Cryptography (CS-501

Introduction to Modern Symmetric-key Ciphers

Dr Samayveer Singh
Assistant Professor
Department of Computer Science & Engineering
National Institute Technology Jalandhar, Punjab, India
samays@nitj.ac.in

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.

1 Continued

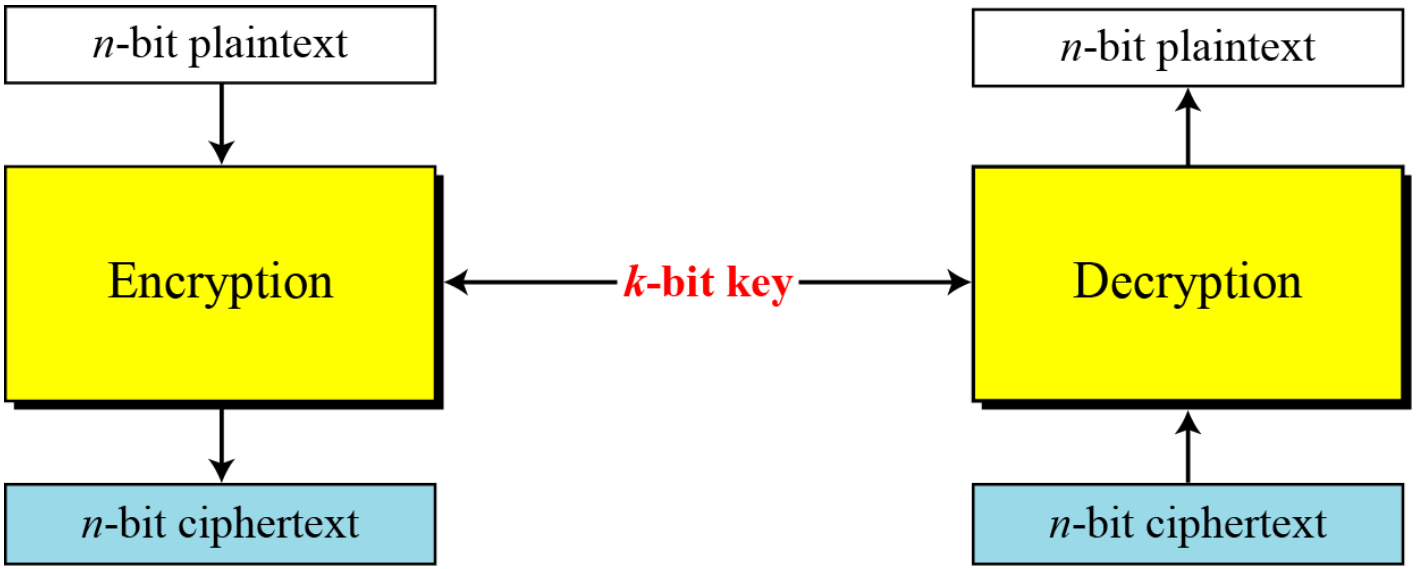


Figure 1 *A modern block cipher*

1 Continued

Example 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,

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

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.

1.1 Continued

Example 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.**

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 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 2.

1.2 Continued

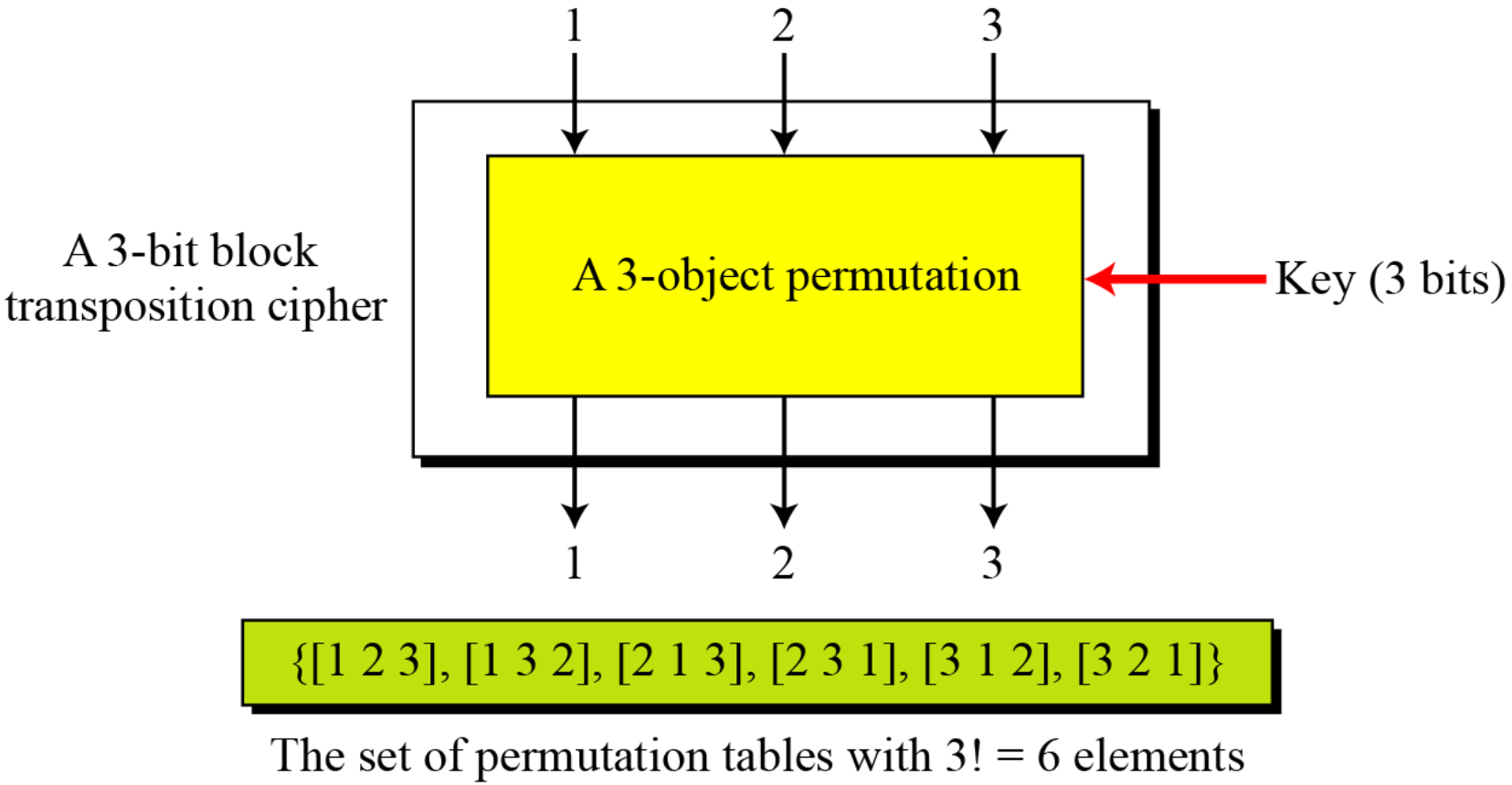


Figure 2 ***A transposition block cipher modeled as a permutation***

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 4

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

Solution

Figure 3 shows the model and the set of permutation tables. The key is also much longer, $\lceil \log_2 40{,}320 \rceil = 16$ bits.

1.2 Continued

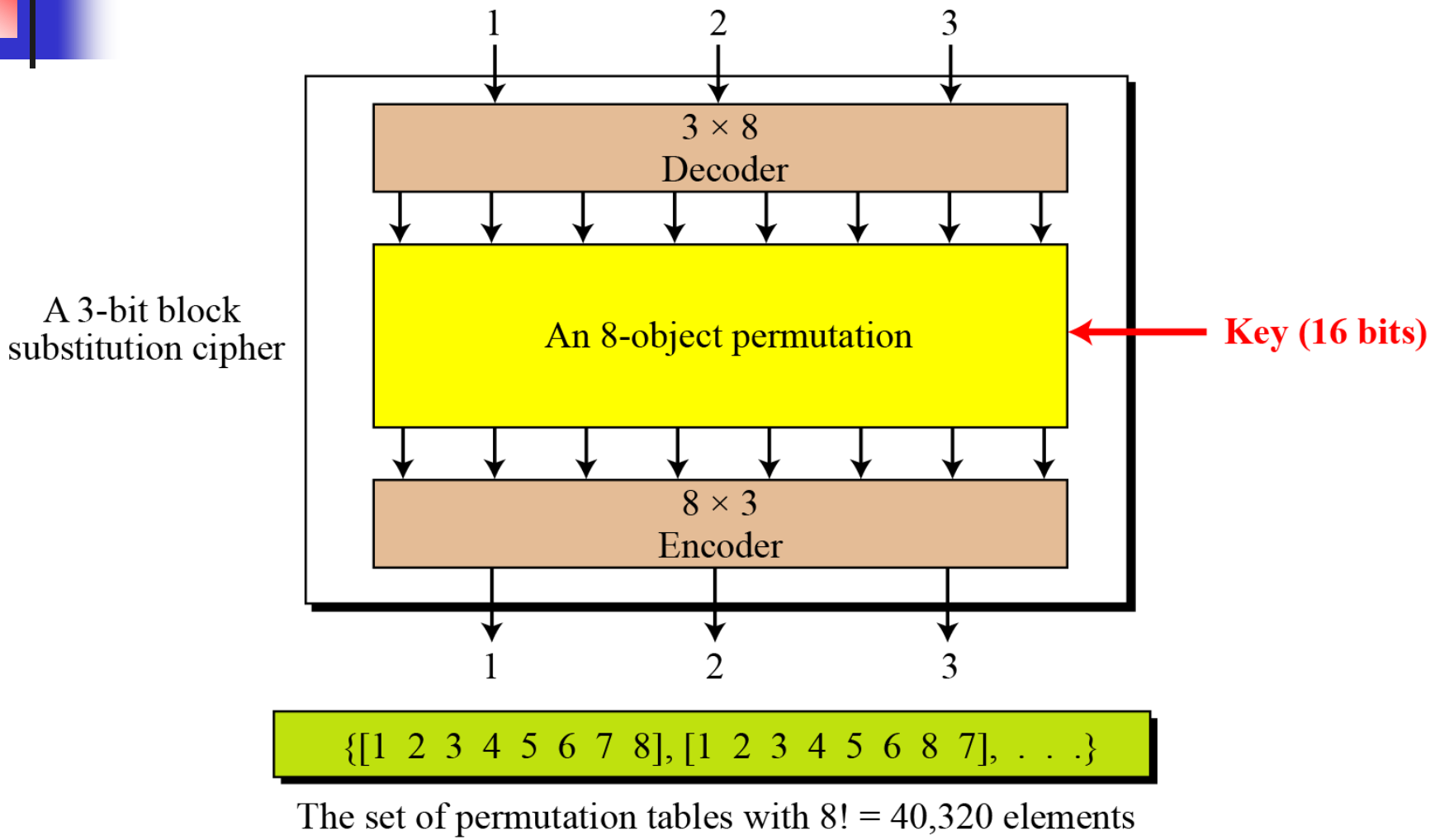


Figure 3 ***A substitution block cipher model as a permutation***

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.

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.

1.3 Continued

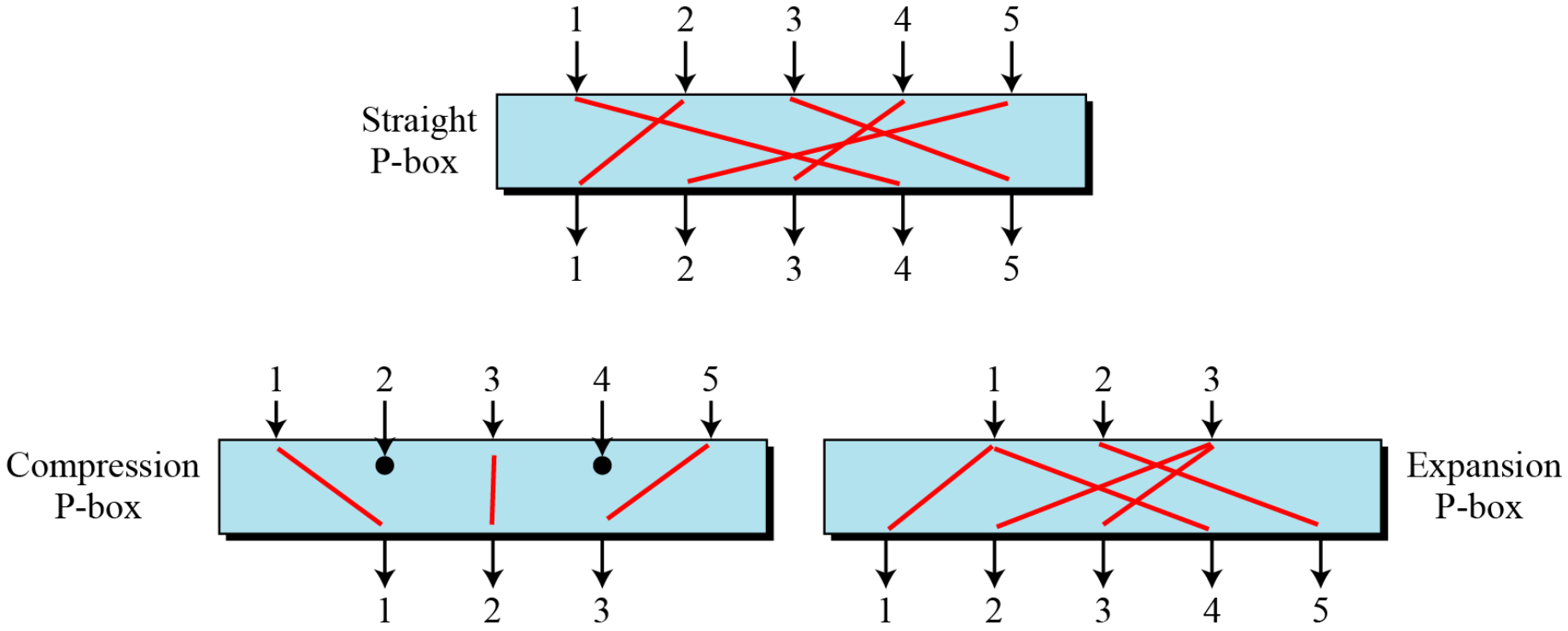


Figure 4 *Three types of P-boxes*

Example 5

Figure 5 shows all 6 possible mappings of a 3 × 3 P-box.

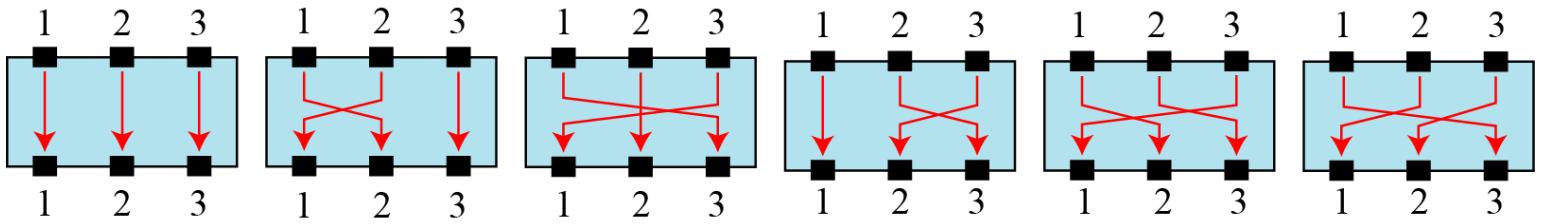


Figure 5 *The possible mappings of a 3 × 3 P-box*

1.3 Continued

Straight P-Boxes

Table 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

Example 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.

