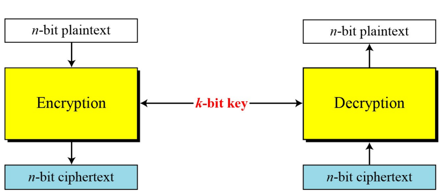
5-1 MODERN BLOCK CIPHERS

A symmetric-key modern block cipher encrypts an n-bit block of plaintext or decrypts an n-bit block of ciphertext. The encryption or decryption algorithm uses a k-bit key.

Topics discussed in this section:

5.1 Continued

Figure 5.1 *A modern block cipher*



5.1 Continued

Example 5.1

How many padding bits must be added to a message of 100 characters if 8-bit ASCII is used for encoding and the block cipher accepts blocks of 64 bits?

Solution

Encoding 100 characters using 8-bit ASCII results in an 800-bit message. The plaintext must be divisible by 64. If | M | and |Pad| are the length of the message and the length of the padding,

$$|M| + |Pad| = 0 \bmod 64 \quad \rightarrow \quad |Pad| = -800 \bmod 64 \quad \rightarrow \quad 32 \bmod 64$$

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.

5.1.1 Continued

Example 5.2

Suppose that we have a block cipher where $n = 64$. If there are 10 1's in the ciphertext, how many trial-and-error tests does Eve need to do to recover the plaintext from the intercepted ciphertext in each of the following cases?

a. The cipher is designed as a substitution cipher.
b. The cipher is designed as a transposition cipher.

Solution

a. In the first case, Eve has no idea how many 1's are in the plaintext. Eve needs to try all possible 2^{64} 64-bit blocks to find one that makes sense.

b. In the second case, Eve knows that there are exactly 10 1's in the plaintext. Eve can launch an exhaustive-search attack using only those 64-bit blocks that have exactly 10 1's.

5.1.2 Block Ciphers as Permutation Groups

Is a modern block cipher a group?

Full-Size Key Transposition Block Ciphers

In a full-size key transposition cipher We need to have n! possible keys, so the key should have $\lceil \log_2 n! \rceil$ bits.

Example 5.3

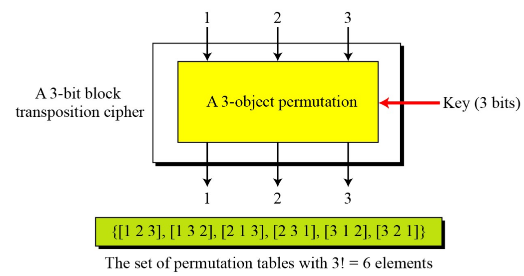
Show the model and the set of permutation tables for a 3-bit block transposition cipher where the block size is 3 bits.

Solution

The set of permutation tables has 3! = 6 elements, as shown in Figure 5.2.

5.1.2 Continued

Figure 5.2 *A transposition block cipher modeled as a permutation*



5.1.2 Continued

Full-Size Key Substitution Block Ciphers

A full-size key substitution cipher does not transpose bits; it substitutes bits. We can model the substitution cipher as a permutation if we can decode the input and encode the output.

Example 5.4

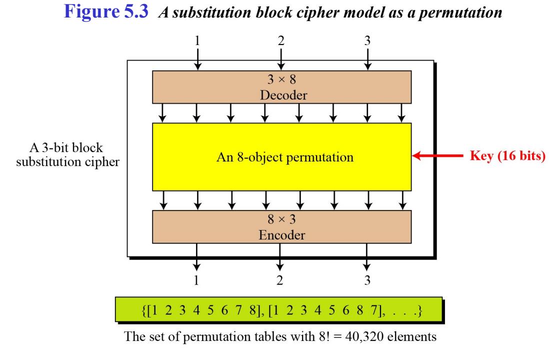
Show the model and the set of permutation tables for a 3-bit block substitution cipher.

Solution

Figure 5.3 shows the model and the set of permutation tables. The key is also much longer, $\lceil \log_2 40{,}320 \rceil = 16$ bits.

5.1.2 Continued

Figure 5.3 *A substitution block cipher model as a permutation*



5.1.2 Continued

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 $\lceil \log_2 (2^n)! \rceil$ 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.

