Exercise 4.8.7
Suppose that four-digit PINs are randomly distributed. How many people must be in a room such that the probability that two of them have the same PIN is at least 1/2?

Exercise 4.8.8
Prove that the Caesar cipher does not have perfect secrecy.

Exercise 4.8.9
Consider the linear block cipher with block length n and alphabet $\{0,1\}^n$. On the key space of matrices $A \in \{0,1\}^{(n,n)}$ with $\det(A) \equiv 1 \bmod 2$, choose the random distribution. Does this cryptosystem have perfect secrecy?

5 CHAPTER DES

In Chapter 3, we have defined cryptosystems and we have described some historical examples. All of the cryptosystems in Chapter 3 could all be broken because they are affine linear. A cryptosystem with perfect secrecy, the Vernam one-time pad, was presented in Chapter 4, but it turns out to be very inefficient. In this chapter, we describe the Data Encryption Standard (DES). For many years, this cryptosystem was the encryption standard in the U.S. and was used worldwide. Today, simple DES is no longer secure and the US National Institute of Standards (NIST) has chosen the Rijndael cryptosystem as the Advanced Encryption Standard (AES) [1] (see Chapter 6). AES is described in Chapter 6. Nevertheless, there are secure variants of DES (see Section 3.7) that are widely use. Also, DES remains an important model for the construction of secure block ciphers.

5.1 Feistel Ciphers

The DES algorithm is a so-called *Feistel cipher*. In this section, we explain Feistel ciphers.

We use a block cipher with alphabet $\{0, 1\}$. Let t be its block length. Let f_K be the encryption function for the key K. The Feistel cipher that is constructed from these ingredients is a block cipher with block length $2t$ and alphabet $\{0, 1\}$. We fix a number $r \geq 1$ of rounds, a key space $\mathcal{K}$, and a method that, from any key $k \in \mathcal{K}$, generates a sequence $K_1, \dots, K_r$ of round keys that belong to the key space of the underlying block cipher.

The encryption function E_k of the Feistel cipher for key $k \in \mathcal{K}$ works as follows. Let p be a plaintext of length $2t$. We split it into two halves of length t; that is, we write $p = (L_0, R_0)$, where L_0 is the left half and R_0 is the right half. Then the sequence

$$(L_i, R_i) = (R_{i-1}, L_{i-1} \oplus f_{K_i}(R_{i-1})), \quad 1 \leq i \leq r \tag{5.1}$$

is constructed, and we set

$$E_k(L_0, R_0) = (R_r, L_r).$$

Clearly, the security of the Feistel cipher depends on the security of the internal block cipher. This security is increased by iterated application.

We explain the decryption of the Feistel cipher. From (5.1), we immediately obtain

$$(R_{i-1}, L_{i-1}) = (L_i, R_i \oplus f_{K_i}(L_i)), \quad 1 \leq i \leq r. \tag{5.2}$$

Using this equation in r rounds with the reverse key sequence $(K_r, K_{r-1}, \dots, K_1)$, the plaintext pair (R_0, L_0) is reconstructed from the ciphertext (R_r, L_r). Hence, for the Feistel cipher, encryption and decryption are the same except that the key sequence is reversed.

5.2 DES Algorithm

The DES cryptosystem is a slightly modified Feistel cipher with alphabet $\{0, 1\}$ and block length 64. In this section, we explain in detail how DES works.

TABLE 5.1 Valid DES key.

0	0	0	1	0	0	1	1
0	0	1	1	0	1	0	0
0	1	0	1	0	1	1	1
0	1	1	1	1	0	0	1
1	0	0	1	1	0	1	1
1	0	1	1	1	1	0	0
1	1	0	1	1	1	1	1
1	1	1	1	0	0	0	1

5.2.1 Plaintext and ciphertext space

The plaintext and ciphertext spaces of DES are $\mathcal{P} = \mathcal{C} = \{0, 1\}^{64}$. The DES keys are all bitstrings of length 64 with the following property. If a 64-bit DES key is divided into eight bytes, then the sum of the eight bits of each byte is odd. This means that seven of the eight bits determine the value of the eighth bit. Transmission errors of one bit can be corrected. Therefore, the key space is

$$\mathcal{K} = \{(b_1, \dots, b_{64}) \in \{0, 1\}^{64} : \sum_{i=1}^{8} b_{8k+i} \equiv 1 \mod 2, 0 \leq k \leq 7\}.$$

The number of DES keys is $2^{56} \sim 7.2 * 10^{16}$.

