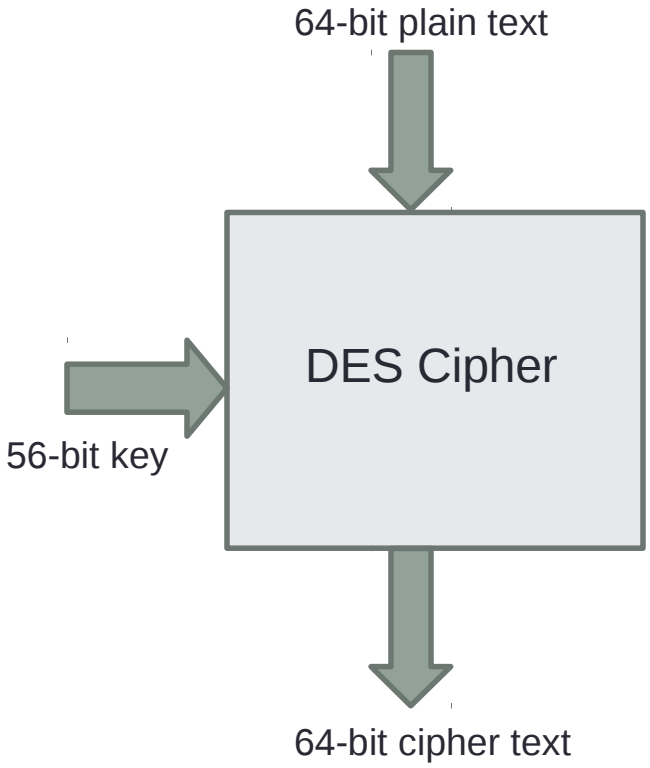
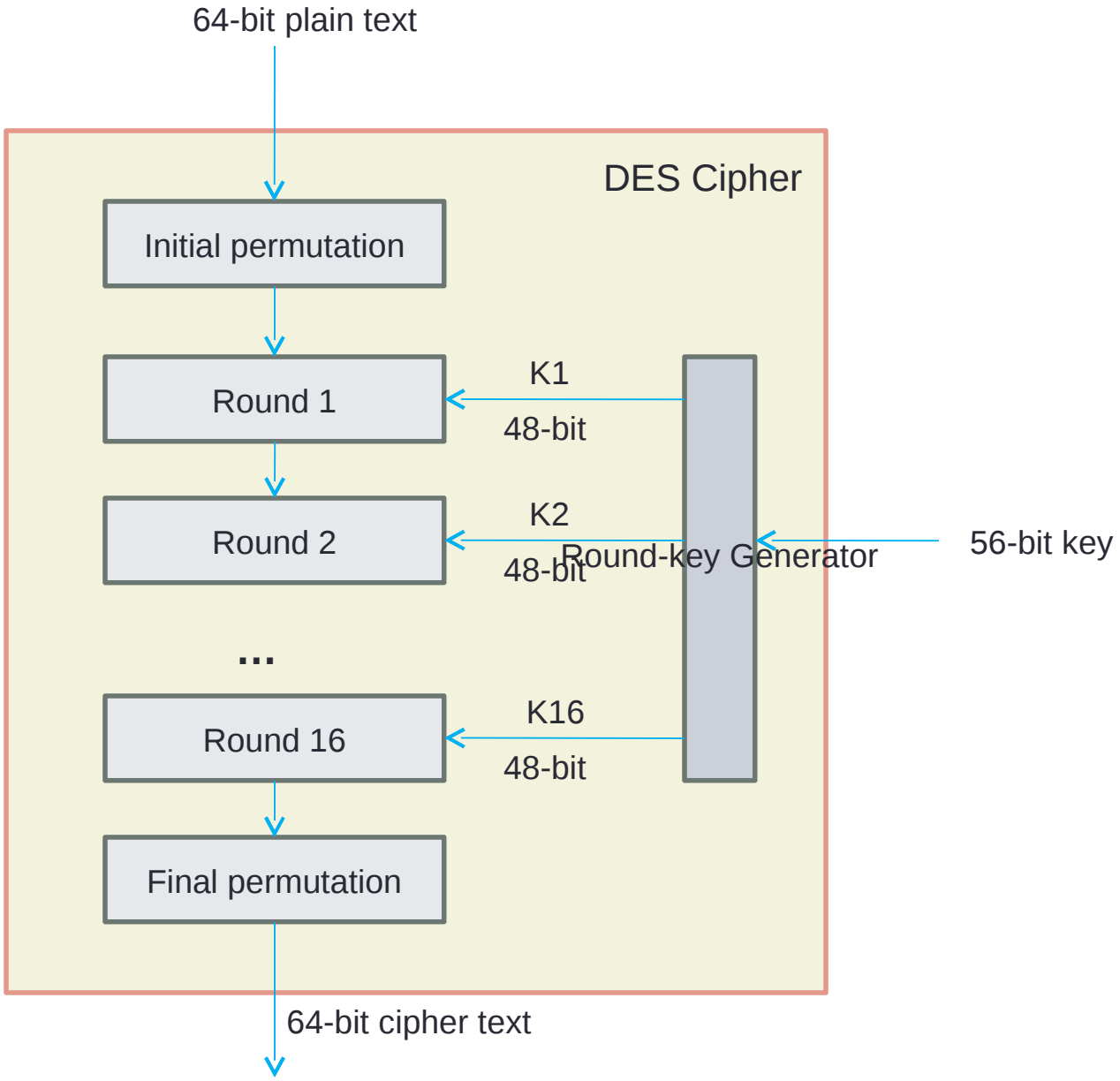
DES is a Block cipher, which takes 64-bit plain text and creates a 64-bit cipher text



