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*

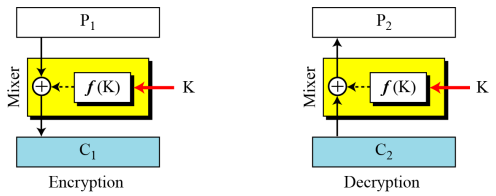
5.1.5 Continued

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.

5.1.5 Continued

Figure 5.15 *The first thought in Feistel cipher design*



Note

Diffusion hides the relationship between the ciphertext and the plaintext.

5.1.3 Continued

Example 5.12

This is a trivial example. The plaintext and ciphertext are each 4 bits long and the key is 3 bits long. Assume that the function takes the first and third bits of the key, interprets these two bits as a decimal number, squares the number, and interprets the result as a 4-bit binary pattern. Show the results of encryption and decryption if the original plaintext is 0111 and the key is 101.

Solution

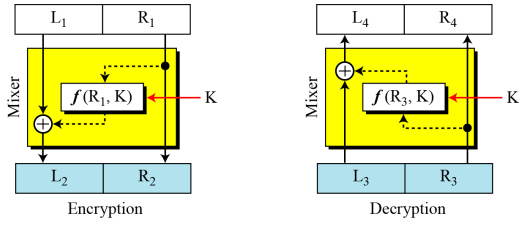
The function extracts the first and second bits to get 11 in binary or 3 in decimal. The result of squaring is 9, which is 1001 in binary.

Encryption: $C = P \oplus f(K) = 0111 \oplus 1001 = 1110$

Decryption: $P = C \oplus f(K) = 1110 \oplus 1001 = 0111$

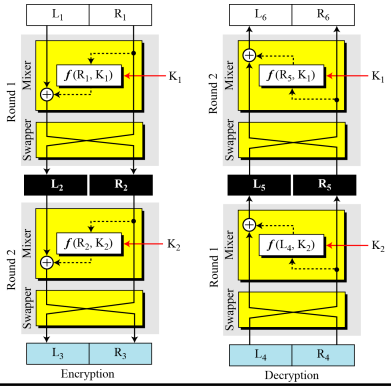
5.1.5 Continued

Figure 5.16 *Improvement of the previous Feistel design*



5.1.5 Continued

Figure 5.17 *Final design of a Feistel cipher with two rounds*



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.

5.51

5.1.6 Attacks on Block Ciphers

Attacks on traditional ciphers can also be used on modern block ciphers, but today's block ciphers resist most of the attacks discussed in Chapter 3.

5.52

5.1.5 Continued

Differential Cryptanalysis

Eli Biham and Adi Shamir introduced the idea of differential cryptanalysis. This is a chosen-plaintext attack.

5.53

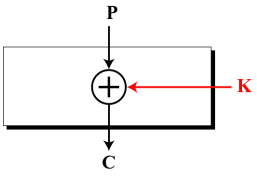
5.1.6 Continued

Example 5.13

Assume that the cipher is made only of one exclusive-or operation, as shown in Figure 5.18. Without knowing the value of the key, Eve can easily find the relationship between plaintext differences and ciphertext differences if by plaintext difference we mean P1 ⊕ P2 and by ciphertext difference, we mean C1⊕ C2. The following proves that C1 ⊕ C2 = P1 ⊕ P2:

$$C_1 = P_1 \oplus K \quad C_2 = P_2 \oplus K \quad \rightarrow \quad C_1 \oplus C_2 = P_1 \oplus K \oplus P_2 \oplus K = P_1 \oplus P_2$$

Figure 5.18 *Diagram for Example 5.13*



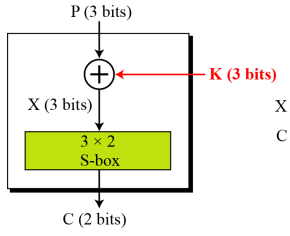
5.54

5.1.6 Continued

Example 5.14

We add one S-box to Example 5.13, as shown in Figure 5.19.