Example 5.2.1
A valid hexadecimal DES key is

133457799BBCDFF1.

Its binary expansion can be found in Table 5.1.

5.2.2 Initial permutation

Given a plaintext p, DES works in three steps.

Prior to the Feistel encryption, DES applies an *initial permutation* (IP) to p. This is a bit permutation on bit vectors of length 64 that is independent of the chosen key. The permutation IP and its inverse are shown in Table 5.2. Table 5.2 is read as follows: If $p \in \{0, 1\}^{64}$, $p = p_1 p_2 p_3 \dots p_{64}$, then $\text{IP}(p) = p_{58} p_{50} p_{42} \dots p_7$.

TABLE 5.2 The initial permutation, IP.

IP							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

IP^{-1}							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

A 16-round Feistel cipher is applied to the permuted plaintext. Finally, the ciphertext is constructed using the inverse permutation IP^{-1}:

$$c = \mathrm{IP}^{-1}(R_{16}L_{16}).$$

5.2.3 Internal block cipher

We describe the block cipher on which the DES Feistel cipher is based. Its alphabet is $\{0,1\}$, its block length is 32, and its key space is $\{0,1\}^{48}$. We explain the encryption function $f_K : \{0,1\}^{32} \to \{0,1\}^{32}$ for a key $K \in \{0,1\}^{48}$ (see Figure 5.0).

The argument $R \in \{0,1\}^{32}$ is expanded by the expansion function E: $\{0,1\}^{32} \to \{0,1\}^{48}$. This function is shown in Table 5.3. If $R = R_1R_2\dots R_{32}$, then $E(R) = R_{32}R_1R_2\dots R_{32}R_1$.

Next, $E(R) \oplus K$ is computed, and the result is divided into eight blocks B_i, $1 \le i \le 8$ of length 6, namely,

$$E(R) \oplus K = B_1B_2B_3B_4B_5B_6B_7B_8 \tag{5.3}$$

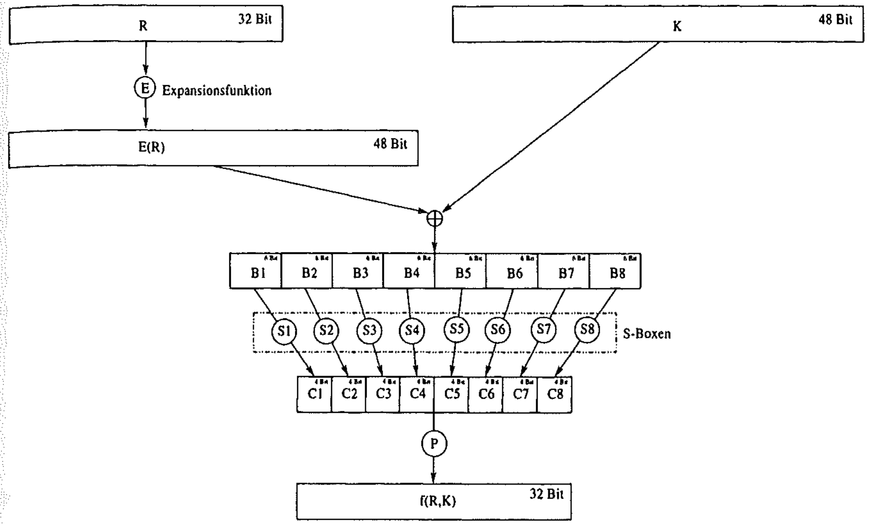

FIGURE 5.1 The f-function of DES.

is computed with $B_i \in \{0,1\}^6$, $1 \le i \le 8$. In the next step, functions

$$S_i : \{0,1\}^6 \to \{0,1\}^4, \quad 1 \le i \le 8$$

are used (the so-called S-boxes). They are described below. Using those functions, the string

$$C = C_1C_2C_3C_4C_5C_6C_7C_8$$

is determined, where $C_i = S_i(B_i)$, $1 \le i \le 8$. It has length 32. The permutation P from Table 5.3 is applied to this string. The result is $f_K(R)$.

5.2.4 S-boxes

Now we describe the S-boxes S_i, $1 \le i \le 8$. They are the heart of DES because they are highly nonlinear (see Exercise 5.5.6). They are shown in Table 5.4.Each S-box is represented by a table with four rows and 16 columns. For each string $B = b_1b_2b_3b_4b_5b_6$, the value $S_i(B)$ is computed as follows. The integer with binary expansion b_1b_6 is used as the row index. The integer with binary expansion $b_2b_3b_4b_5$ is used as the column index. The entry of the S-box in this row and column is written in binary expansion. This expansion is padded with leading zeros such that its length is four. The result is $S_i(B)$.

TABLE 5.3 The functions E and P.

E					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

P			
16	7	10	21
29	12	28	17
1	15	23	26
5	18	31	20
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Example 5.2.2

We compute $S_1(001011)$. The first bit is 0 and the last bit is 1. Therefore, the row index is the integer with binary expansion 01 (i.e., 1). The four middle bits are 0101. This is the binary expansion of 5. Therefore, the column index is 5. The entry in row 1 and column 5 of the first S-box is 2. The binary expansion of 2 is 10. Therefore, $S_1(001011) = 0010$.

5.2.5 Keys

Finally, we explain how the round keys are computed. Let $k \in \{0,1\}^{64}$ be a DES key. We generate the round keys K_i, $1 \le i \le 16$, of length 48. We define the values v_i, $1 \le i \le 16$, as follows.

$$v_i = \begin{cases} 1 & \text{for } i \in \{1, 2, 9, 16\} \\ 2 & \text{otherwise.} \end{cases}$$

The round keys are computed by the following algorithm using the functions

$$\text{PC1} : \{0,1\}^{64} \rightarrow \{0,1\}^{28} \times \{0,1\}^{28}, \quad \text{PC2} : \{0,1\}^{28} \times \{0,1\}^{28} \rightarrow \{0,1\}^{48},$$

which are described later.

1. Set $(C_0, D_0) = \text{PC1}(k)$.
2. For $1 \le i \le 16$, do the following:
   (a) Let C_i be the string that is obtained from C_{i-1} by a circular left shift of v_i positions.

TABLE 5.4 S-boxes of DES.

Row	Column															
	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[14]	[15]
S_1																
[0]	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
[1]	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
[2]	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
[3]	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2																
[0]	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
[1]	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
[2]	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
[3]	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3																
[0]	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
[1]	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
[2]	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
[3]	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4																
[0]	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
[1]	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
[2]	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
[3]	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5																
[0]	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
[1]	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
[2]	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
[3]	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6																
[0]	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
[1]	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
[2]	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
[3]	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7																
[0]	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
[1]	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
[2]	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
[3]	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8																
[0]	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
[1]	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
[2]	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
[3]	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

TABLE 5.5 The functions PC1 and PC2.

PC1						
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

PC2					
14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

(b) Let D_i be the string that is obtained from D_{i-1} by a circular left shift of v_i positions.

(c) Determine $K_i = \mathrm{PC2}(C_i, D_i)$.

The function PC1 maps a bitstring k of length 64 to two bitstrings C and D of length 28. This is done according to Table 5.5. The upper half of the table describes C. If $k = k_1 k_2 \dots k_{64}$, then $C = k_{57} k_{49} \dots k_{36}$. The lower half of the table represents D, so $D = k_{63} k_{55} \dots k_4$. The function PC2 maps a pair (C, D) of bitstrings of length 28 (i.e., a bitstring of length 56) to a bitstring of length 48. The function is shown in Table 5.5. The value $\mathrm{PC2}(b_1 \dots b_{56})$ is $b_{14} b_{17} \dots b_{32}$.

This concludes the description of the DES encryption algorithm.

