5 Der gesamte Algorithmus

Nun ist noch die Initial-Permutation

$$IP\colon \mathbf{F}_2^{64} \longrightarrow \mathbf{F}_2^{64}$$

zu beschreiben; das geschieht durch diese Tabelle:

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

Invers zu IP ist die Ausgabe-Permutation IP^{-1}; der Bequemlichkeit halber wird die zugehörige Tabelle ebenfalls angegeben:

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

Der gesamte DES-Algorithmus DES_k zum Schlüssel $k \in \mathbf{F}_2^{56}$ ist nun die Zusammensetzung

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

Dabei ist T die Vertauschung der linken und der rechten 32-Bit-Hälften, die man einschiebt, damit DES_k^{-1} bis auf die umgekehrte Reihenfolge der Runden wie DES_k aussieht.

Anmerkung. Der Sinn von Initial- und Ausgabe-Permutation liegt wohl in einer bequemen Verdrahtung von Input und Output auf kleinen Prozessoren. Kryptologisch ergeben die Permutationen keinen Effekt, da beide ja vom Kryptoanalytiker ohne weiteres abgestreift werden können. Für eine Software-Implementierung wirken sie nur als Bremsen; dennoch dürfen sie nicht weggelassen werden, wenn man keine zum Standard inkompatible Implementation will.