4.4 The Key Selection

To complete the description of the rounds we have yet to describe the key selection. First we expand the 56 bit key to 64 bits by appending a parity bit after each 7 bit subblock. However it doesn't matter which bit we append: the additional bits never enter the algorithm. In any case the first step is a map

$$\mathrm{Par}\colon \mathbb{F}_2^{56} \longrightarrow \mathbb{F}_2^{64}.$$

In the second step we extract the original 56 bits, but in a different order, given by the following table.

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

We have constructed a map

$$\mathrm{PC}_1\colon \mathbb{F}_2^{64} \longrightarrow \mathbb{F}_2^{56}$$

("Permuted Choice 1"). Now we divide the 56 bits into two 28 bit halves, and cyclically shift these to the left, all in all 16 times. This gives 16 maps

$$\mathrm{LS}_i\colon \mathbb{F}_2^{28} \longrightarrow \mathbb{F}_2^{28} \quad (i = 1, \ldots 16).$$

the amount of the shifts is given by the table:

1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

The first two shifts are by one bit, the next 6 ones by two bits, and so on. To get the i-th key selection A_i we apply the "Permuted Choice 2" after the i-th shift:

$$\mathrm{PC}_2\colon \mathbb{F}_2^{56} \longrightarrow \mathbb{F}_2^{48}$$

where the 48 bits are chosen in the order of the following table (omitting the bits 9, 18, 22, 25, 35, 38, 43, 54).

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

The complete key selection is

$$A_i = \mathrm{PC}_2 \circ \mathrm{LS}_i \circ \cdots \circ \mathrm{LS}_1 \circ \mathrm{PC}_1 \circ \mathrm{Par}\,.$$

We summarize this construction in the following diagram: