1 Die Kern-Abbildung

Im Innern des DES steckt die „Kern-Abbildung“

$$f\colon \mathbb{F}_2^{32} \times \mathbb{F}_2^{48} \longrightarrow \mathbb{F}_2^{32},$$

die als Input 32 Textbits und einen 48-Bit-Teilschlüssel hat. Zuerst werden die 32 Textbits durch teilweise Wiederholung zu 48 Bits aufgebläht; die „Expansionsabbildung“

$$E\colon \mathbb{F}_2^{32} \longrightarrow \mathbb{F}_2^{48}$$

wird durch die folgende Tabelle beschrieben:

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

Die Tabelle ist so zu interpretieren dass

$$E(b_1 b_2 \dots b_{32}) = b_{32} b_1 b_2 b_3 \dots b_{31} b_{32} b_1.$$

Die expandierten 48 Bits werden mit dem 48-Bit-Teilschlüssel per $\oplus$ überlagert. Die resultierenden 48 Bits werden in 8 Gruppen zu je 6 Bits zerteilt und auf diese die 1. bis 8. S(ubstitutions)-Box

$$S_j\colon \mathbb{F}_2^6 \longrightarrow \mathbb{F}_2^4 \quad (j = 1, \dots, 8)$$

angewendet. Die S-Boxen werden im nächsten Abschnitt beschrieben.

Insgesamt erhält man die (polyalphabetisch zusammengesetzte) Substitution

$$S\colon \mathbb{F}_2^{48} \longrightarrow \mathbb{F}_2^{32}.$$

Schließlich wird noch die P(ermutations)-Box

$$P\colon \mathbb{F}_2^{32} \longrightarrow \mathbb{F}_2^{32}$$

ausgeführt, die durch die folgende Tabelle beschrieben wird; das heißt,

$$P(b_1 b_2 \dots b_{32}) = b_{16} b_7 \dots b_4 b_{25}.$$

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

Zusammengefasst wird die Kernabbildung in der folgenden Abbildung: