4.5 The Complete Algorithm

The last thing to do is to describe the initial permutation

$$\mathrm{IP}\colon \mathbb{F}_2^{64} \longrightarrow \mathbb{F}_2^{64}.$$

This is done by the following table:

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

The inverse of IP is the final permutation IP^{-1}. For convenience here is the corresponding table:

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

Now the complete DES algorithm DES_k with key $k \in \mathbb{F}_2^{56}$ is the composition

$$\mathbb{F}_2^{64} \xrightarrow{\mathrm{IP}} \mathbb{F}_2^{64} \xrightarrow{R_1(\bullet,k)} \dots \xrightarrow{R_{16}(\bullet,k)} \mathbb{F}_2^{64} \xrightarrow{T} \mathbb{F}_2^{64} \xrightarrow{\mathrm{IP}^{-1}} \mathbb{F}_2^{64}.$$

Here T is the interchange of the left and right 32 bit halves. The effect of this additional interchange is that DES_k^{-1} looks exactly like DES_k except that the order of the rounds is reversed.

Remark. The initial and final permutations maybe lead to a convenient wiring of input and output contacts on small processors. They have no cryptological effect because the cryptanalyst simply may strip them off. For a software implementation they function as brakes—but one must not omit them for a standard conforming implementation.