General Structure of DES



Initial and Final permutations

Initial permutation table

58	50	42	34	26	18	10	02
60	52	44	36	28	20	12	04
62	54	46	38	30	22	14	06
64	56	48	40	32	24	16	08
57	49	41	33	25	17	09	01
59	51	43	35	27	19	11	03
61	53	45	37	29	21	13	05
63	55	47	39	31	23	15	07

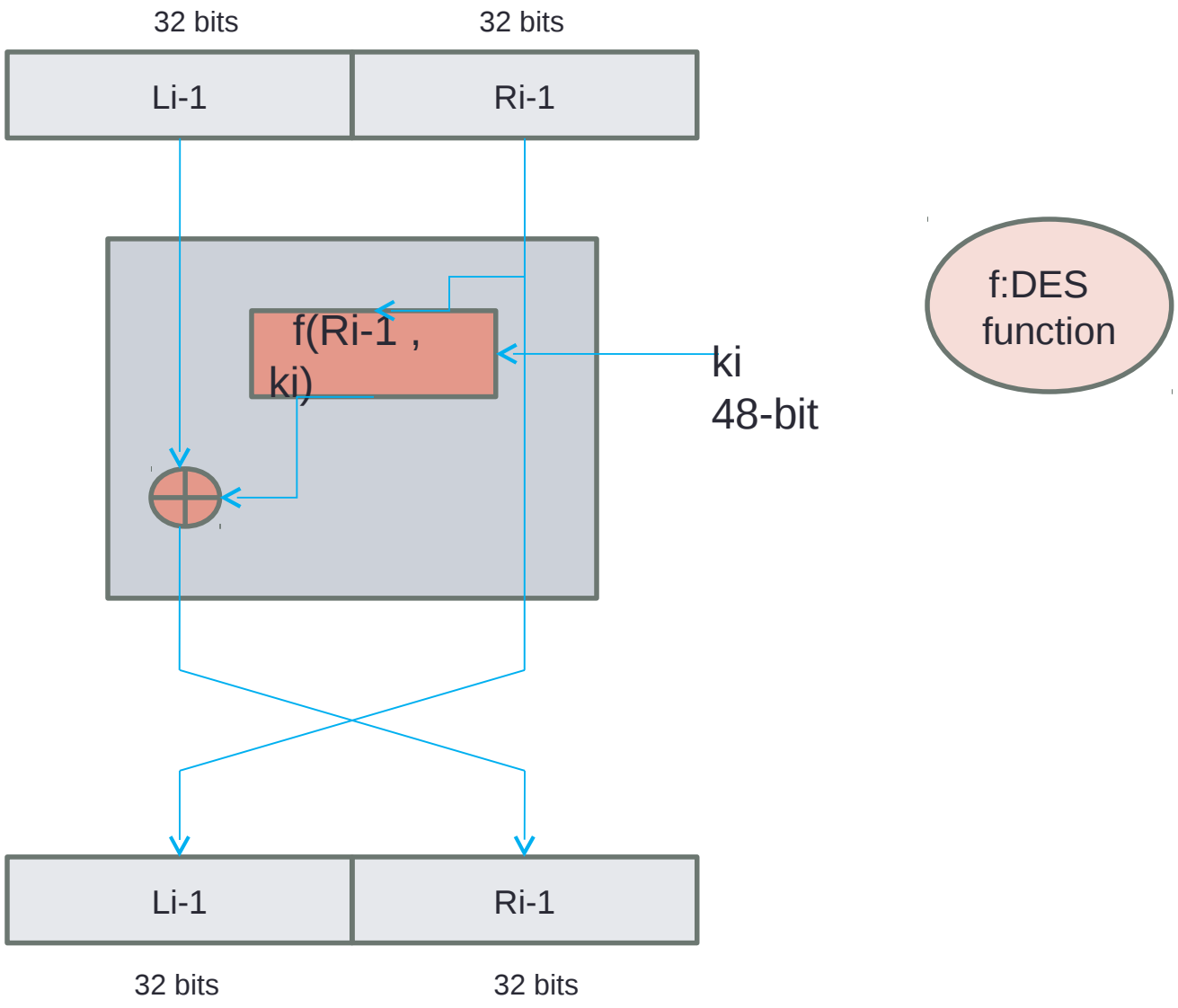
The 58th bit of the input 64-bit plain text becomes the 1st bit, the 50th bit becomes the 2nd bit and so on according to the initial permutation table