1.3 Continued

Compression P-Boxes

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

Table 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

1.3 Continued

Compression P-Box

Table 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

1.3 Continued

Expansion P-Boxes

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

Table 3 *Example of a 12 × 16 permutation table*

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

P-Boxes: Invertibility

Note

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

Example 7

Figure 6 shows how to invert a permutation table represented as a one-dimensional table.

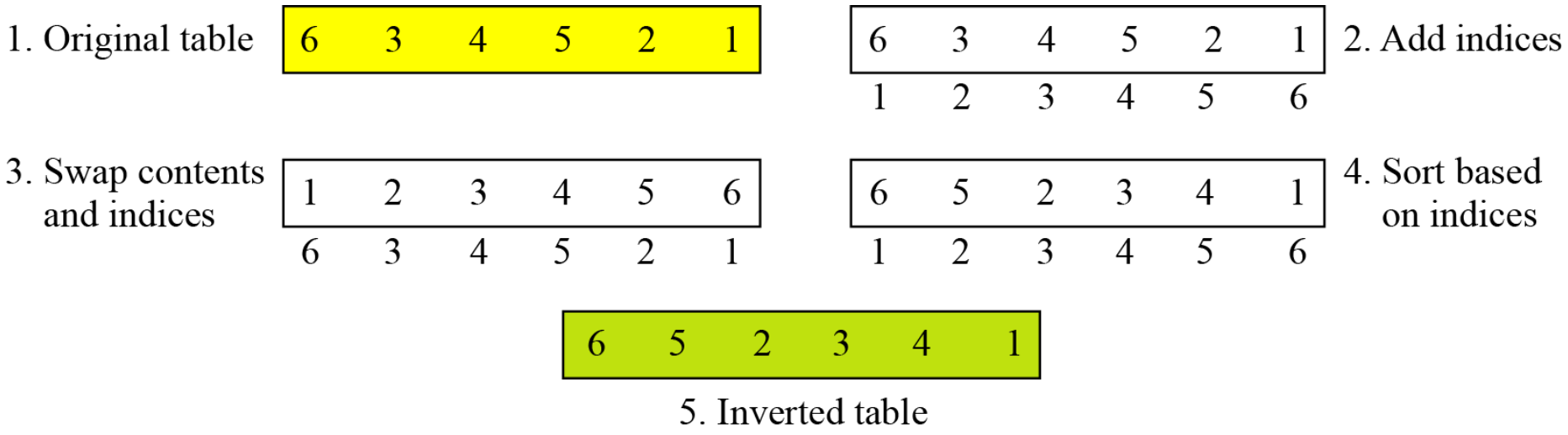


Figure 6 ***Inverting a permutation table***

1.3 Continued

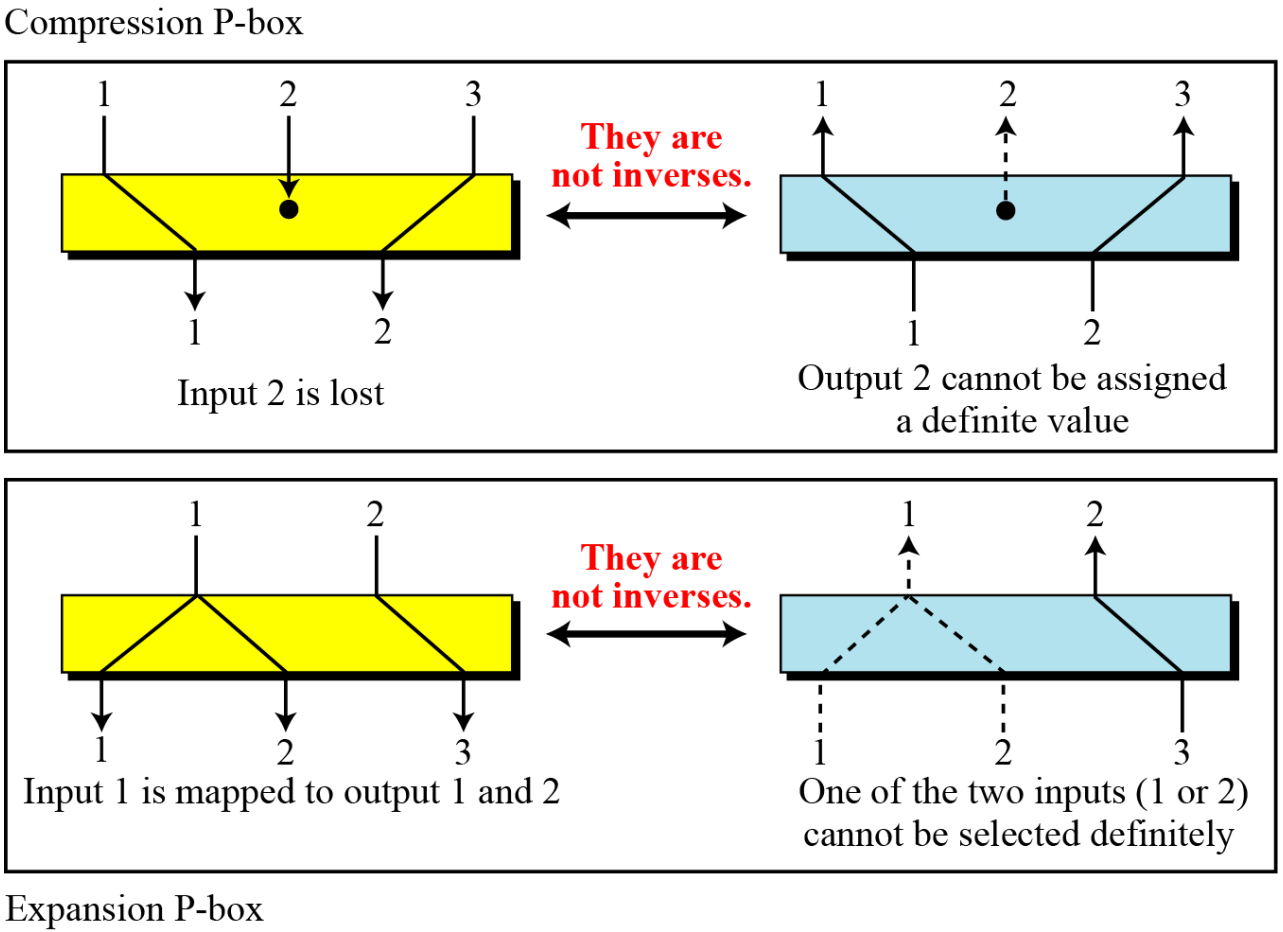


Figure 7 *Compression and expansion P-boxes are non-invertible*

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.

Example 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:

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

Example 9

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

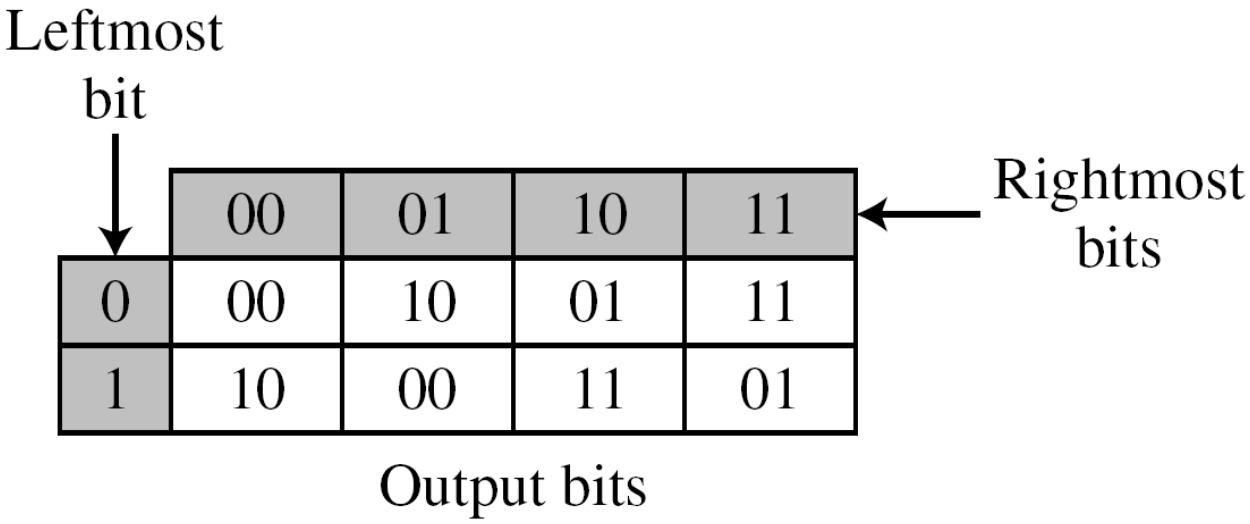
$$y_1 = (x_1)^3 + x_2 \qquad y_2 = (x_1)^2 + x_1x_2 + x_3$$

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.

1.3 Continued

Example 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.



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

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.

Example 11

Figure 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.

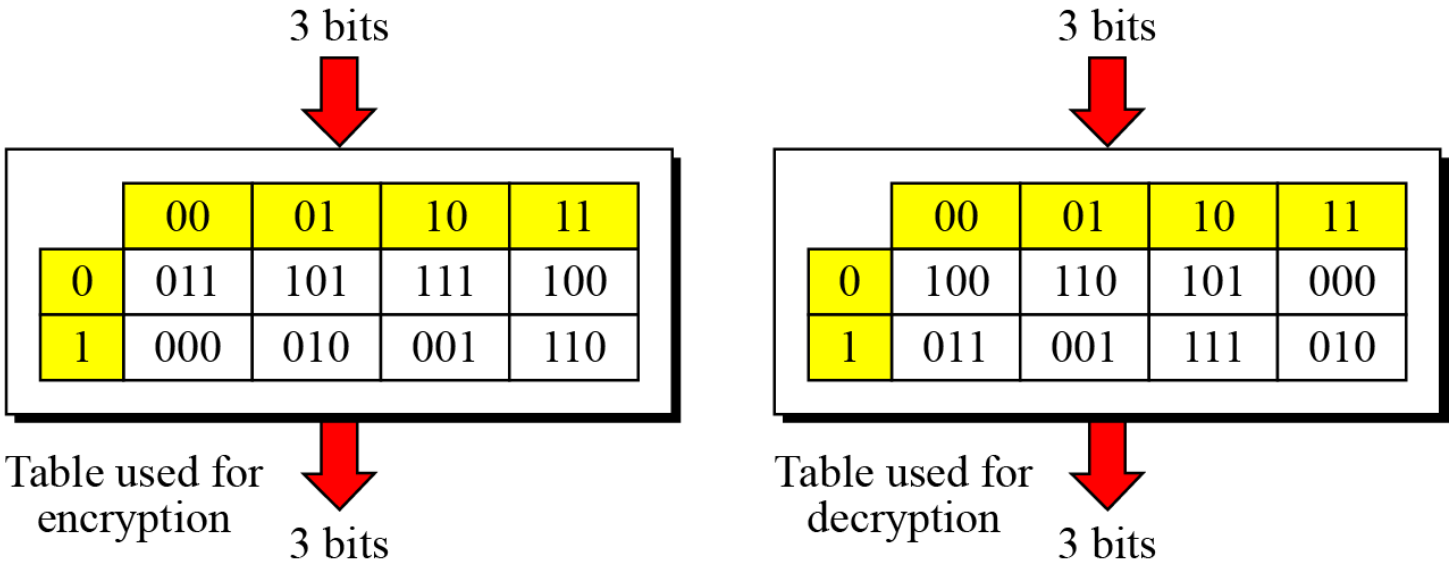


Figure 8 *S-box tables for Example 11*

Exclusive-Or

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

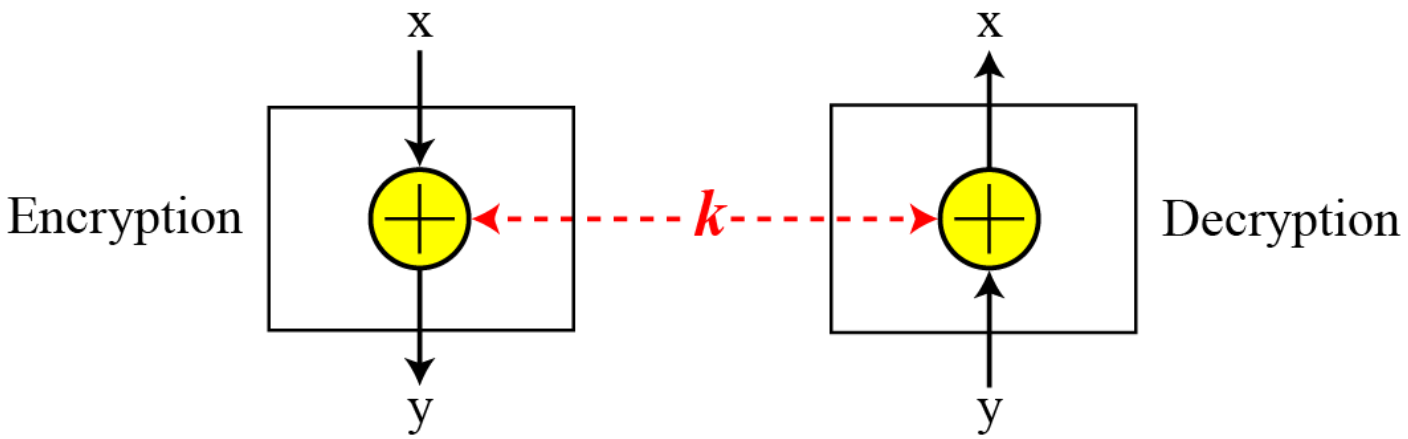
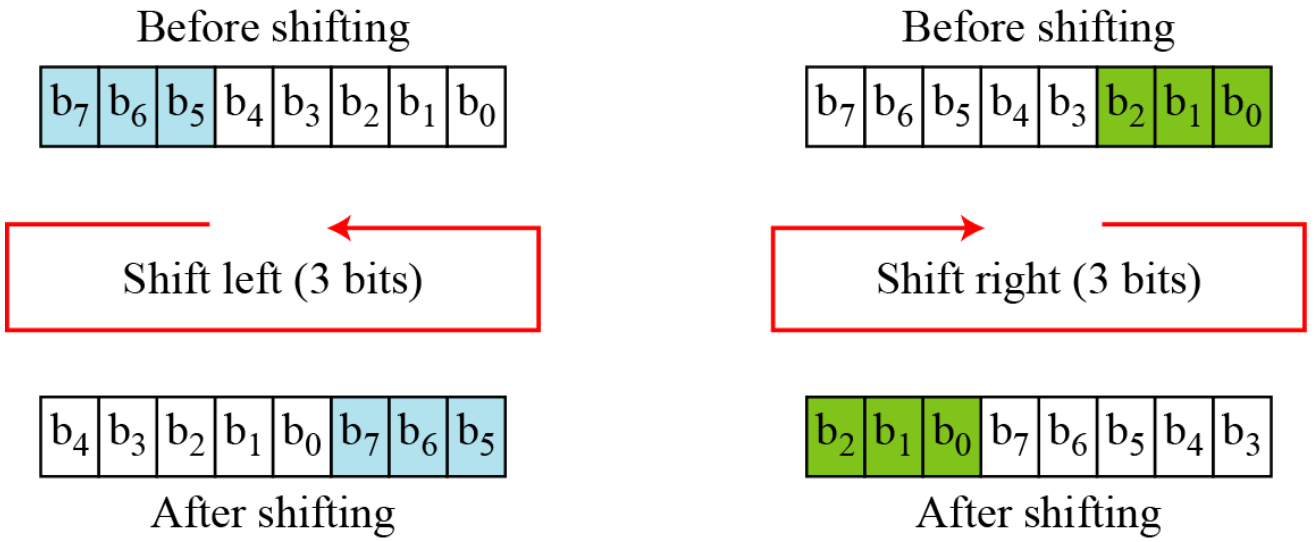


