Simplified DES

Why S-DES?

- DES is a complex algorithm for conventional encryption, it encode the plaintext to ciphertext with a secret key.
- It is used as realistic, and too difficult to educate the student well know the DES basics. A lot data to be fed into the algorithm, hand writing is impossible!
- Thus, simplified DES is developed with Edward Schaefer, professor at Santa Clara University. It's a good teaching tool for student to realize the operations of DES.

Conventional Cryptography Algorithm

- Five ingredients,
  - Plaintext
  - Secret Key
  - Encryption algorithm
  - Ciphertext
  - decryption algorithm
- All operations of encryption and decryption are based on two basic kinds of manipulations on the data.
  - Permutation
  - Substitution

Permutation & Subistitution in S-DES

IP							
2	6	3	1	4	8	5	7

IP^{-1}							
4	1	3	5	7	2	8	6

P10									
3	5	2	7	4	10	1	9	8	6

P8							
6	3	7	4	8	5	10	9

E/P							
4	1	2	3	2	3	4	1

P4			
2	4	3	1

S0 =

	0	1	2	3
0	1	0	3	2
1	3	2	1	0
2	0	2	1	3
3	3	1	**3**	2

S1 =

	0	1	2	3
0	0	1	2	3
1	2	0	1	3
2	3	0	1	0
3	**2**	1	0	3

Figure 1: Simplified DES Scheme

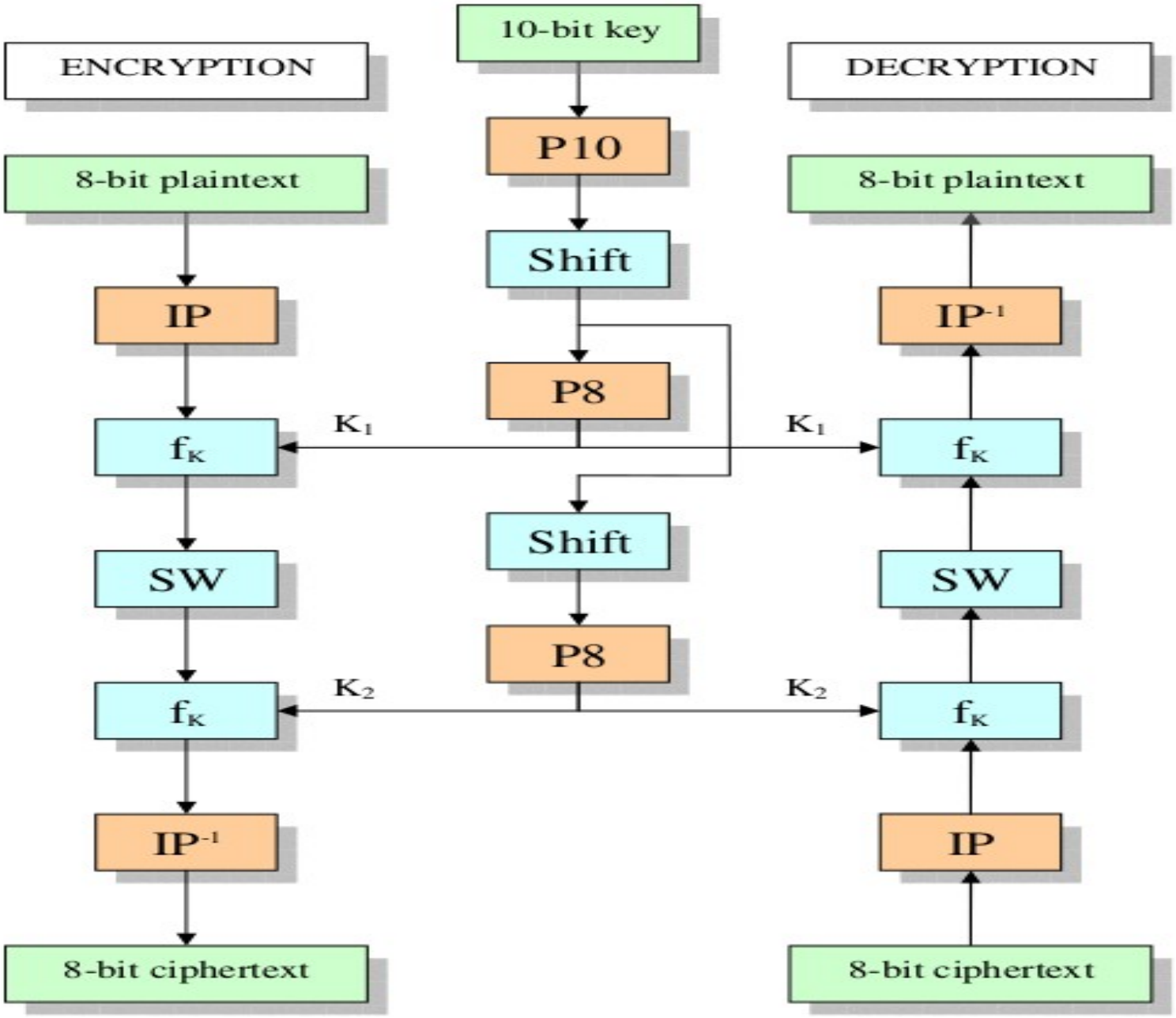


Figure 2: Key Generation for Simplified DES

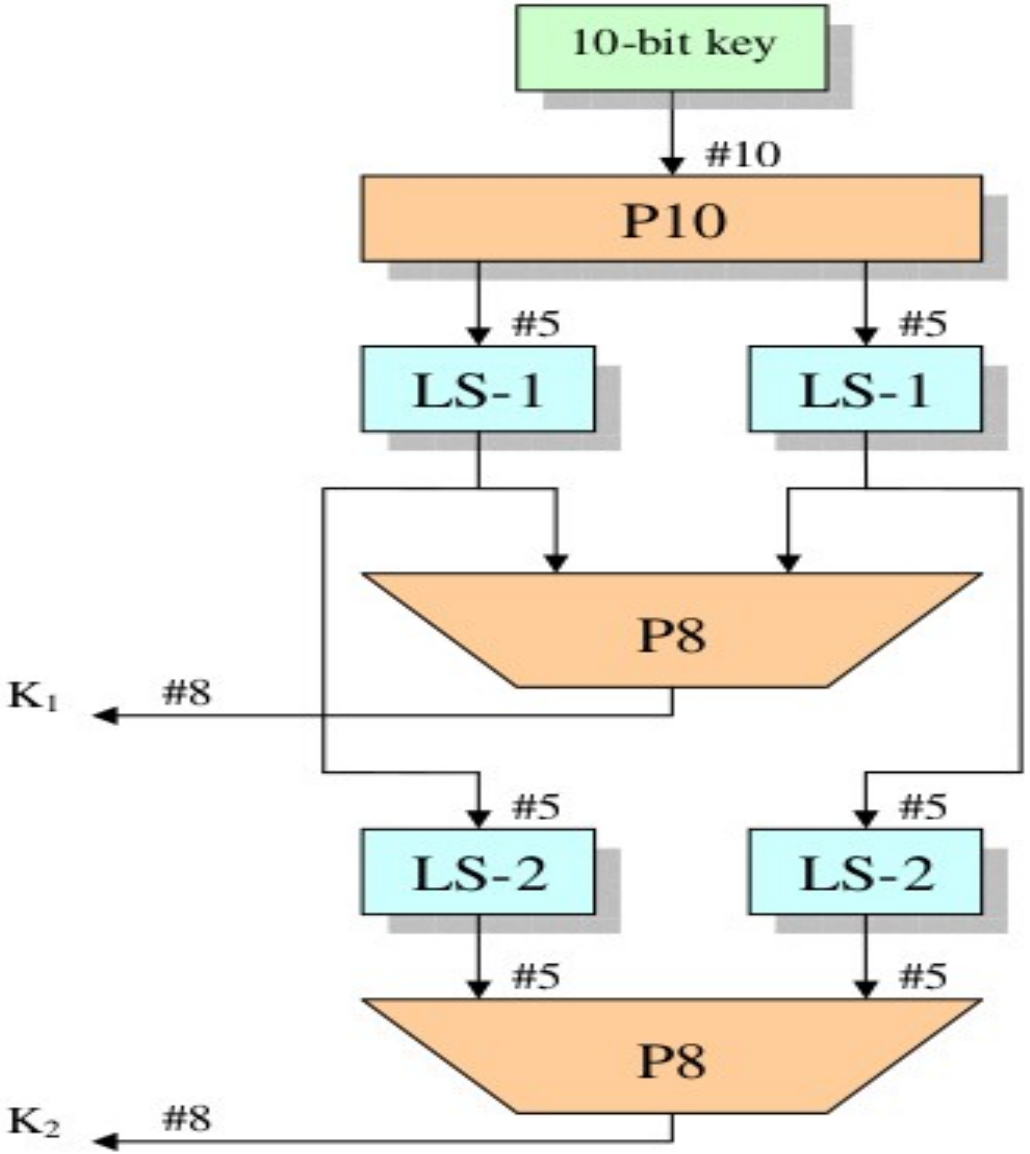
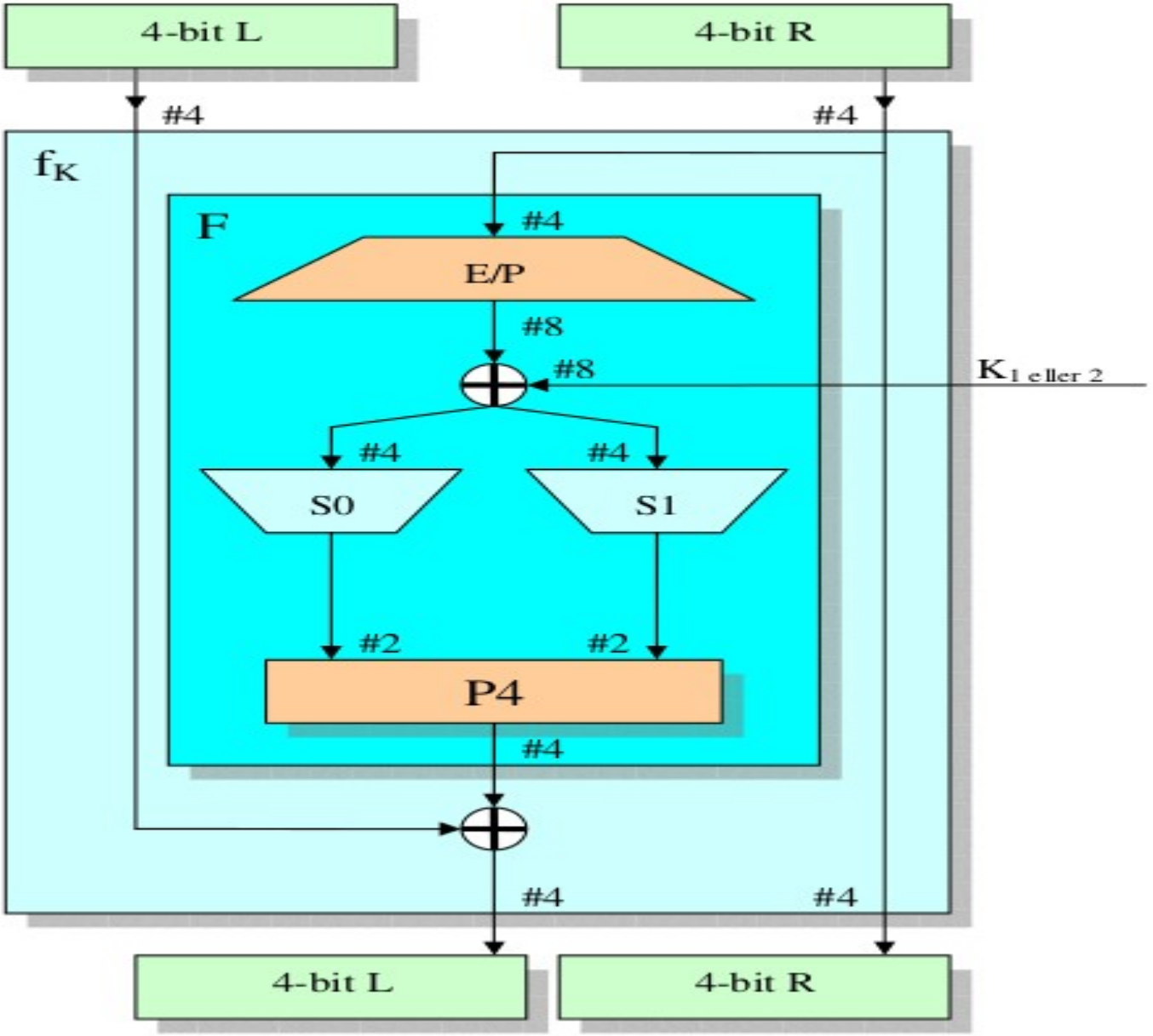
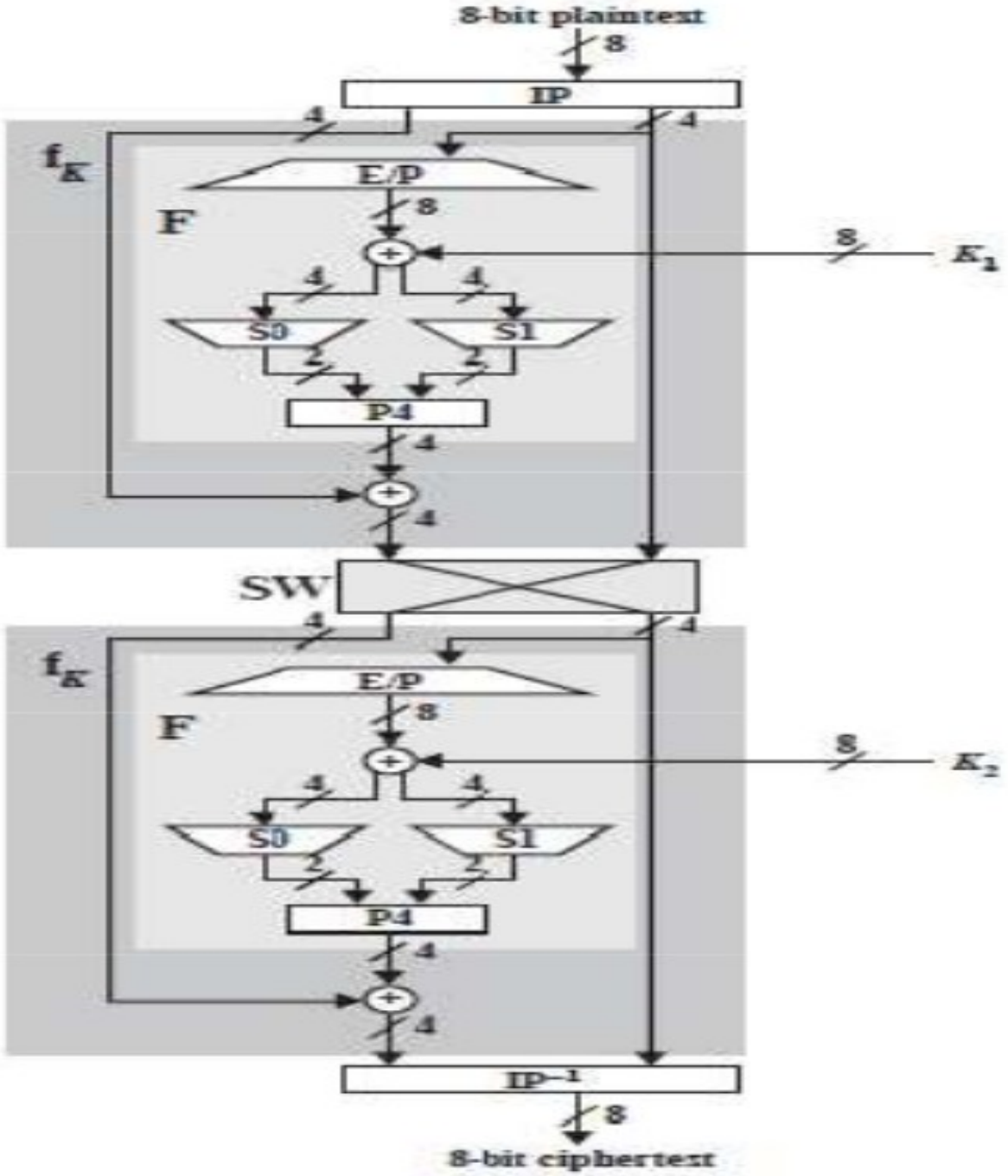