Final permutation table

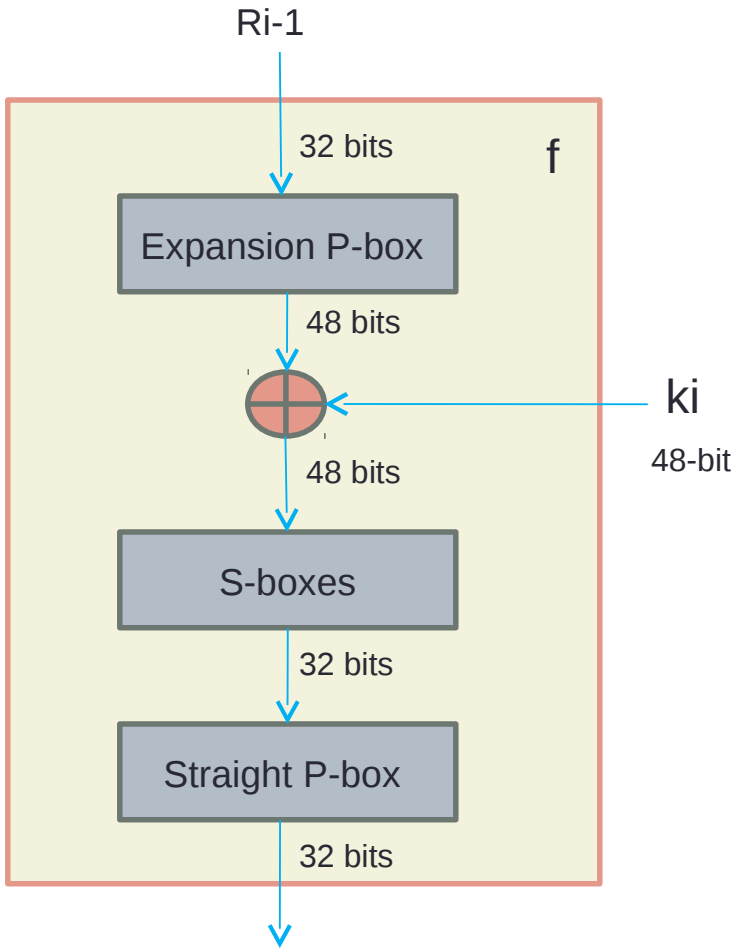
40	08	48	16	56	24	64	32
39	07	47	15	55	23	63	31
38	06	46	14	54	22	62	30
37	05	45	13	53	21	61	29
36	04	44	12	52	20	60	28
35	03	43	11	51	19	59	27
34	02	42	10	50	18	58	26
33	01	41	09	49	17	57	25

