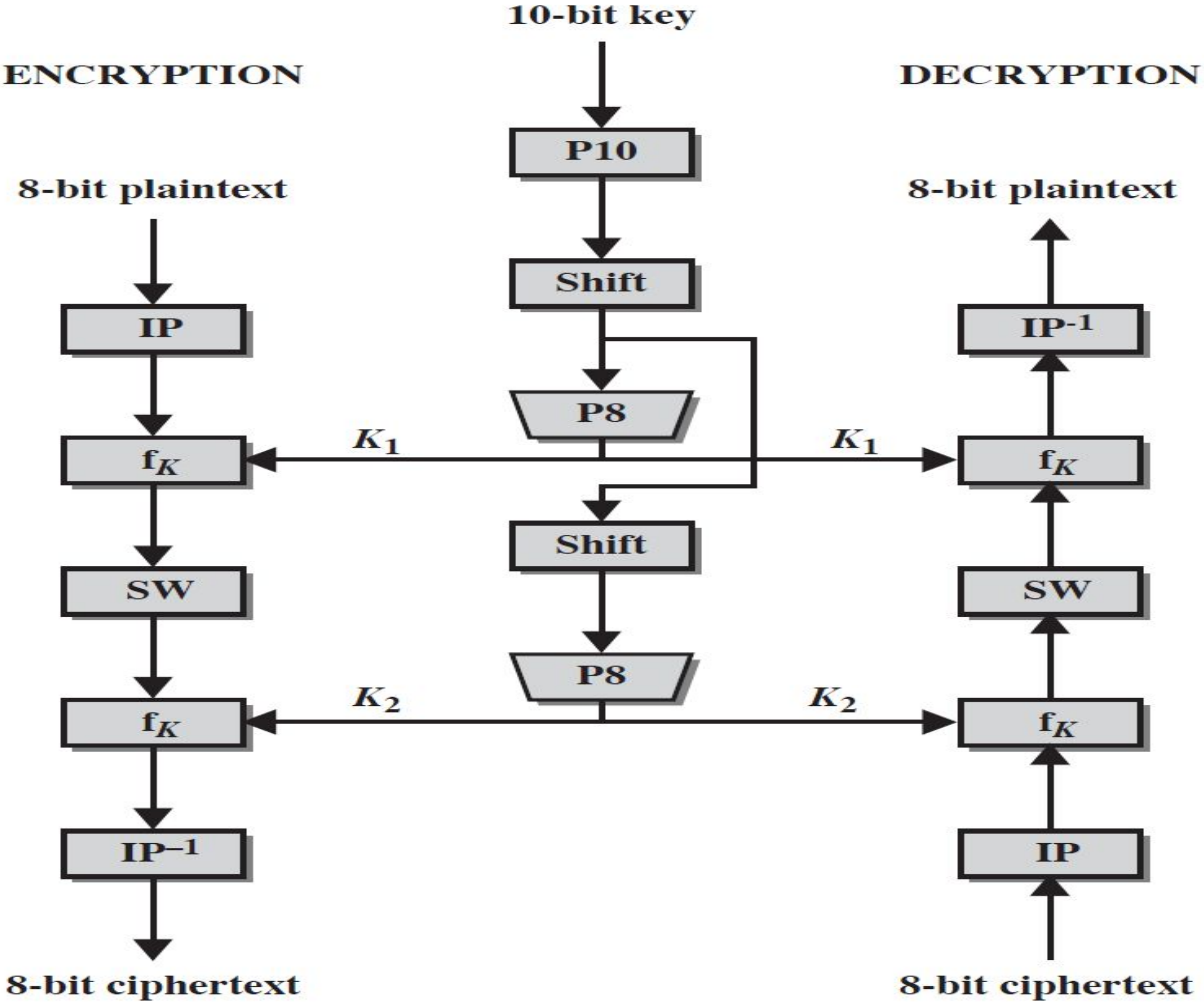
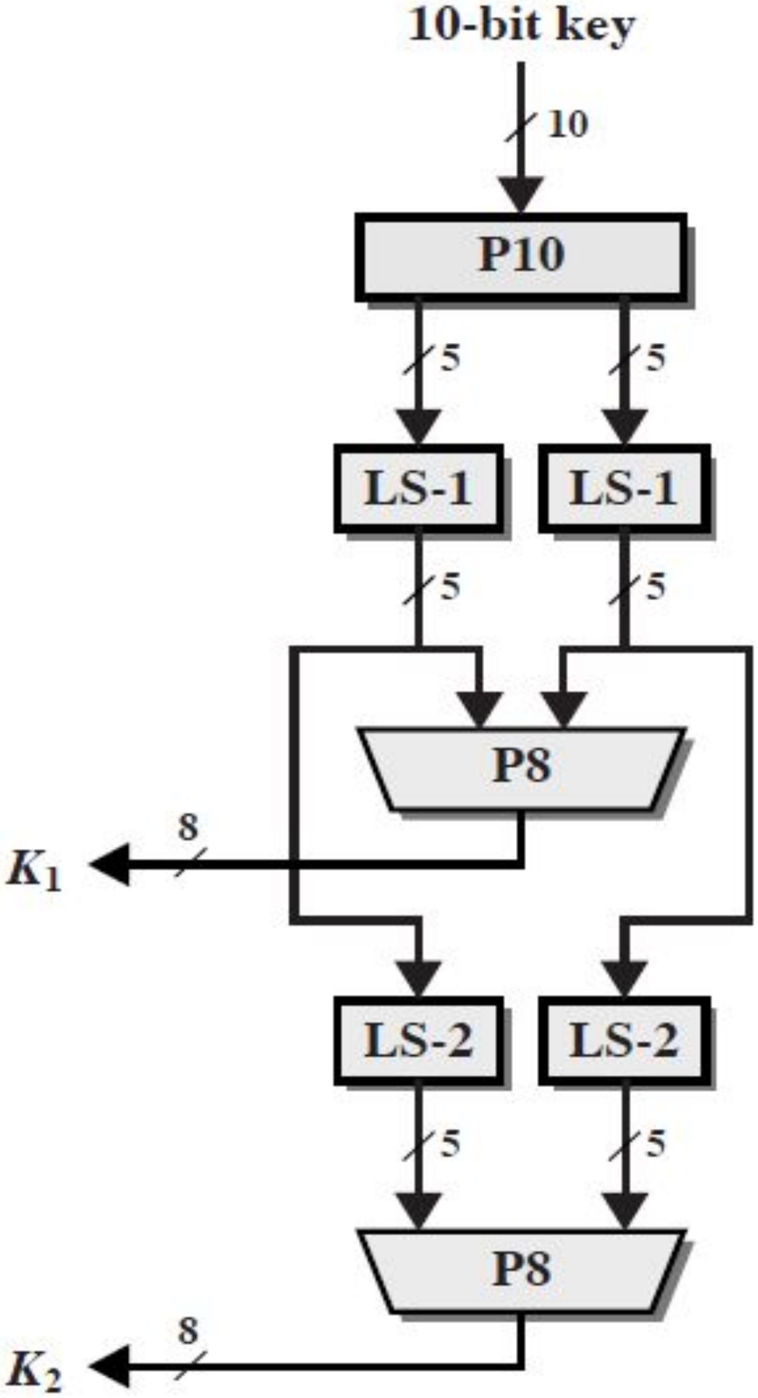
Simplified DES

Dr. S. R. Shinde


10-bit key
ENCRYPTION
DECRYPTION
P10
8-bit plaintext
8-bit plaintext
Shift
IP
IP-1
P8
K1
K1
fK
fK
Shift
SW
SW
P8
K2
K2
fK
fK
IP–1
IP
8-bit ciphertext
8-bit ciphertext

Key Generation



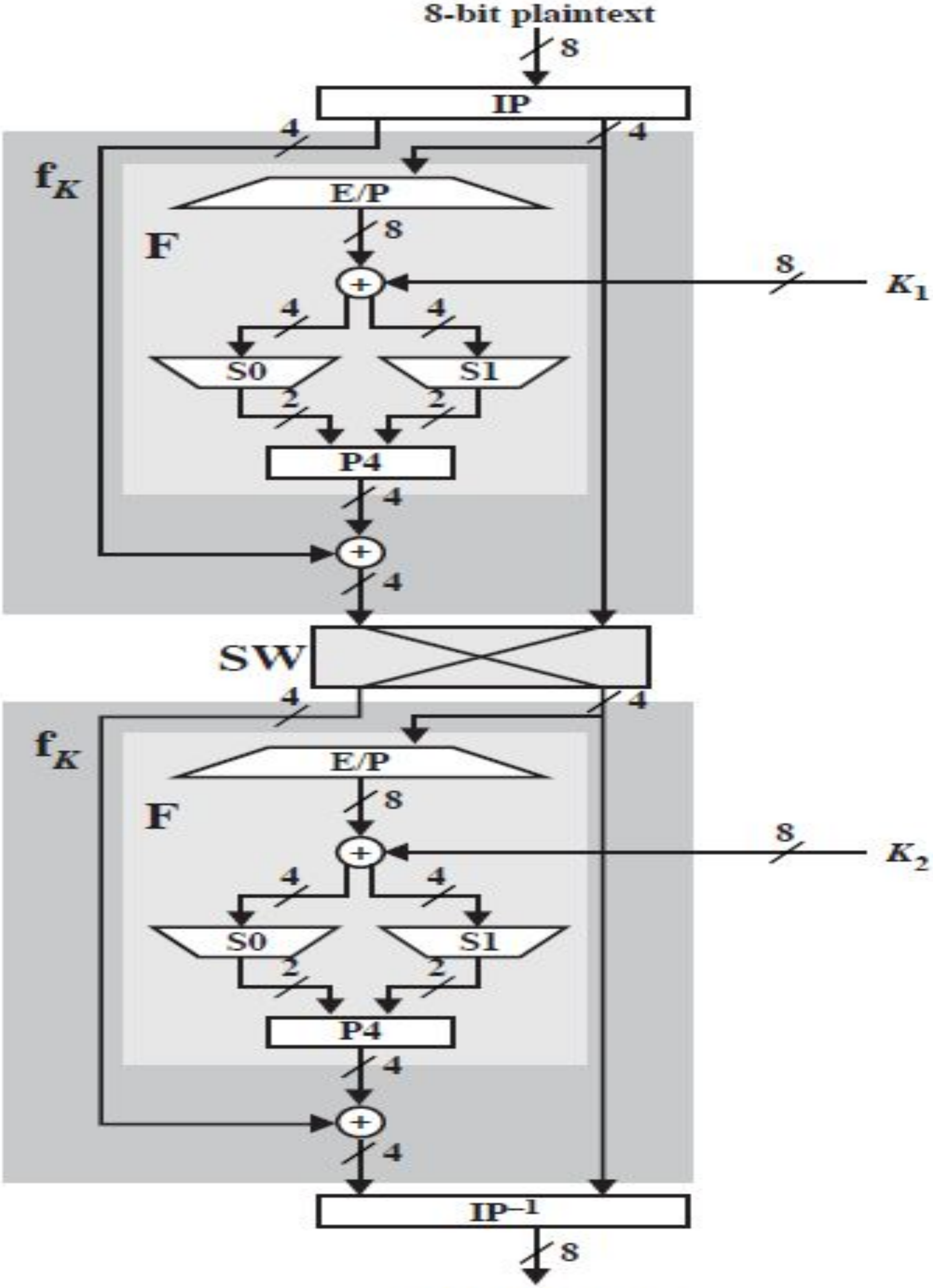
Key Generation

- Plain text = 8 bit data=10100101
- Key is=10 bit key=0010010111
- P10=3 5 2 7 4 10 1 9 8 6
- P8=6 3 7 4 8 5 10 9
- IP=2 6 3 1 4 8 5 7
- IP inverse= 4 1 3 5 7 2 8 6
- E/P=4 1 2 3 2 3 4 1
- P4= 2 4 3 1