Figure 9 *Invertibility of the exclusive-or operation*

Circular Shift

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

Figure 10 *Circular shifting an 8-bit word to the left or right*



Swap

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

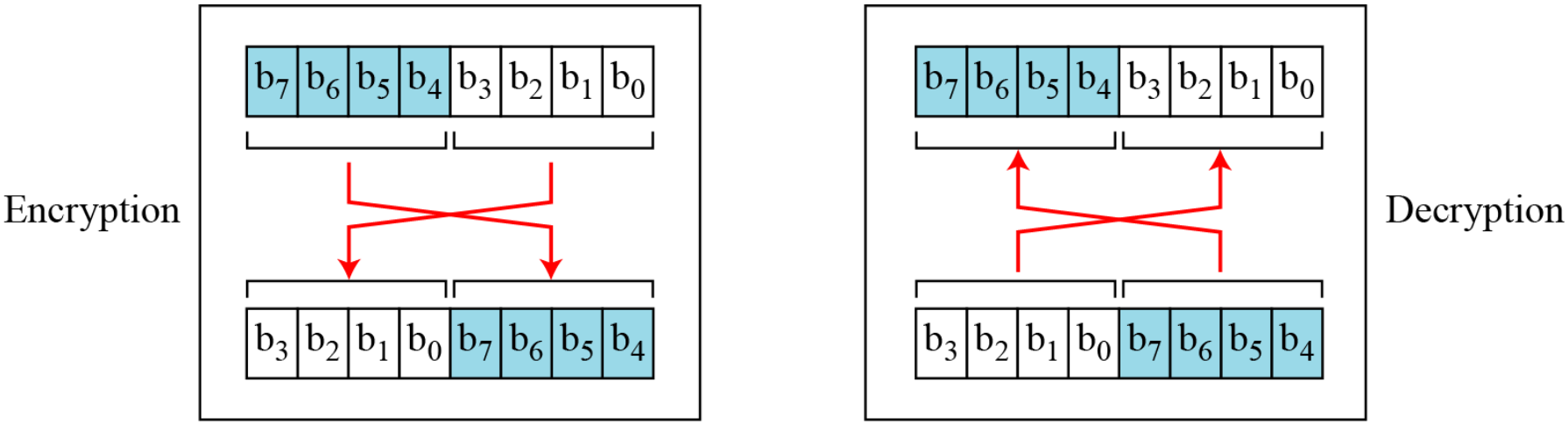


Figure 11 ***Swap operation on an 8-bit word***

1.3 Continued

Split and Combine

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

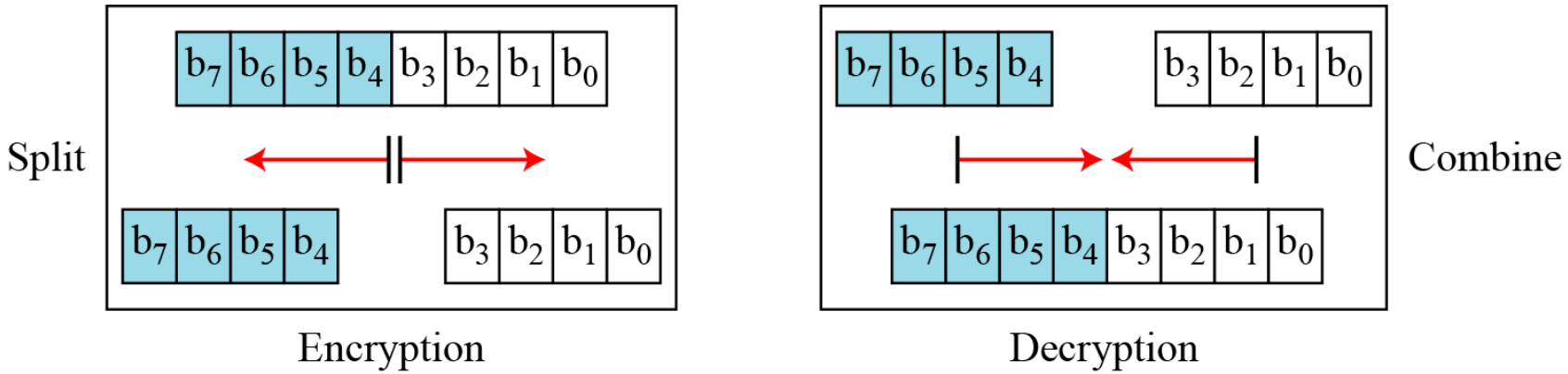


Figure 12 ***Split and combine operations on an 8-bit word***

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.

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.

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.

1.4 Continued

Rounds

Diffusion and confusion can be achieved using iterated product ciphers where each iteration is a combination of S-boxes, P-boxes, and other components.