The 40th bit of the 64-bit output of the Round 16 becomes the 1st bit, the 8th bit becomes the 2nd bit and so on according to The final permutation table

One round in DES (Feistel structure)

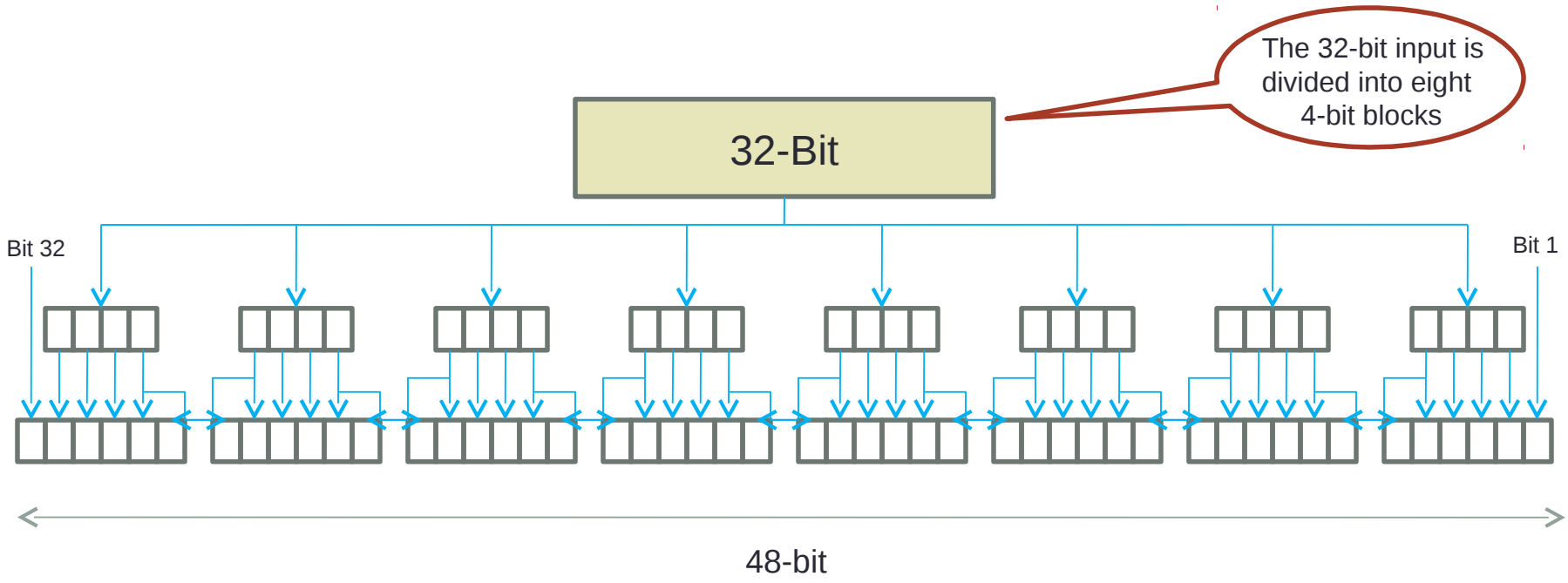


DES Function



DES Function : Expansion permutation

The input 32-bits are expanded to 48 bits in the Expansion P-Box module in the following way