Figure 2: Key Generation for Simplified DES.

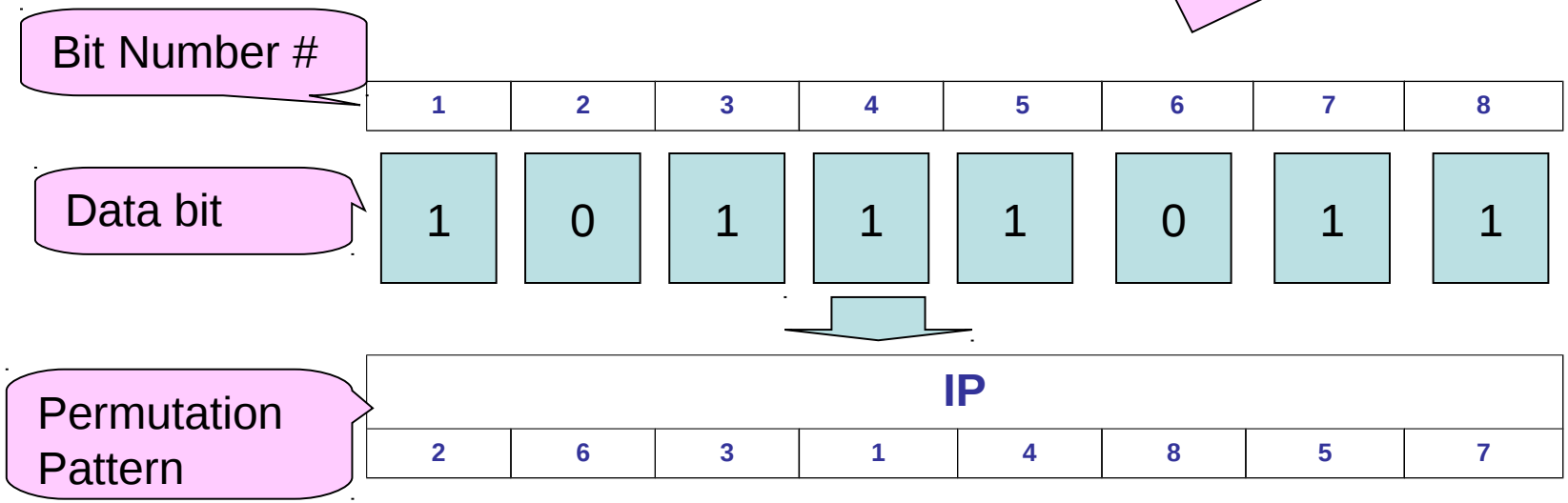
Figure 3: Simplified DES Scheme Encryption Detail




8-bit plaintext
8
IP
4
4
f_K
E/P
F
8
8
K_1
4
4
S0
S1
2
2
P4
4
4
SW
4
4
f_K
E/P
F
8
8
K_2
4
4
S0
S1
2
2
P4
4
4
IP^{-1}
8
8-bit ciphertext

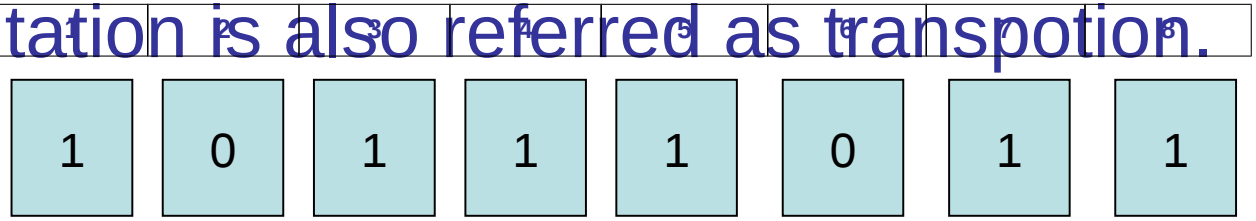
Permutation

This animation shows how the bits will be arranged from the permutation pattern.



Permutation

- Permutation is to rearrange the locations of the bits of data according to the permutation pattern. Permutation is also referred as transpotion.



Substitution

This animation shows how the substitution process will be done.

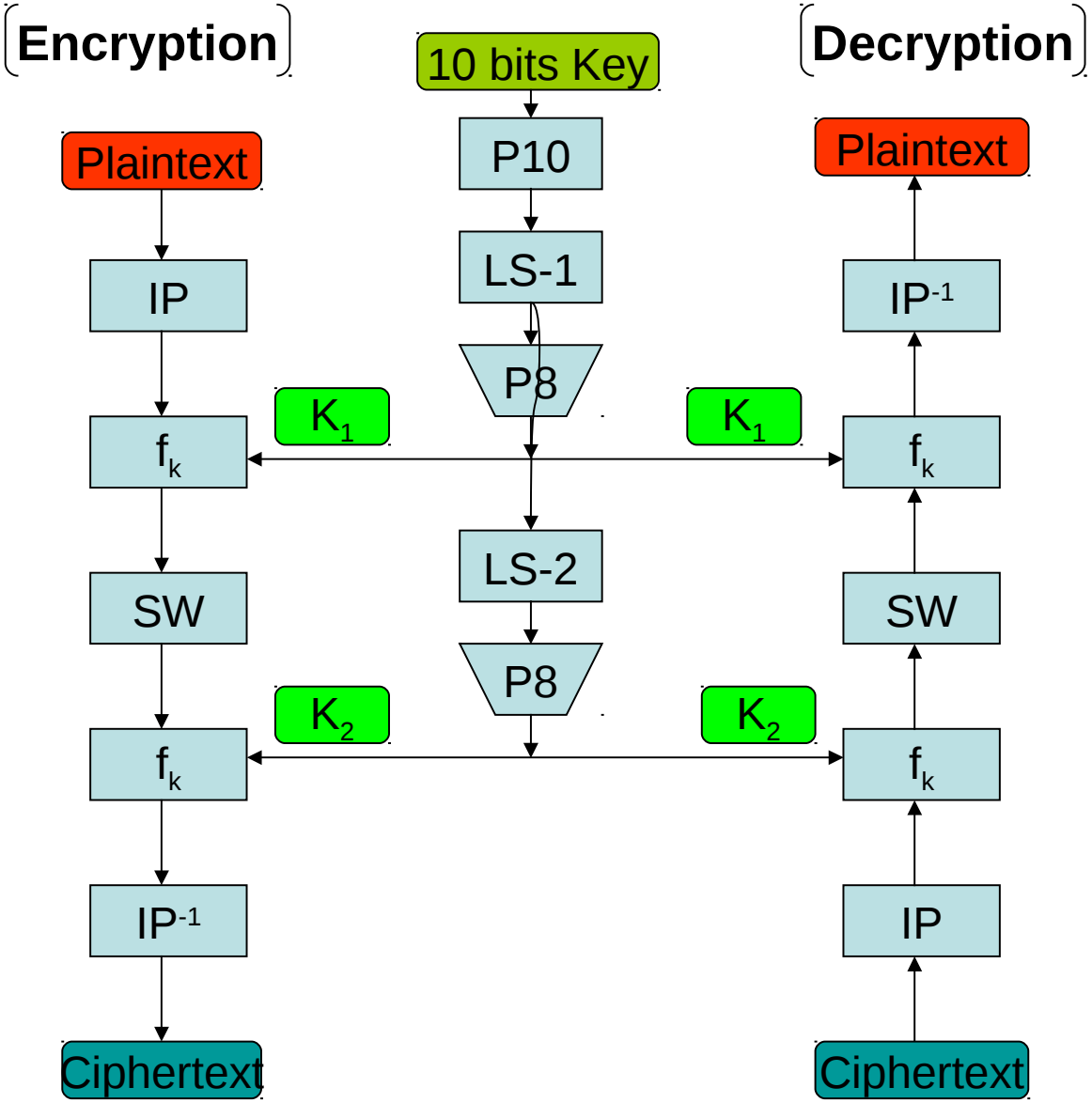
0	1	0	0

0	0	0	0	0	1
0	0	0	1	1	1
0	0	1	0	0	0
0	0	1	1	1	0
0	1	0	0	1	1
0	1	0	1	0	1
0	1	1	0	1	0
0	1	1	1	0	0
1	0	0	0	0	0
1	0	0	1	1	1
1	0	1	0	1	0
1	0	1	1	0	1
1	1	0	0	0	1
1	1	0	1	1	1
1	1	1	0	1	1
1	1	1	1	1	0

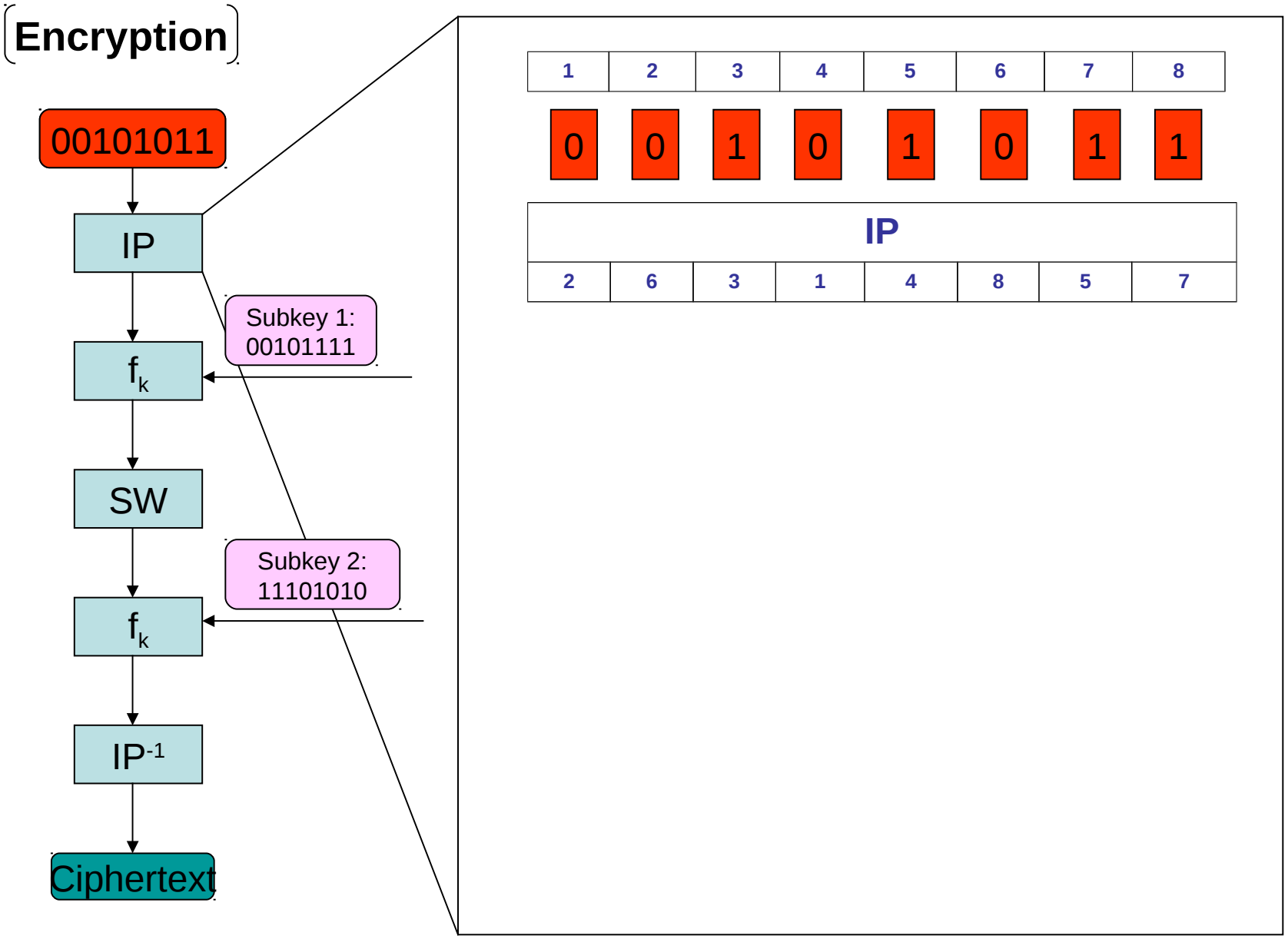
Substitution Box (Known as S-Box)