5.1.3 Components of a Modern Block Cipher

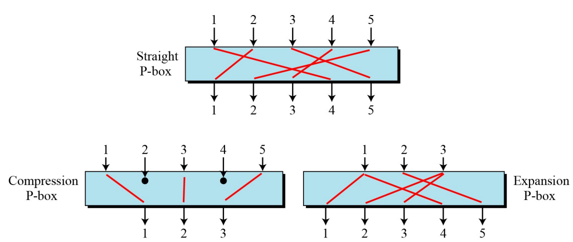
Modern block ciphers normally are keyed substitution ciphers in which the key allows only partial mappings from the possible inputs to the possible outputs.

P-Boxes

A P-box (permutation box) parallels the traditional transposition cipher for characters. It transposes bits.

5.1.3 Continued

Figure 5.4 ***Three types of P-boxes***

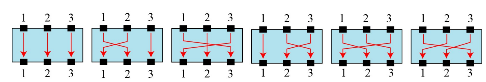


5.1.3 Continued

Example 5.5

Figure 5.5 shows all 6 possible mappings of a 3 × 3 P-box.

Figure 5.5 ***The possible mappings of a 3 × 3 P-box***



5.1.3 Continued

Straight P-Boxes

Table 5.1 ***Example of a permutation table for a straight P-box***

58	50	42	34	26	18	10	02	60	52	44	36	28	20	12	04
62	54	46	38	30	22	14	06	64	56	48	40	32	24	16	08
57	49	41	33	25	17	09	01	59	51	43	35	27	19	11	03
61	53	45	37	29	21	13	05	63	55	47	39	31	23	15	07

5.1.2 Continued

Example 5.6

Design an 8 × 8 permutation table for a straight P-box that moves the two middle bits (bits 4 and 5) in the input word to the two ends (bits 1 and 8) in the output words. Relative positions of other bits should not be changed.

Solution

We need a straight P-box with the table [4 1 2 3 6 7 8 5]. The relative positions of input bits 1, 2, 3, 6, 7, and 8 have not been changed, but the first output takes the fourth input and the eighth output takes the fifth input.

5.1.3 Continued

Compression P-Boxes

A compression P-box is a P-box with n inputs and m outputs where m < n.

Table 5.2 *Example of a 32 × 24 permutation table*

01	02	03	21	22	26	27	28	29	13	14	17
18	19	20	04	05	06	10	11	12	30	31	32

5.1.3 Continued

Compression P-Box

Table 5.2 *Example of a 32 × 24 permutation table*

01	02	03	21	22	26	27	28	29	13	14	17
18	19	20	04	05	06	10	11	12	30	31	32

5.1.3 Continued

Expansion P-Boxes

An expansion P-box is a P-box with n inputs and m outputs where m > n.

Table 5.3 *Example of a 12 × 16 permutation table*

01	09	10	11	12	01	02	03	03	04	05	06	07	08	09	12

5.1.3 Continued

P-Boxes: Invertibility

Note

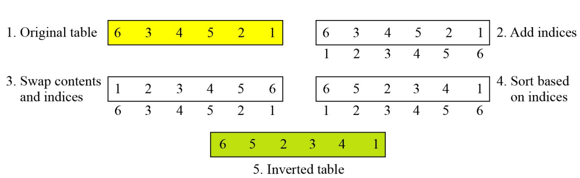
A straight P-box is invertible, but compression and expansion P-boxes are not.

5.1.3 Continued

Example 5.7

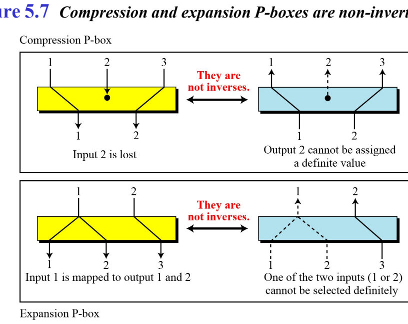
Figure 5.6 shows how to invert a permutation table represented as a one-dimensional table.

Figure 5.6 *Inverting a permutation table*



5.1.3 Continued

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.

5.1.3 Continued

Example 5.8

In an S-box with three inputs and two outputs, we have

$$y_1 = x_1 \oplus x_2 \oplus x_3 \qquad y_2 = x_1$$

The S-box is linear because $a_{1,1} = a_{1,2} = a_{1,3} = a_{2,1} = 1$ and $a_{2,2} = a_{2,3} = 0$. The relationship can be represented by matrices, as shown below:

$$\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

5.1.3 Continued

Example 5.9

In an S-box with three inputs and two outputs, we have

$$y_1 = (x_1)^3 + x_2 \qquad y_2 = (x_1)^2 + x_1x_2 + x_3$$

where multiplication and addition is in GF(2). The S-box is nonlinear because there is no linear relationship between the inputs and the outputs.