The resulting 48-bit output is permuted using the Expansion P-Box

DES Function : Expansion Permutation and Straight permutation

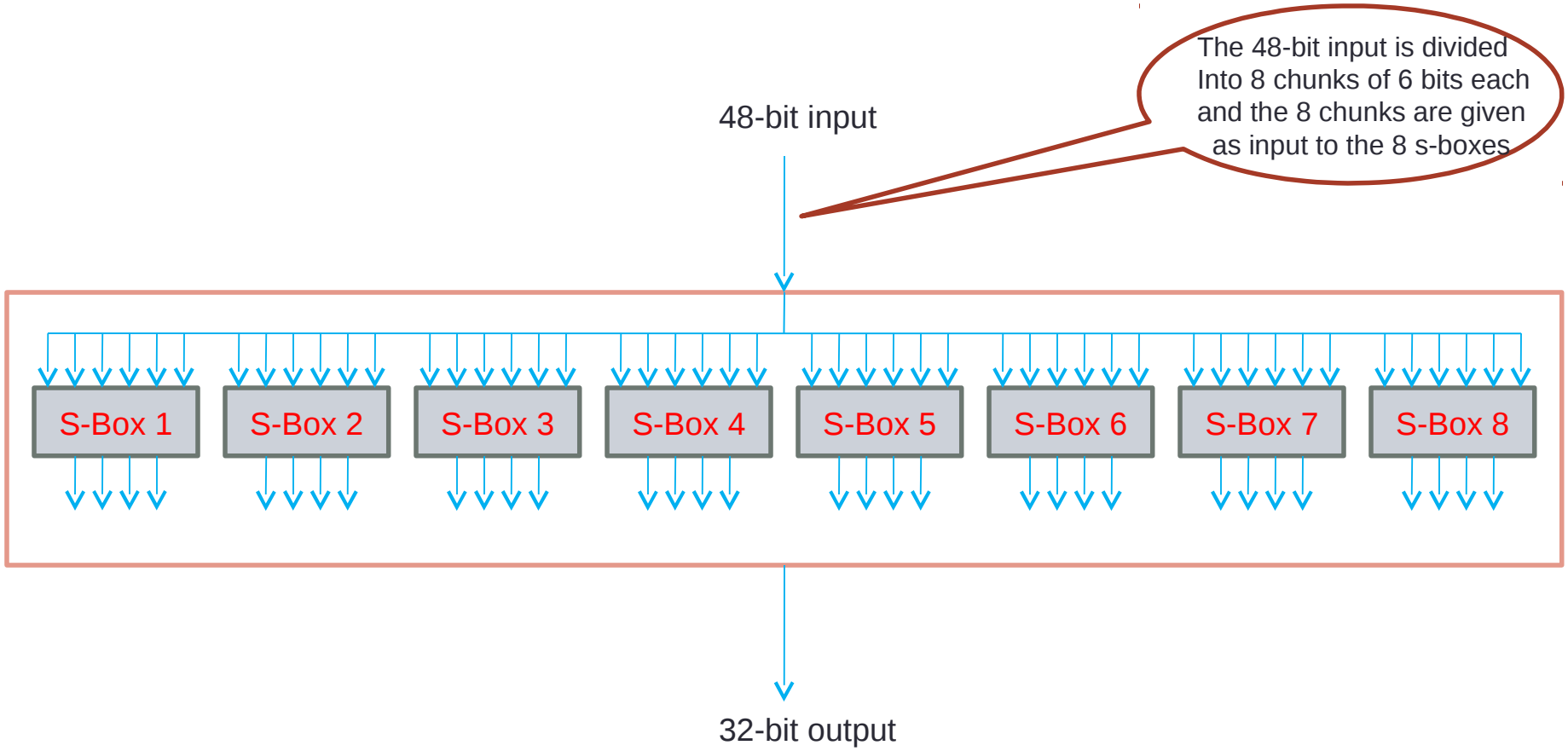
Expansion P-box

32	01	02	03	04	05
04	05	06	07	08	09
08	09	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	01

Straight P-box

16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

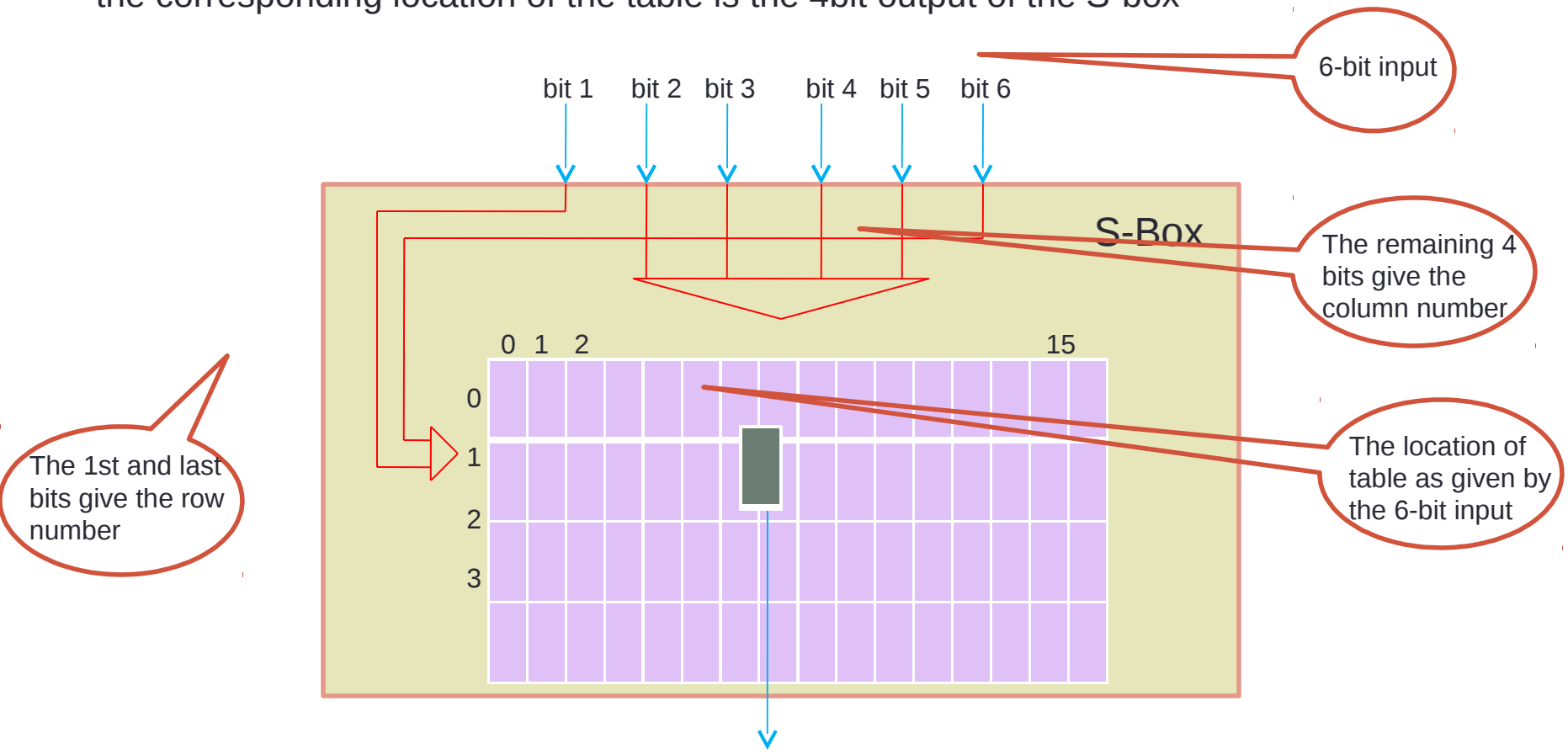
DES Function : Substitution Boxes



The output of each S-box is 4-bit. When these are combined the result is a 32-bit output

DES Function : Substitution Boxes

Each S-box uses a corresponding 4 row by 16 column table
Given a 6-bit input, the 1st and the 6th bits are used to address one of the rows and the remaining 4 bits are used to address one of the 16 columns. Finally, the value found in the corresponding location of the table is the 4bit output of the S-box



