4.1 The Kernel Map

The innermost layer of DES is the “kernel map”

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

that takes 32 text bits and 48 key bits as input. First some of the 32 text bits are repeated, blowing them up to 48 bits. This “expansion map”

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

is given by the following table:

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

The correct interpretation of this table is

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

The expanded 48 bits and the 48 bit partial key are added (as binary vectors). The resulting 48 bits are divided into 8 groups each consisting of 6 bits. These groups are fed into the S-boxes 1 to 8:

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

The description of the S-boxes is in the next section.

The S-boxes together make up the substitution

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

Finally we apply the “P-box” (permutation)

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

that is given by the following table meaning

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

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

The complete kernel map is in the following figure: