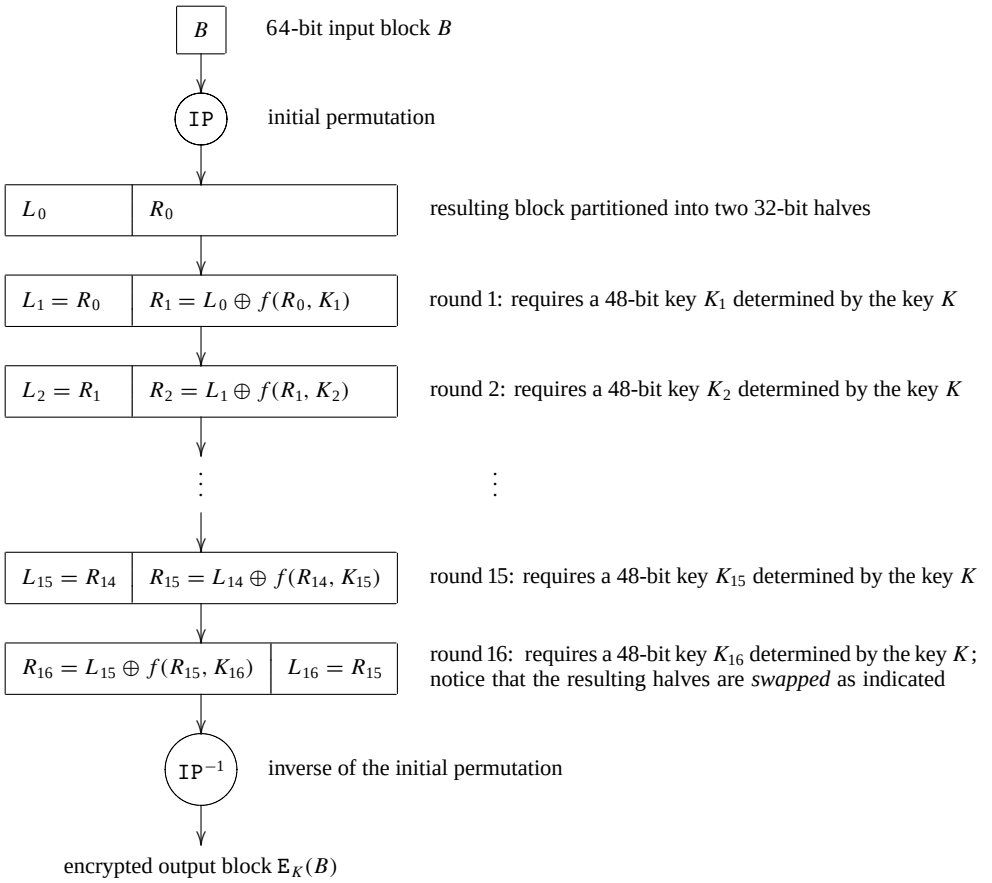

Figure 3.4. Coarse structure of the DES algorithm in its encryption state, operating on a 64-bit input block B in the electronic codebook (ECB) mode.

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

Figure 3.5. The initial permutation IP of the 64-bit input block B. The 50th bit of B renders the second bit of IP(B), the 52nd bit of B will be the 10th bit of IP(B), etc.

the details of constructing C_0 and D_0. The first table lists C_0: the 57th bit of K is the first bit of C_0, the 58th bit of K is the 9th bit of $C_0, \ldots$; the second table specifies D_0 in the same manner. Notice that the numbers $8, 16, \ldots, 64$ are all absent from these tables, since they are merely parity bits and not part of the actual 56-bit key. Before computing K_i, we compute blocks C_i and D_i as circular left shifts of their previous version C_{i-1}