DES Function : Substitution Boxes

An Example

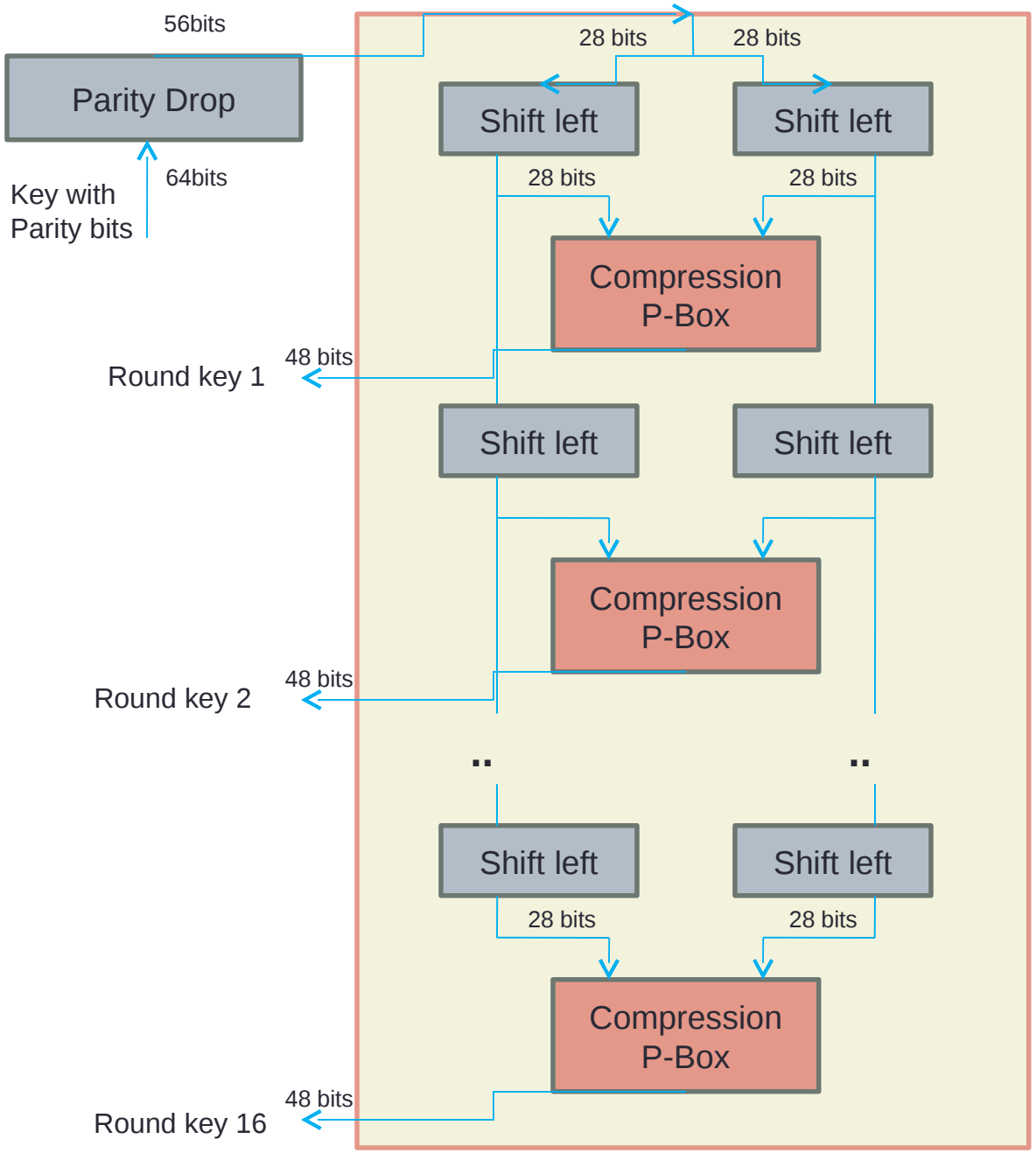
Consider the 6-bit input to s-box 1 is 100011
The 1st and last bits put together is 11 which is ‘3’ in decimal. So we select the 3rd row
The middle bits are 00001 which is ‘1’ in decimal. So we select the 1st column

The corresponding table for S-box 1 is shown below

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	10	03	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

The value in the 3rd [illegible] in binary)

Key Generation



Shifting

Rounds	Shift
1,2,9,16	One bit
Others	Two bits

Parity Drop and Compression Permutation

The parity drop module drops the parity bits (bits 8,16,24,..,64) from the 64-bit key and permutes the rest of the 56 bits according to the parity drop table

The Compression permutation module changes the 56 bits to 48 bits using the key compression table, which are used as the key for a round

Parity drop table

57	49	41	33	25	17	09	01
58	50	42	34	26	18	10	02
59	51	43	35	27	19	11	03
60	52	44	36	63	55	47	39
31	23	15	07	62	54	46	38
30	22	14	06	61	53	45	37
29	21	13	05	28	20	12	04

Key compression table

14	17	11	24	01	05	03	28
15	06	21	10	23	19	12	04
26	08	16	07	27	20	13	02
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32