## 1.1 CONVENTIONAL AND PUBLIC-KEY CRYPTOGRAPHY

## CONVENTIONAL CRYPTOGRAPHY: SYMMETRIC KEY CIPHERS:

### SDES

Symmetric ciphers use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. They are faster than asymmetric ciphers and allow encrypting large sets of data. However, they require sophisticated mechanisms to securely distribute the secret keys to both parties

### SDES- SIMPLIFIED DATA ENCRYPTION STANDARD

The most widely used encryption scheme is based on the Data Encryption Standard (DES) adopted in 1977.

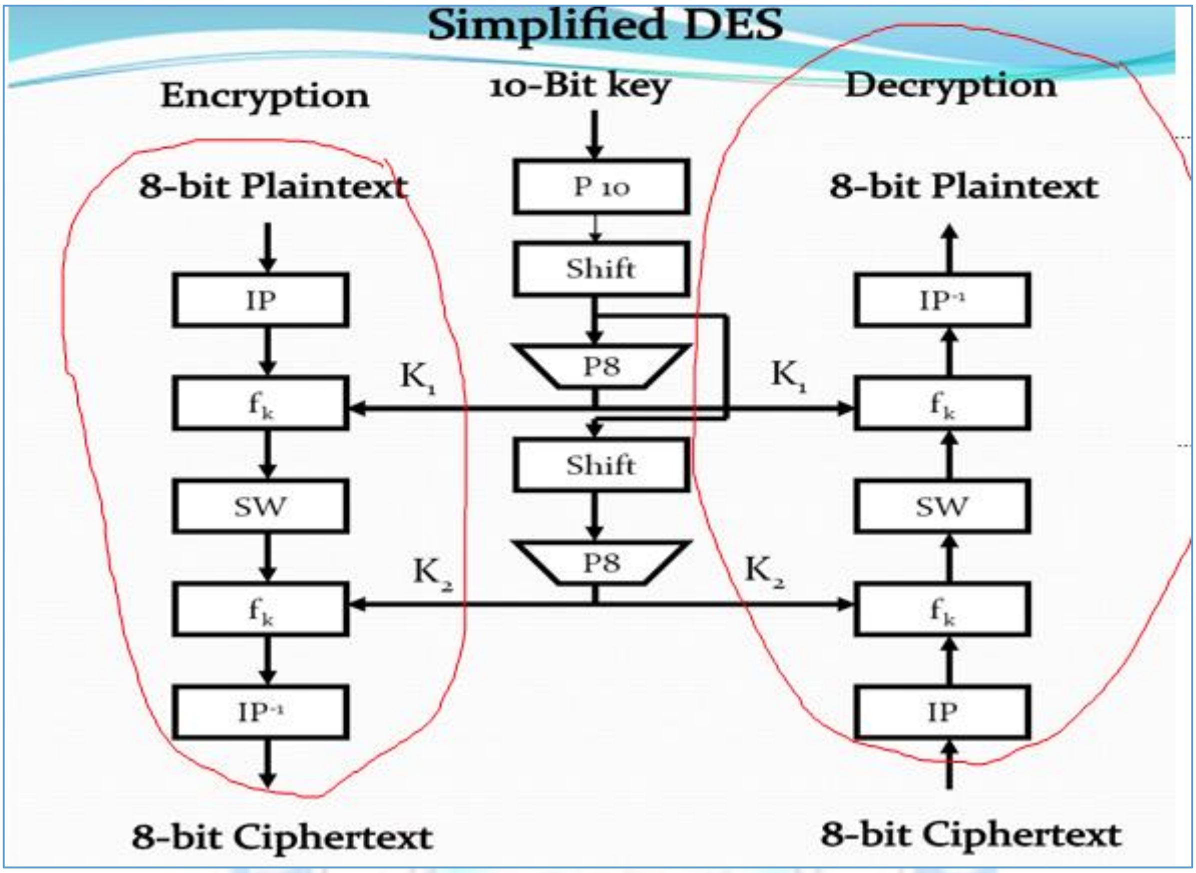
### Encryption

Takes an 8-bit block of plaintext and a 10-bit key as input and produces an 8-bit of cipher.

### Decryption

Takes an 8-bit block of cipher and the same 10-bit key as input and produces an 8-bit of original plaintext.

- Both substitution and transposition operations are used
- It is a complex, multi-phase algorithm



The encryption algorithm involves five functions:

1. An initial permutation (IP)
2. A complex function labeled fk, which involves both permutation and substitution operations and depends on a key input.
3. A simple permutation function that switches (SW) the two halves of the data.
4. The function fk again.
5. A permutation function that is the inverse of the initial permutation

## Key Generation

- The function fk takes as input not only the data passing through the encryption algorithm, but also an 8-bit key. Here a 10-bit key is used from which two 8-bit subkeys are generated.

