5-2 MODERN STREAM CIPHERS

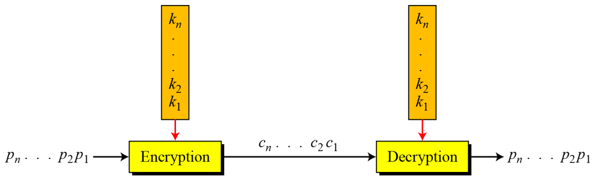
In a modern stream cipher, encryption and decryption are done r bits at a time. We have a plaintext bit stream $P = p_n \ldots p_2\ p_1$, *a ciphertext bit stream* $C = c_n \ldots c_2\ c_1$, *and a key bit stream* $K = k_n \ldots k_2\ k_1$, *in which* p_i, c_i, *and* k_i *are r-bit words.*

Topics discussed in this section:

5.2.1 Synchronous Stream Ciphers
5.2.2 Nonsynchronous Stream Ciphers

5.2 Continued

Figure 5.20 *Stream cipher*



Note

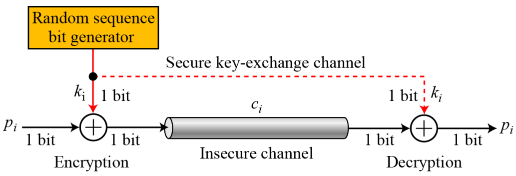
In a modern stream cipher, each *r*-bit word in the plaintext stream is enciphered using an *r*-bit word in the key stream to create the corresponding *r*-bit word in the ciphertext stream.

5.2.1 Synchronous Stream Ciphers

Note

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

Figure 5.22 *One-time pad*



5.2.1 Continued

Example 5.17

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.**

5.2.1 Continued

Example 5.7 **(Continued)**

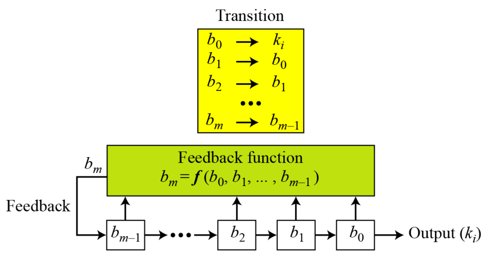
b. **Because** $1 \oplus k_i = \overline{k_i}$ **where** $\overline{k_i}$ **is the complement of** k_i, **the ciphertext stream is the complement of the key stream. If the key stream is random, the ciphertext is also random. Again the patterns in the plaintext are not preserved in the ciphertext.**

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.**

5.2.1 Continued

Figure 5.23 *Feedback shift register (FSR)*



5.2.1 Continued

Example 5.18

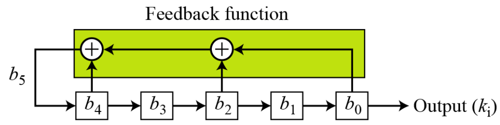
Create a linear feedback shift register with 5 cells in which $b_5 = b_4 \oplus b_2 \oplus b_0$.

Solution

If $c_i = 0$, b_i has no role in calculation of b_m. This means that b_i is not connected to the feedback function. If $c_i = 1$, b_i is involved in calculation of bm. In this example, c1 and c3 are 0's, which means that we have only three connections. Figure 5.24 shows the design.

5.2.1 Confidentiality

Figure 5.24 *LSFR for Example 5.18*



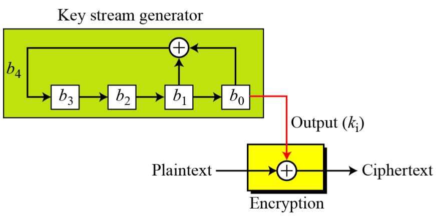
5.2.1 Continued

Example 5.19

Create a linear feedback shift register with 4 cells in which $b_4 = b_1 \oplus b_0$. Show the value of output for 20 transitions (shifts) if the seed is $(0001)_2$.

Solution

Figure 5.25 *LFSR for Example 5.19*



5.2.1 Continued

Example 5.19 (Continued)

Table 4.6 *Cell values and key sequence for Example 5.19*

States	b_4	b_3	b_2	b_1	b_0	k_i
Initial	1	0	0	0	1	
1	0	1	0	0	0	1
2	0	0	1	0	0	0
3	1	0	0	1	0	0
4	1	1	0	0	1	0
5	0	1	1	0	0	1
6	1	0	1	1	0	0
7	0	1	0	1	1	0
8	1	0	1	0	1	1
9	1	1	0	1	0	1
10	1	1	1	0	1	0

5.2.1 Continued

Example 5.19 (Continued)

Table 4.6 Continued

11	1	1	1	1	0	1
12	0	1	1	1	1	0
13	0	0	1	1	1	1
14	0	0	0	1	1	1
15	1	0	0	0	1	1
16	0	1	0	0	0	1
17	0	0	1	0	0	0
18	1	0	0	1	0	0
19	1	1	0	0	1	0
20	1	1	1	0	0	1

5.2.1 Continued

Example 5.19 (Continued)

Note that the key stream is 100010011010111 10001…. This looks like a random sequence at first glance, but if we go through more transitions, we see that the sequence is periodic. It is a repetition of 15 bits as shown below:

100010011010111 **100010011010111** 100010011010111 **100010011010111** …

The key stream generated from a LFSR is a pseudorandom sequence in which the the sequence is repeated after N bits.

Note

The maximum period of an LFSR is to $2^m - 1$.

5.2.1 *Continued*

Example 5.20

The characteristic polynomial for the LFSR in Example 5.19 is ($x^4 + x + 1$), which is a primitive polynomial. Table 4.4 (Chapter 4) shows that it is an irreducible polynomial. This polynomial also divides ($x^7 + 1$) = ($x^4 + x + 1$) ($x^3 + 1$), which means $e = 2^3 - 1 = 7$.

5.2.2 *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.