After the operation, the data “0100” is substituted with “11”.

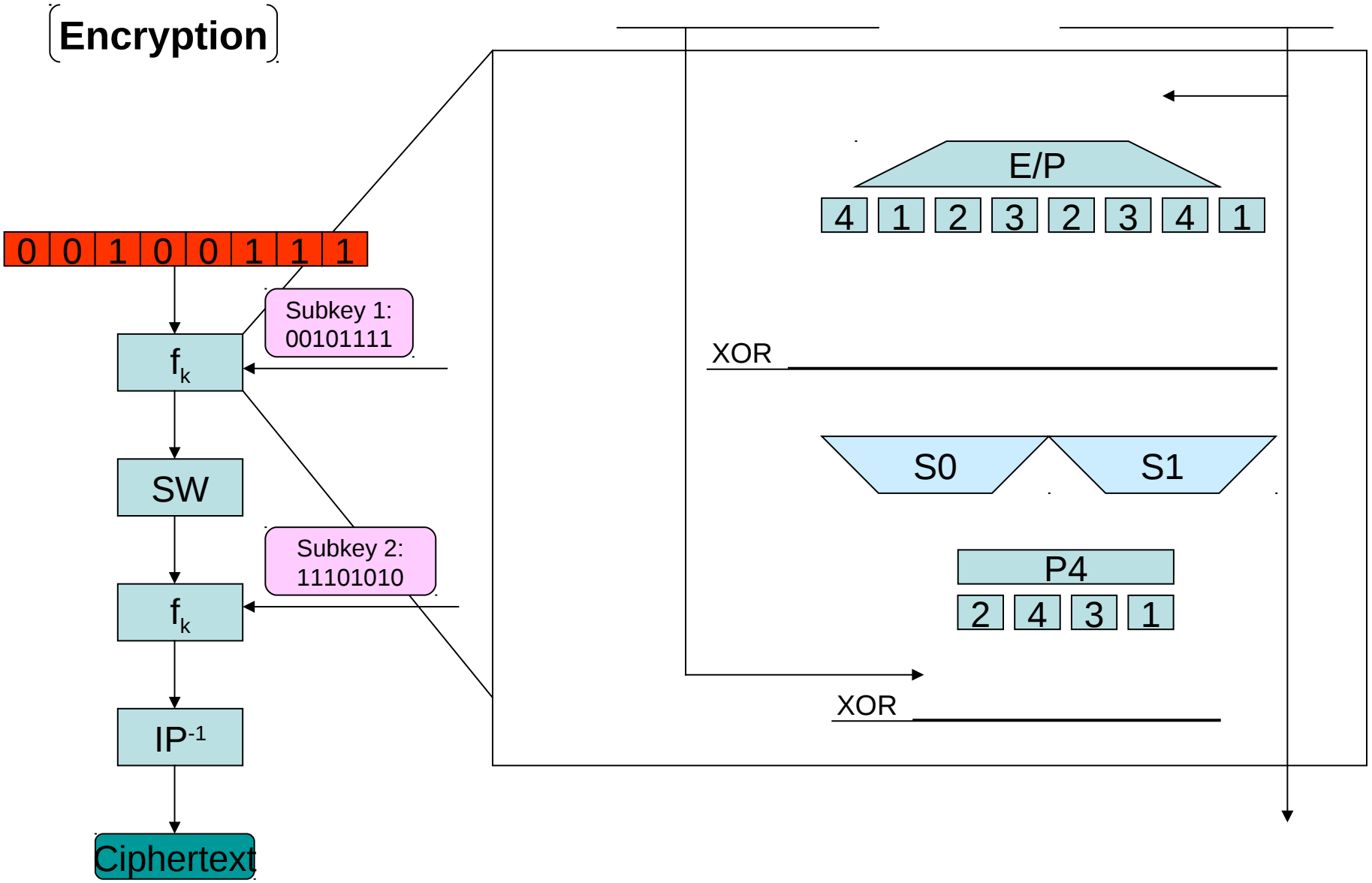
S-DES Flow Diagram



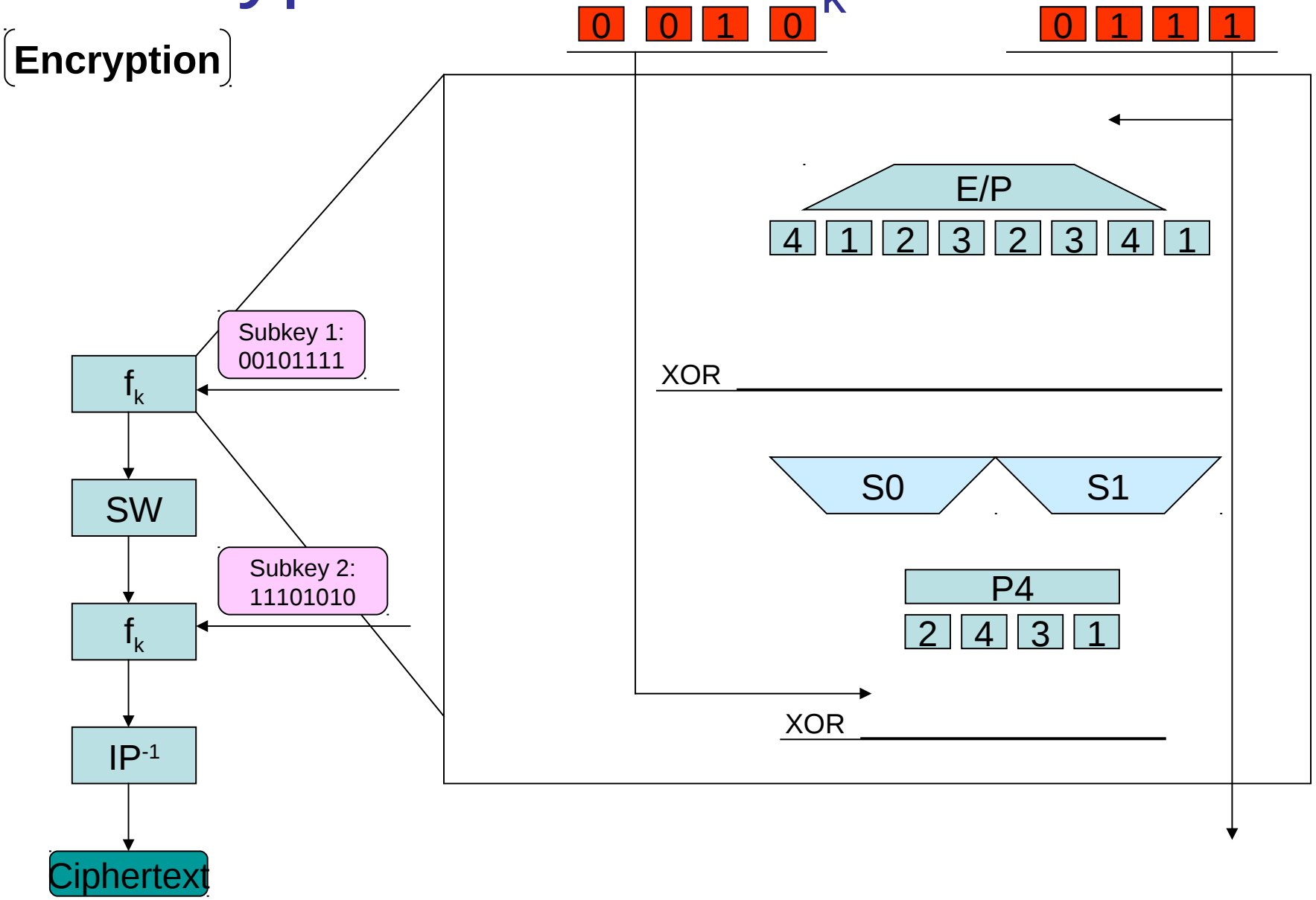
Encryption Phase IP of S-DES



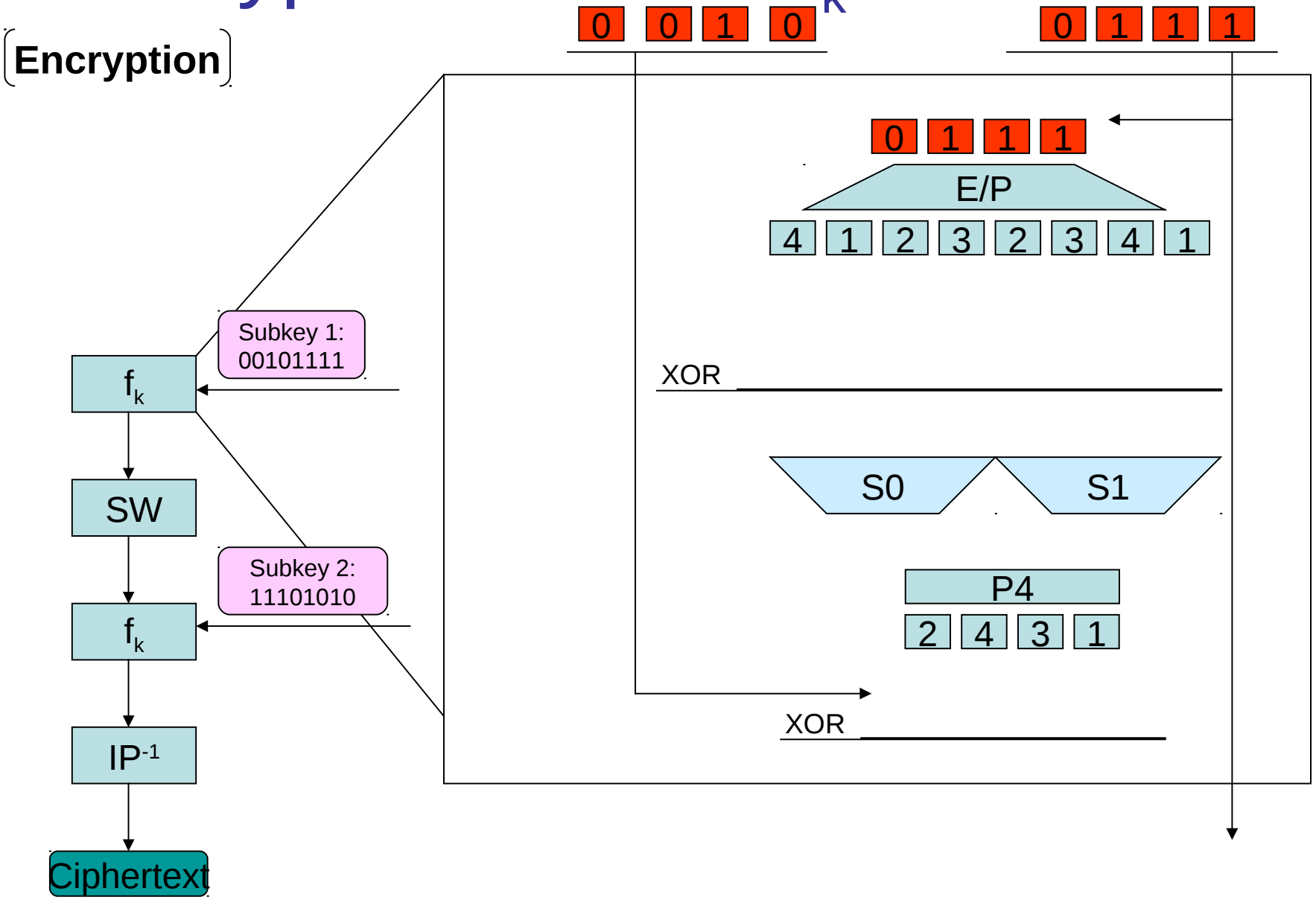
Encryption Phase F_k of S-DES



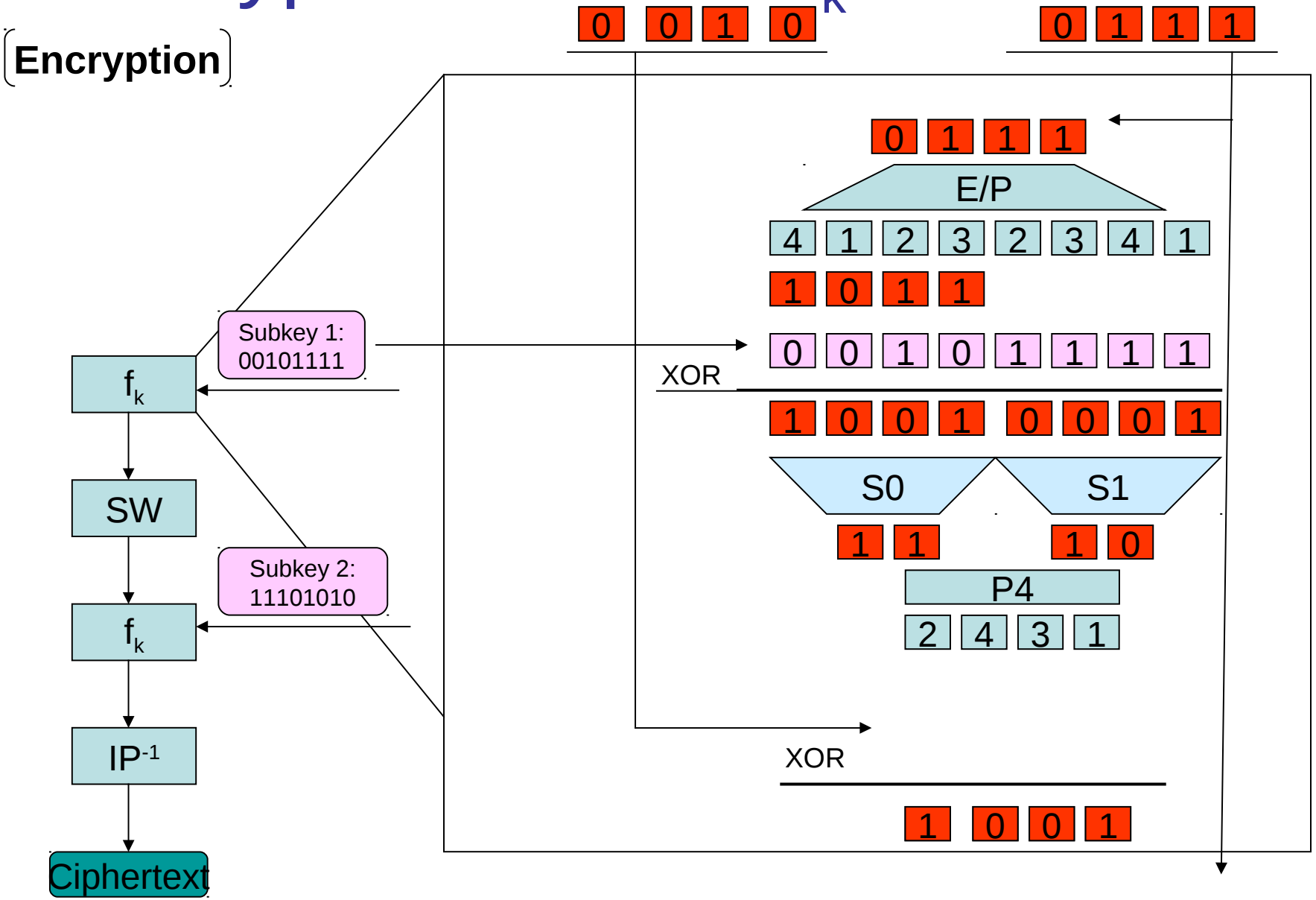
Encryption Phase F_k of S-DES



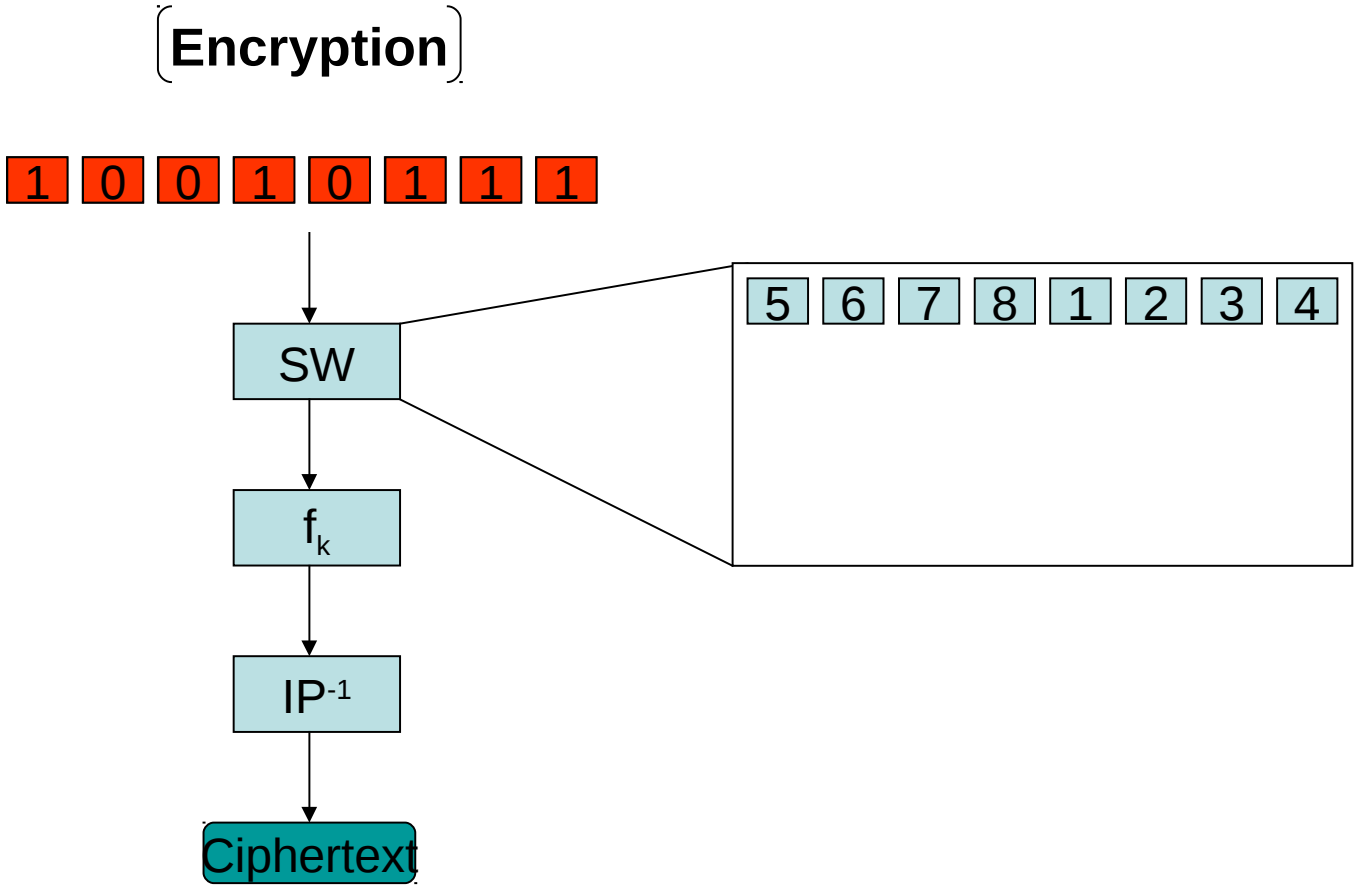
Encryption Phase F_k of S-DES



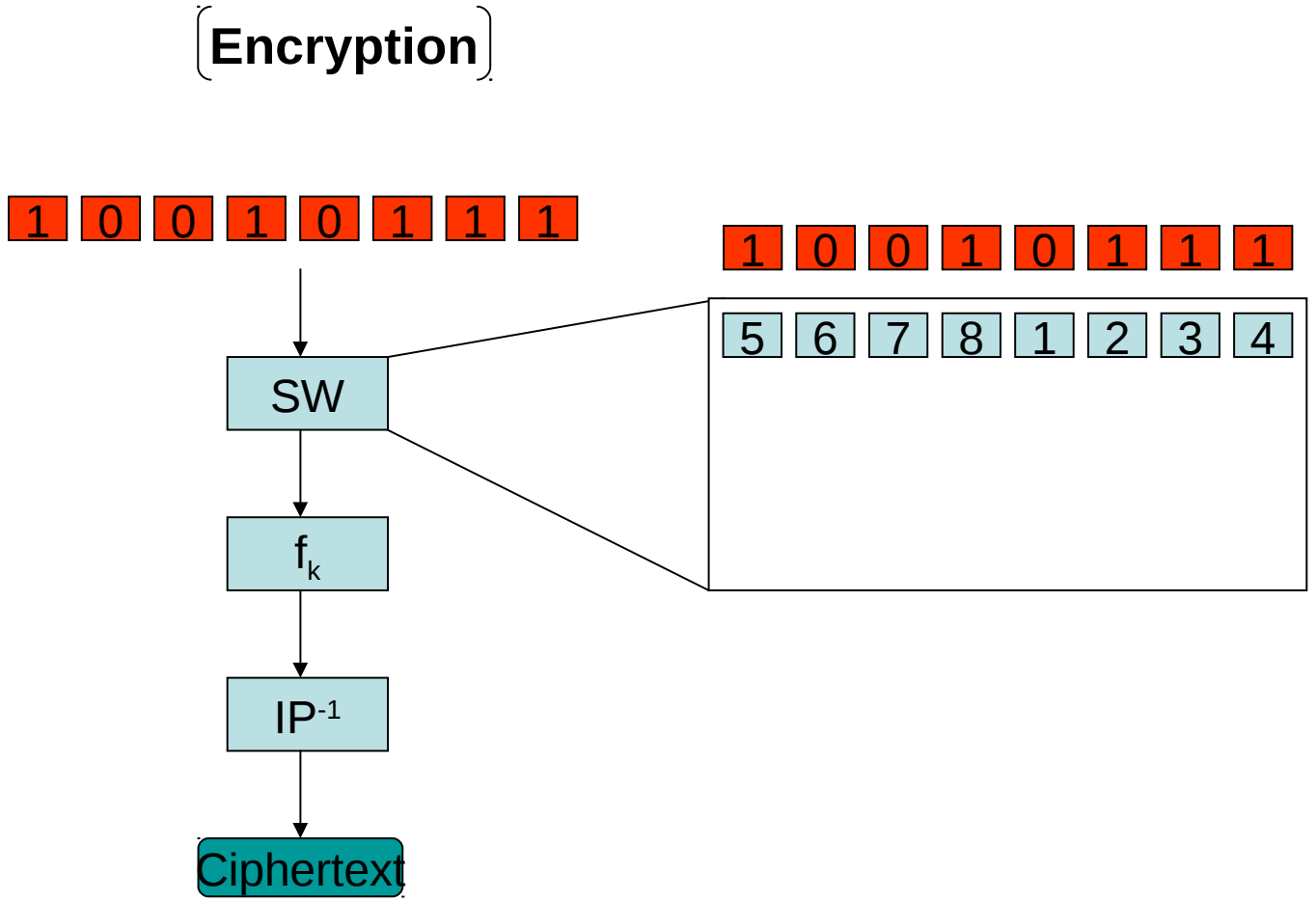
Encryption Phase F_k of S-DES