5.2.6 Decryption

To decrypt a ciphertext, DES is applied with the reverse key sequence.

5.3 An Example

We illustrate the DES algorithm by way of an example.

We encrypt the plaintext $p = 0123456789ABCDEF$. Its binary expansion is

0	0	0	0	0	0	0	1
0	0	1	0	0	0	1	1
0	1	0	0	0	1	0	1
0	1	1	0	0	1	1	1
1	0	0	0	1	0	0	1
1	0	1	0	1	0	1	1
1	1	0	0	1	1	0	1
1	1	1	0	1	1	1	1

The application of IP yields

1	1	0	0	1	1	0	0
0	0	0	0	0	0	0	0
1	1	0	0	1	1	0	0
1	1	1	1	1	1	1	1
1	1	1	1	0	0	0	0
1	0	1	0	1	0	1	0
1	1	1	1	0	0	0	0
1	0	1	0	1	0	1	0

so we obtain

$$L_0 = 11001100000000001100110011111111,$$
$$R_0 = 11110000101010101111000010101010.$$

We use the DES key from Example 5.2.1,

$$133457799BBCDFF1,$$

whose binary expansion is

0	0	0	1	0	0	1	1
0	0	1	1	0	1	0	0
0	1	0	1	0	1	1	1
0	1	1	1	1	0	0	1
1	0	0	1	1	0	1	1
1	0	1	1	1	1	0	0
1	1	0	1	1	1	1	1
1	1	1	1	0	0	0	1

We compute the first round key. We have

$$C_0 = 1111000011001100101010101111,$$

$$C_1 = 1110000110011001010101011111,$$
$$D_0 = 0101010101100110011110001111,$$
$$D_1 = 1010101011001100111100011110,$$

and therefore

$$K_1 = 000110110000001011101111111111000111000001110010.$$

Using this key, we obtain

$$E(R_0) \oplus K_1 = 011000010001011110111010100001100110010100100111,$$

$$f(R_0, K_1) = 00000011010010111010100110111011,$$

and finally

$$R_1 = 11001111010010110110010101000100.$$

The other rounds are computed analogously.

5.4 Security of DES

Since its invention, the security of DES has been studied very intensively. Special techniques such as differential and linear cryptanalysis have been invented to attack DES (see [49] and [70]), but the most successful attack has been an exhaustive search of the key space. With special hardware or large networks of workstations, it is now possible to decrypt DES ciphertexts in a few days or even hours. We expect that soon DES will be broken on a single PC as PCs become increasingly Fast.

Today, DES can only be considered secure if triple encryption as described in Section 3.7 is used. In this context, it is important to know that DES is not a group. This means that for two DES keys k_1 and k_2 there is, in general, not a third DES key k_3 such that $\mathrm{DES}_{k_1} \circ \mathrm{DES}_{k_2} = \mathrm{DES}_{k_3}$. If DES were a group, then multiple encryption would not lead to increased security. In fact, the subgroup that the DES encryption permutations generate in the permutation group $S_{64!}$ is at least of order 10^{2499} (see [49]).

5.5 Exercises

Exercise 5.5.1
Verify the example from Section 5.3 and compute the second round.

Exercise 5.5.2
Compute the third round of the encryption in Section 5.3.

Exercise 5.5.3
Prove that $\overline{\mathrm{DES}(m,k)} = \mathrm{DES}(\overline{m}, \overline{k})$ holds for any $m, k \in \{0,1\}^{64}$.

Exercise 5.5.4
Show that C_{16} and D_{16} are obtained from C_1 and D_1 by a circular right shift of one position.

Exercise 5.5.5

1. Suppose that $K_1 = K_2 = \ldots = K_{16}$. Show that all bits in C_1 are equal as well as all bits of D_1.
2. Conclude that there are exactly four DES keys for which all round keys are the same. They are called *weak DES keys*.
3. Determine the four weak DES keys.

Exercise 5.5.6
Which of the functions IP, $E(R) \oplus K$, S_i, $1 \le i \le 8$, P, PC1, and PC2 are linear for a fixed key? Prove the linearity or give a counterexample.