1.4 Continued

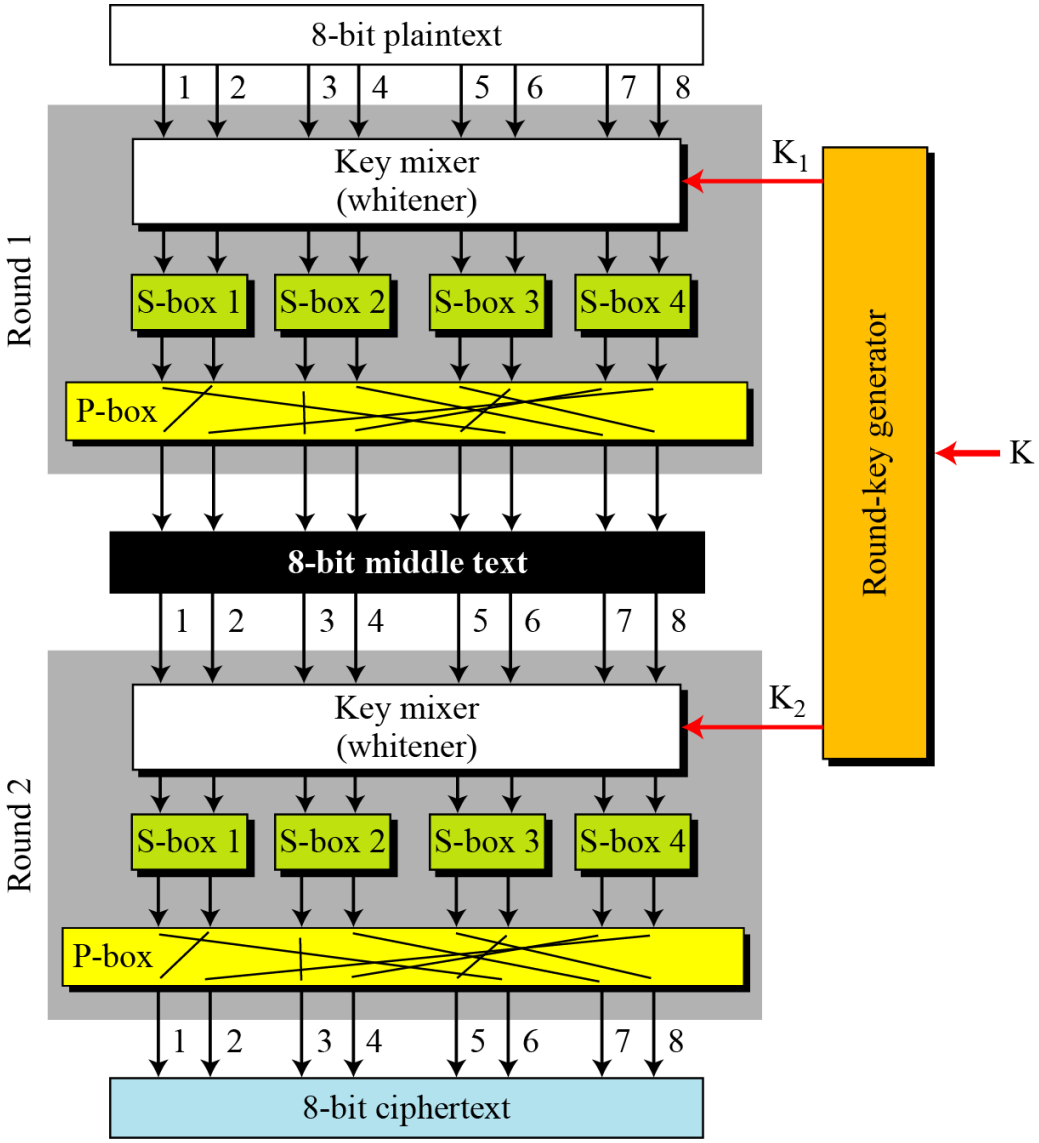


Figure 13 *A product cipher made of two rounds*

1.4 Continued

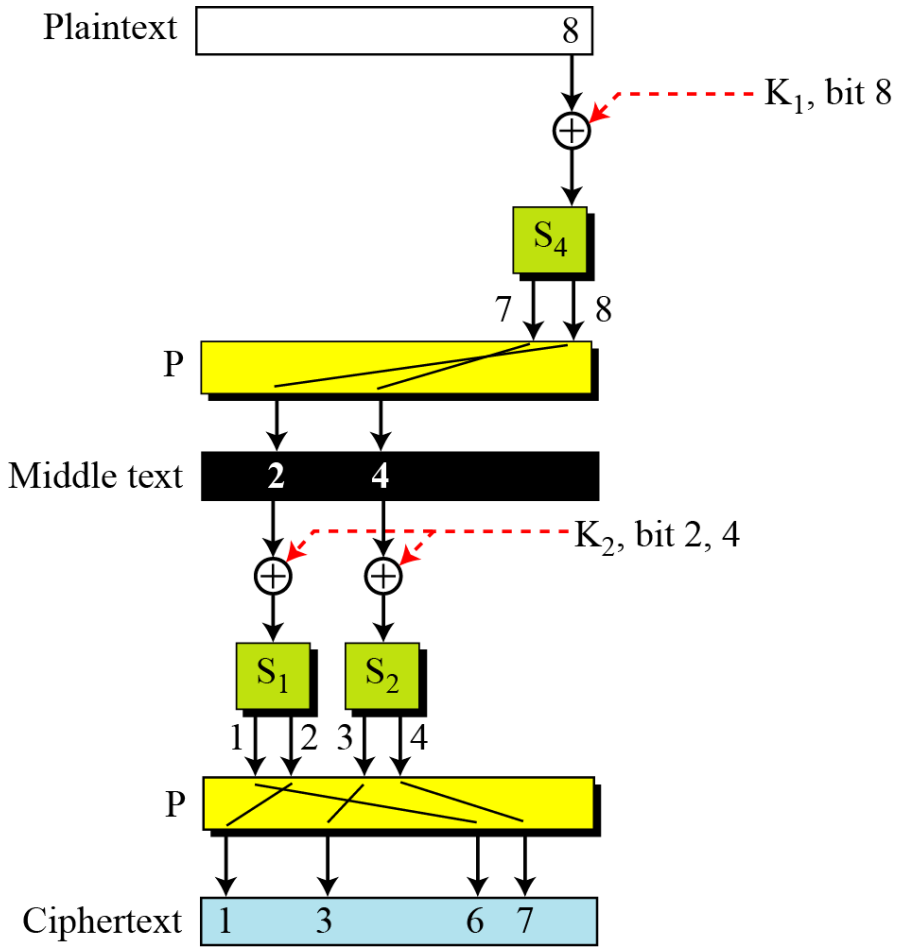


Figure 14 *Diffusion and confusion in a block cipher*

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***

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.

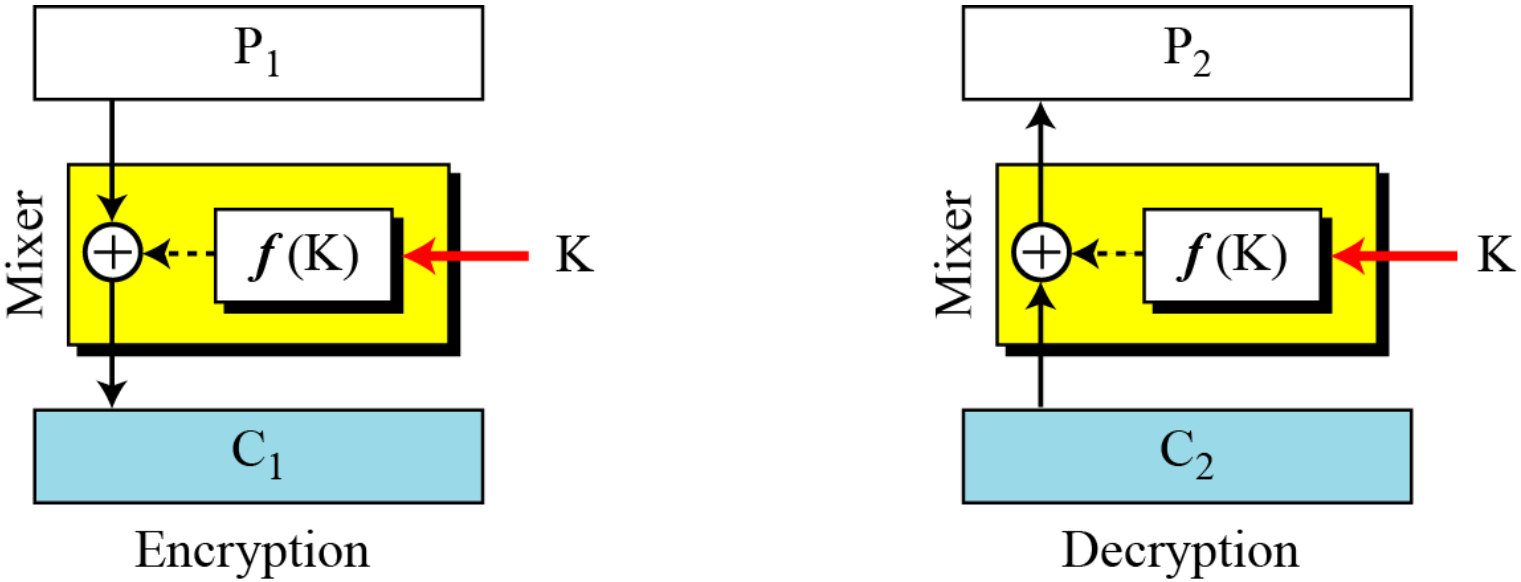


Figure 15 *The first thought in Feistel cipher design*

Note

Diffusion hides the relationship between the ciphertext and the plaintext.