Figure 5.19 *Diagram for Example 5.14*



X	000	001	010	011	100	101	110	111
C	11	00	10	10	01	00	11	00

S-box table

5.55

5.1.6 Continued

Example 5.14 Continued

Eve now can create a probabilistic relationship as shown in Table 5.4.

Table 5.4 *Differential input/output*

$P_1 \oplus P_2$ \ $C_1 \oplus C_2$	00	01	10	11
000	8			
001	2	2		4
010	2	2	4	
011		4	2	2
100	2	2	4	
101		4	2	2
110	4		2	2
111			2	6

5.56

5.1.6 Continued

Example 5.15

The heuristic result of Example 5.14 can create probabilistic information for Eve as shown in Table 5.5.

Table 5.5 *Differential distribution table*

$P_1 \oplus P_2$ \ $C_1 \oplus C_2$	00	01	10	11
000	1	0	0	0
001	0.25	0.25	0	0.50
010	0.25	0.25	0.50	0
011	0	0.50	0.25	0.25
100	0.25	0.25	0.50	0
101	0	0.50	0.25	0.25
110	0.50	0	0.25	0.25
111	0	0	0.25	0.75

Looking at Table 5.5, Eve knows that if $C_1 \oplus C_2 = 11$ then $X_1 \oplus X_2 = 001$ with high probability (0.5).

Eve chooses C_1, C_2 such that $C_1 \oplus C_2 = 11$ and delivers a chosen ciphertext attack.

Eve obtains $P_1 \oplus P_2$ from the attack ($= X_1 \oplus X_2$)

Eve expects $X_1 \oplus X_2 = 001$

Eve guesses K, subject to constraint:
1. $P_1 \oplus X_1 = P_2 \oplus X_2 = K$
2. $P_1 \oplus P_2 = 001$

5.1.6 Continued

Note

Differential cryptanalysis is based on a nonuniform differential distribution table of the S-boxes in a block cipher.

Note

A more detailed differential cryptanalysis is given in Appendix N.

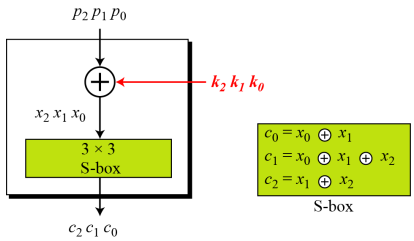
5.1.6 Continued

Linear Cryptanalysis

Linear cryptanalysis was presented by Mitsuru Matsui in 1993. The analysis uses known plaintext attacks.

5.1.6 Continued

Figure 5.20 *A simple cipher with a linear S-box*



5.1.6 Continued

$$c_0 = p_0 \oplus k_0 \oplus p_1 \oplus k_1$$
$$c_1 = p_0 \oplus k_0 \oplus p_1 \oplus k_1 \oplus p_2 \oplus k_2$$
$$c_2 = p_1 \oplus k_1 \oplus p_2 \oplus k_2$$

Solving for three unknowns, we get.

$$k_1 = (p_1) \oplus (c_0 \oplus c_1 \oplus c_2)$$
$$k_2 = (p_2) \oplus (c_0 \oplus c_1)$$
$$k_0 = (p_0) \oplus (c_1 \oplus c_2)$$

This means that three known-plaintext attacks can find the values of k_0, k_1, and k_2.

5.1.6 Continued

In some modern block ciphers, it may happen that some S-boxes are not totally nonlinear; they can be approximated, probabilistically, by some linear functions.

$$(k_0 \oplus k_1 \oplus \cdots \oplus k_x) = (p_0 \oplus p_1 \oplus \cdots \oplus p_y) \oplus (c_0 \oplus c_1 \oplus \cdots \oplus c_z)$$

where $1 \le x \le m$, $1 \le y \le n$, and $1 \le z \le n$.

Note

A more detailed linear cryptanalysis is given in Appendix N.

5.63