5.1.3 Continued

Example 5.10

The following table defines the input/output relationship for an S-box of size 3 × 2. The leftmost bit of the input defines the row; the two rightmost bits of the input define the column. The two output bits are values on the cross section of the selected row and column.

Leftmost bit

Rightmost bits

	00	01	10	11
0	00	10	01	11
1	10	00	11	01

Output bits

Based on the table, an input of 010 yields the output 01. An input of 101 yields the output of 00.

5.1.3 Continued

S-Boxes: Invertibility

An S-box may or may not be invertible. In an invertible S-box, the number of input bits should be the same as the number of output bits.

5.1.3 Continued

Example 5.11

Figure 5.8 shows an example of an invertible S-box. For example, if the input to the left box is 001, the output is 101. The input 101 in the right table creates the output 001, which shows that the two tables are inverses of each other.

Figure 5.8 *S-box tables for Example 5.11*

3 bits

	00	01	10	11
0	011	101	111	100
1	000	010	001	110

Table used for encryption

3 bits

3 bits

	00	01	10	11
0	100	110	101	000
1	011	001	111	010

Table used for decryption

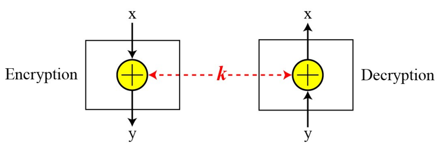
3 bits

5.1.3 Continued

Exclusive-Or

An important component in most block ciphers is the exclusive-or operation.

Figure 5.9 *Invertibility of the exclusive-or operation*



5.1.3 Continued

Exclusive-Or (Continued)

An important component in most block ciphers is the exclusive-or operation. As we discussed in Chapter 4, addition and subtraction operations in the GF(2^n) field are performed by a single operation called the exclusive-or (XOR).

The five properties of the exclusive-or operation in the GF(2n) field makes this operation a very interesting component for use in a block cipher: closure, associativity, commutativity, existence of identity, and existence of inverse.

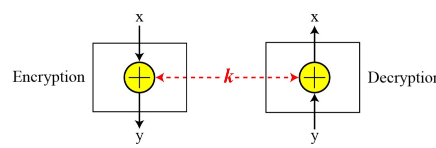
5.1.3 Continued

Exclusive-Or (Continued)

The inverse of a component in a cipher makes sense if the component represents a unary operation (one input and one output). For example, a keyless P-box or a keyless S-box can be made invertible because they have one input and one output. An exclusive operation is a binary operation. The inverse of an exclusive-or operation can make sense only if one of the inputs is fixed (is the same in encryption and decryption). For example, if one of the inputs is the key, which normally is the same in encryption and decryption, then an exclusive-or operation is self-invertible, as shown in Figure 5.9.

5.1.1 Continued

Figure 5.9 *Invertibility of the exclusive-or operation*

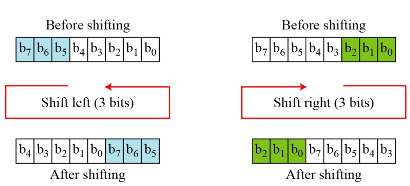


5.1.3 Continued

Circular Shift

Another component found in some modern block ciphers is the circular shift operation.

Figure 5.10 *Circular shifting an 8-bit word to the left or right*

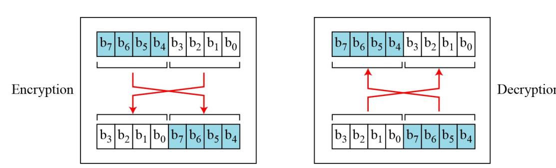


5.1.3 Continued

Swap

The swap operation is a special case of the circular shift operation where k = n/2.

Figure 5.11 *Swap operation on an 8-bit word*

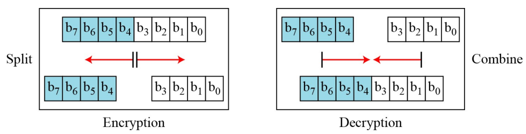


5.1.3 Continued

Split and Combine

Two other operations found in some block ciphers are split and combine.

Figure 5.12 ***Split and combine operations on an 8-bit word***



5.1.3 Continued

Figure 5.12 ***Split and combine operations on an 8-bit word***