1.3 Continued

Example 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.

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

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

1.5 Continued

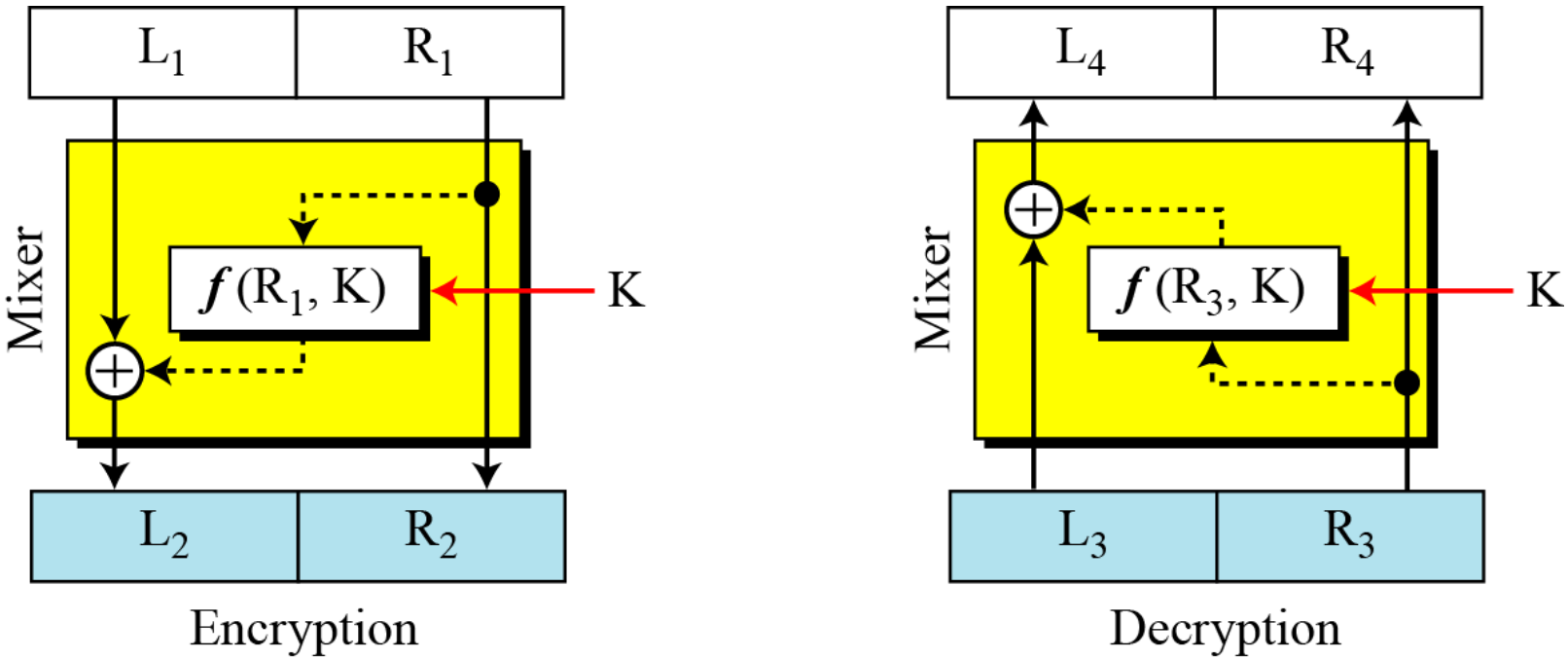


Figure 16 *Improvement of the previous Feistel design*

1.5 Continued

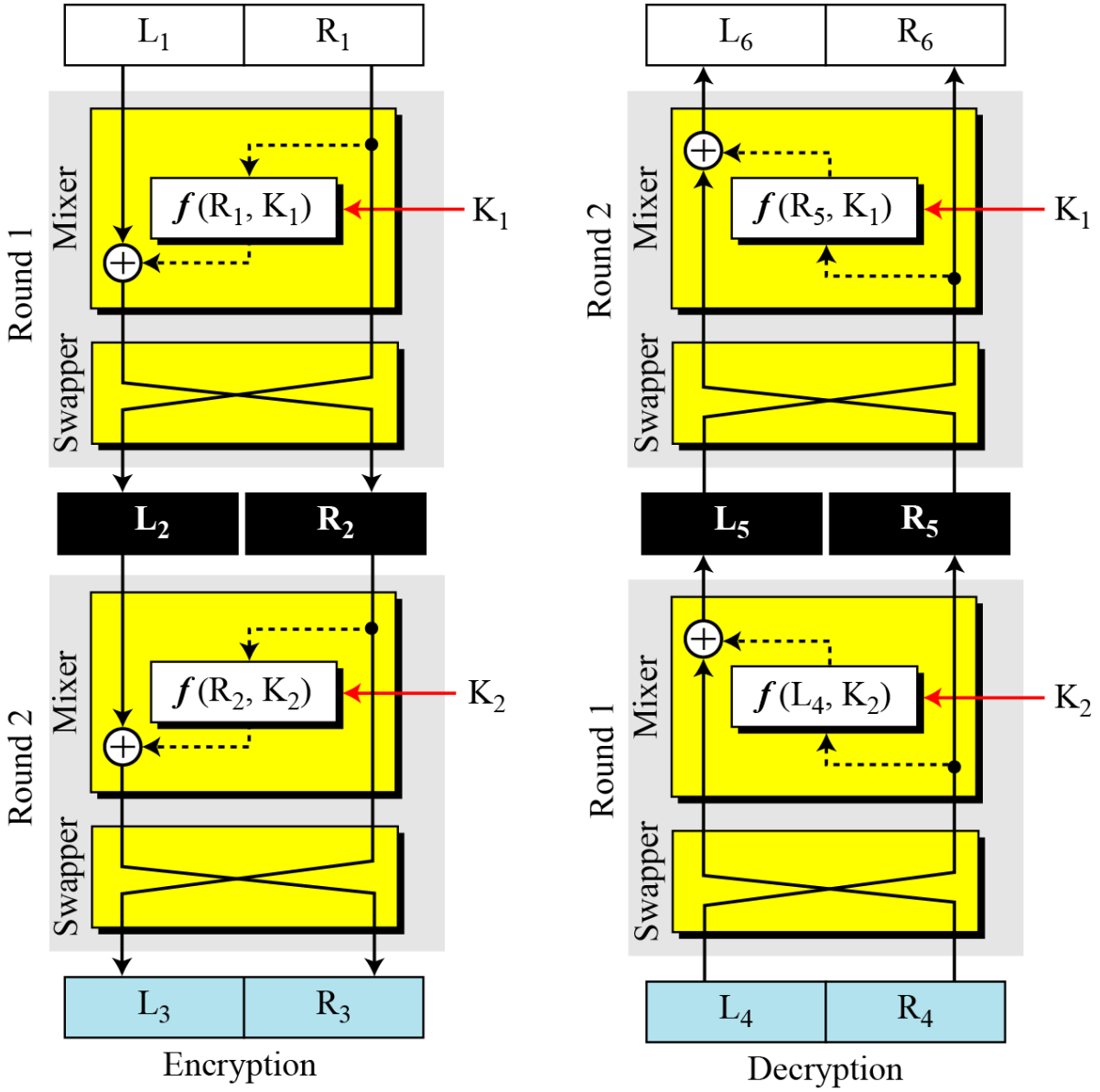


Figure 17 *Final design of a Feistel cipher with two rounds*

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.