- The key is first subjected to a permutation (P10). Then a shift operation is performed.
- The output of the shift operation then passes through a permutation function that produces an 8-bit output (P8) for the first subkey (K1).
- The output of the shift operation also feeds into another shift and another instance of P8 to produce the second subkey (K2)

The encryption algorithm can be expressed as a composition of functions:

$IP^{-1}$ o fK2 o SW o fk1 o IP, which can also be written as

Ciphertext = $IP^{-1}$ (fK2 (SW (fk1 (IP (plaintext)))))

Where

K1 = P8 (Shift (P10 (Key)))

K2 = P8 (Shift (shift (P10 (Key))))

Decryption can be shown as Plaintext = $IP^{-1}$ (fK1 (SW (fk2 (IP (ciphertext)))))

**S-DES Key Generation**

S-DES depends on the use of a 10-bit key shared between sender and receiver. From this key, two 8-bit subkeys are produced for use in particular stages of the encryption and decryption algorithm

First, permute the key in the following fashion. Let the 10-bit key be designated as (k1, K2, k3, k4, k5, k6, k7, k8, k9, k10). Then the permutation P10 is defined as: P10 (k1, K2, k3, k4, k5, k6, k7, k8, k9, k10) = (k3, k5, K2, k7, k4, k10 10, k1, k9, k8, k6).

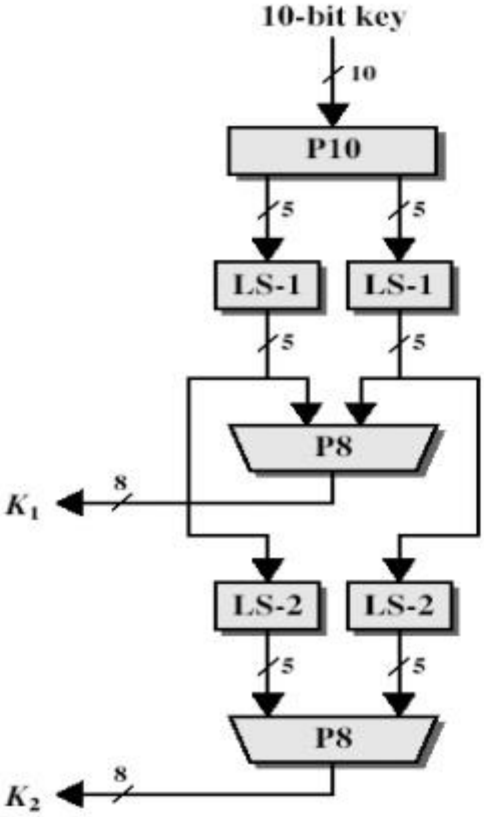
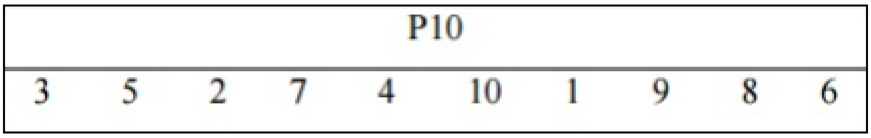


Figure: key generation for S-DES

P10 can be concisely defined by the display:



| P10 | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 3 | 5 | 2 | 7 | 4 | 10 | 1 | 9 | 8 | 6 |

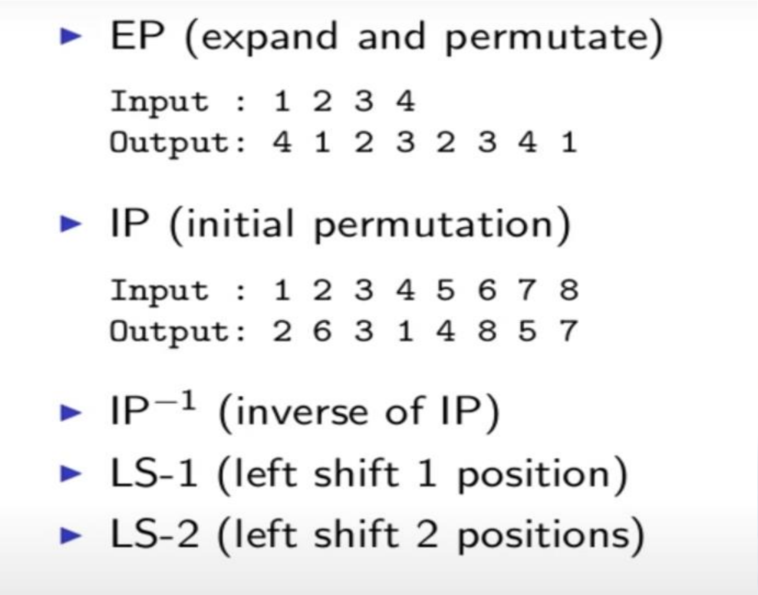
**The Function fk**

The most complex component of S-DES is the function fk, which consists of a combination of permutation and substitution functions.

The functions can be expressed as follows. Let L and R be the leftmost 4 bits and rightmost 4 bits of the 8-bit input to f K, and let F be a mapping (not necessarily one to one) from 4-bit strings to 4-bit strings. Then we let

Fk (L, R) = (L⊕ F (R, SK), R)

Where SK is a sub key and ⊕ is the bit-by- bit exclusive OR function



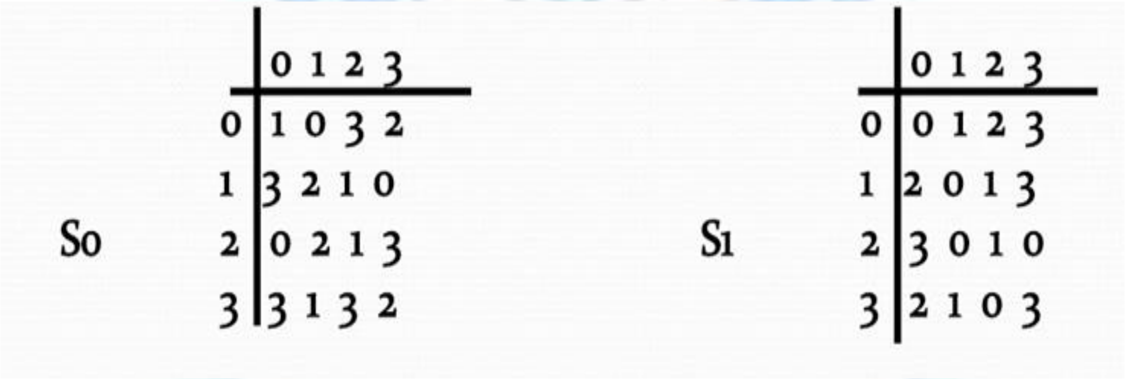
- EP (expand and permutate)

```
Input : 1 2 3 4
Output: 4 1 2 3 2 3 4 1
```

- IP (initial permutation)

```
Input : 1 2 3 4 5 6 7 8
Output: 2 6 3 1 4 8 5 7
```

- $IP^{-1}$ (inverse of IP)
- LS-1 (left shift 1 position)
- LS-2 (left shift 2 positions)



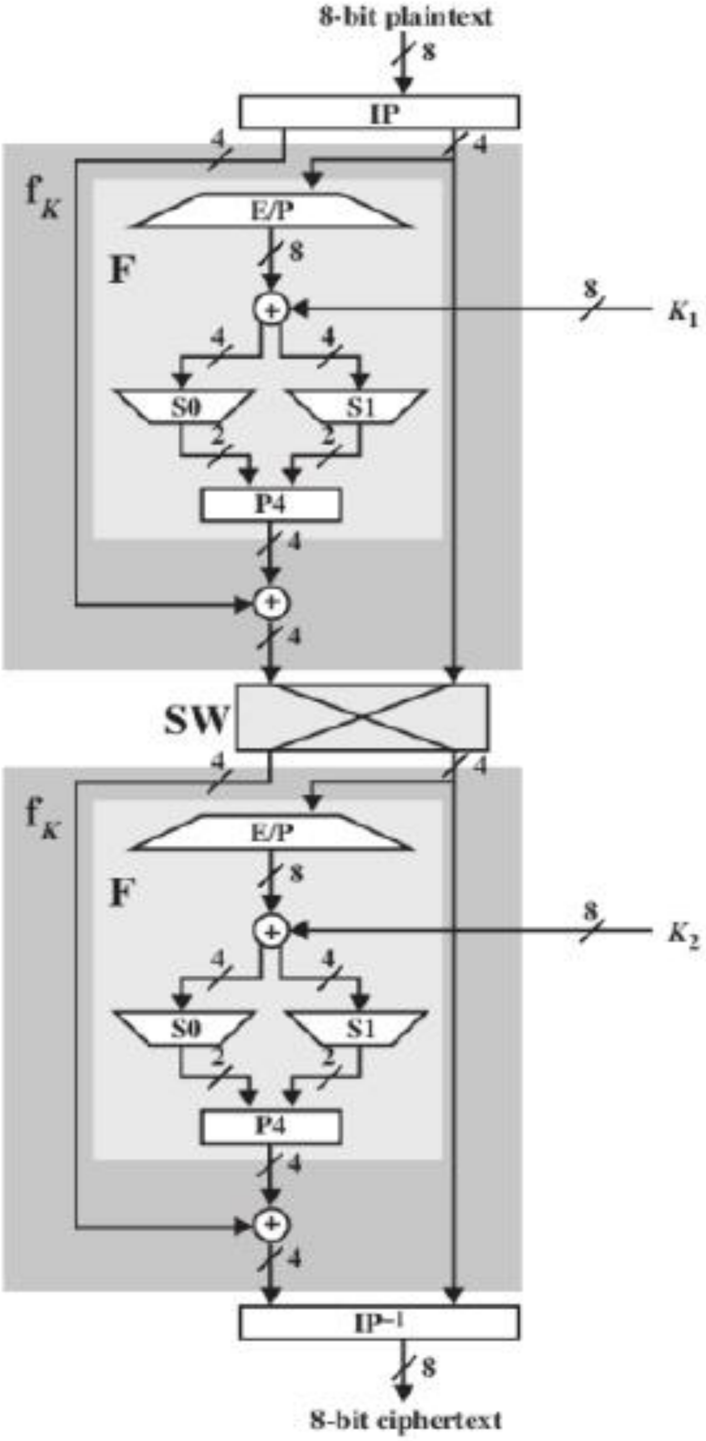
So

|   | 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 |

P4: 2 4 3 1


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