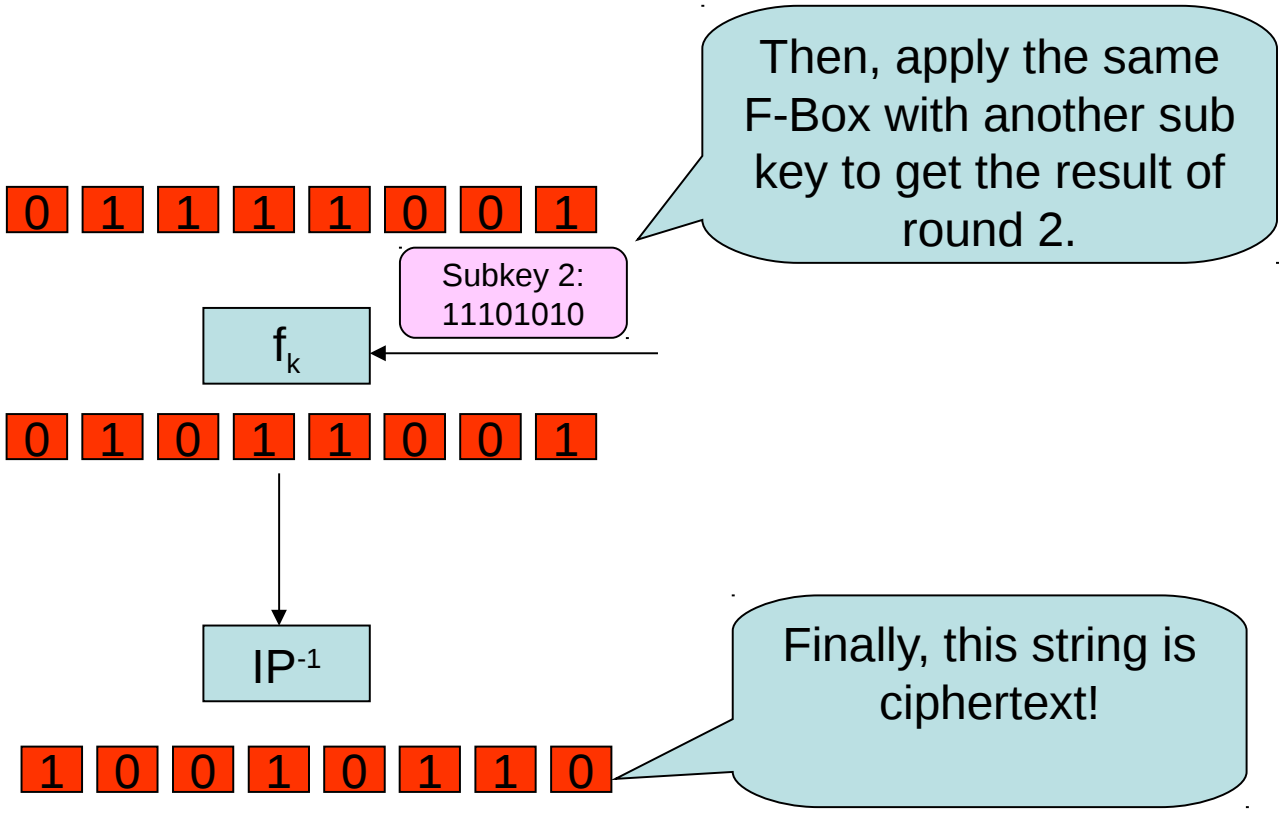
Encryption Round 2 of S-DES



Encryption Round 2 of S-DES



Encryption Round 2 of S-DES



Thanks for your attention!

^_^