2 MODERN STREAM CIPHERS

In a modern stream cipher, encryption and decryption are done r bits at a time. We have a plaintext bit stream $P = p_n \ldots p_2 \; p_1$, a ciphertext bit stream $C = c_n \ldots c_2 \, c_1$, and a key bit stream $K = k_n \ldots k_2 \, k_1$, in which p_i , c_i , and k_i are r-bit words.

2 Continued

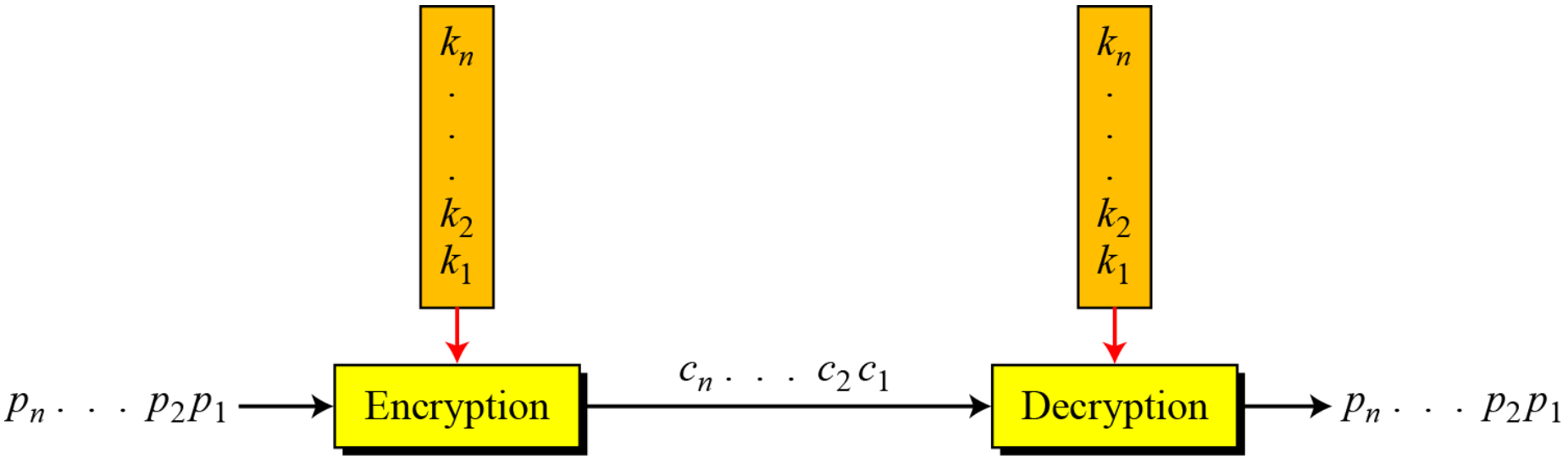


Figure 20 *Stream cipher*

Note

In a modern stream cipher, each *r*-bit word in the plaintext stream is enciphered using an *r*-bit word in the key stream to create the corresponding *r*-bit word in the ciphertext stream.

2.1 Synchronous Stream Ciphers

Note

In a synchronous stream cipher the key is independent of the plaintext or ciphertext.

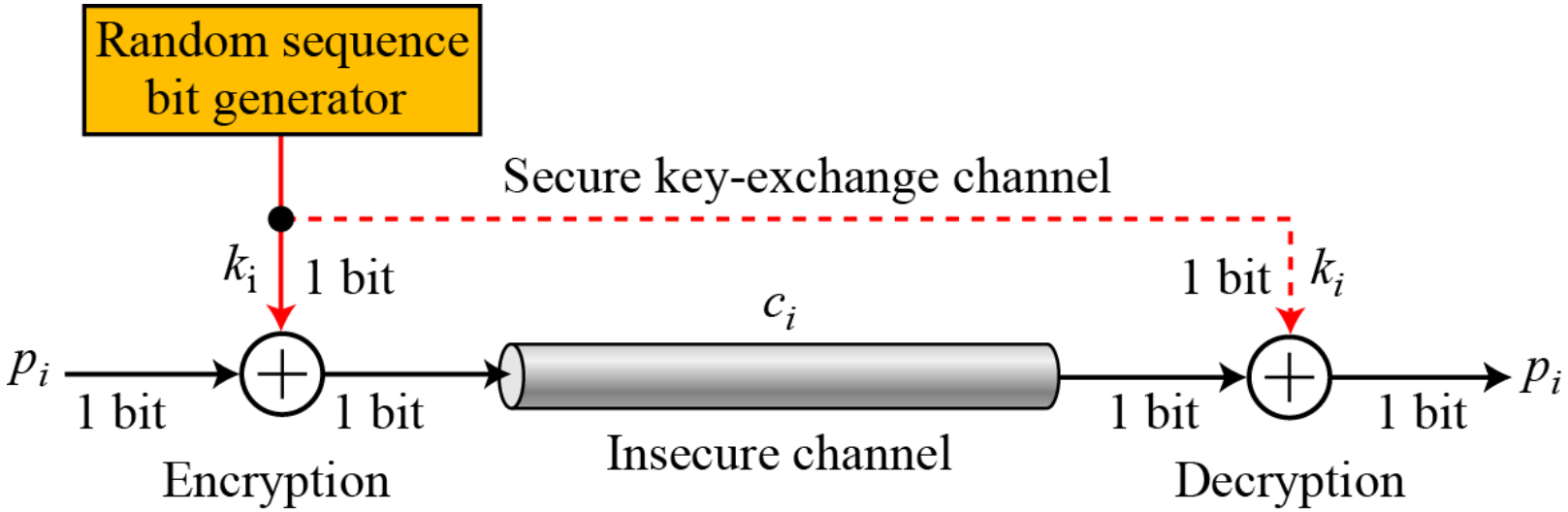


Figure 22 *One-time pad*

2.1 Continued

Example 17

What is the pattern in the ciphertext of a one-time pad cipher in each of the following cases?

a. The plaintext is made of *n* 0's.

b. The plaintext is made of *n* 1's.

c. The plaintext is made of alternating 0's and 1's.

d. The plaintext is a random string of bits.

Solution

a. Because $0 \oplus k_i = k_i$, the ciphertext stream is the same as the key stream. If the key stream is random, the ciphertext is also random. The patterns in the plaintext are not preserved in the ciphertext.

Example 7 (Continued)

b. Because $1 \oplus k_i = \overline{k}_i$ where $\overline{k}_i$ is the complement of k_i, the ciphertext stream is the complement of the key stream. If the key stream is random, the ciphertext is also random. Again the patterns in the plaintext are not preserved in the ciphertext.

c. In this case, each bit in the ciphertext stream is either the same as the corresponding bit in the key stream or the complement of it. Therefore, the result is also a random string if the key stream is random.

d. In this case, the ciphertext is definitely random because the exclusive-or of two random bits results in a random bit.

2.2 Nonsynchronous Stream Ciphers

In a nonsynchronous stream cipher, each key in the key stream depends on previous plaintext or ciphertext.

Note

In a nonsynchronous stream cipher, the key depends on either the plaintext or ciphertext.