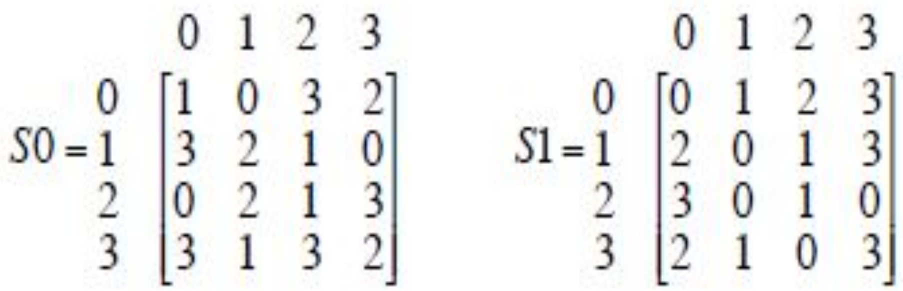
$$S0 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \end{array} \qquad S1 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix} \end{array}$$

- key=0 0 1 0 0 1 0 1 1 1
- 1 2 3 4 5 6 7 8 9 10
- P10=3 5 2 7 4 10 1 9 8 6
- Apply P10 K[P10[i]]= i=1, 2, 3, 4,5 ,6 ,7 ,8,9 ,10
- Key[]=1 0 0 0 0 1 0 1 1 1
- Apply LS-1
- Key[]= 0 0 0 0 1 0 1 1 1 1
- 1 2 3 4 5 6 7 8 9 10
- Apply P8=6 3 7 4 8 5 10 9
- Key[]= 0 0 1 0 1 1 1 1=key1

- Key[]= 0 0 0 0 1 0 1 1 1 1
- 1 2 3 4 5 6 7 8 9 10
- Apply LS-2
- Key[]= 0 0 1 0 0 1 1 1 0 1
- 1 2 3 4 5 6 7 8 9 10
- Apply P8=6 3 7 4 8 5 10 9
- Key[]= 1110 1010=key2


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

- P[]=data=1 0 1 0 0 1 0 1
- 1 2 3 4 5 6 7 8
- Key[]= 0 0 1 0 1 1 1 1=key1
- Key[]= 11101010=key2
- IP=2 6 3 1 4 8 5 7
- Apply IP P[IP[i]]= 0 1 1 1 0 1 0 0
- 1 2 3 4
- Apply EP E/P=4 1 2 3 2 3 4 1
- =0 0 1 0 1 0 0 0 Xor Key1
- =0 0 1 0 1 0 0 0 XOR 0 0 1 0 1 1 1 1
- =0 0 0 0 0 1 1 1



$$S0 = \begin{array}{c|cccc} & 0 & 1 & 2 & 3 \\ \hline 0 & 1 & 0 & 3 & 2 \\ 1 & 3 & 2 & 1 & 0 \\ 2 & 0 & 2 & 1 & 3 \\ 3 & 3 & 1 & 3 & 2 \end{array} \qquad S1 = \begin{array}{c|cccc} & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & 2 & 3 \\ 1 & 2 & 0 & 1 & 3 \\ 2 & 3 & 0 & 1 & 0 \\ 3 & 2 & 1 & 0 & 3 \end{array}$$

- =0 0 0 0 0 1 1 1
- S0 box, S1 box
- S-box substitution
- 1st and 4th bit forms Row , 2nd 3rd forms coln
- 00=0 , 00=0 01
- 01=1, 11=3 11
- S-box substitution gives= 0111
- Apply P4= 2 4 3 1
- = 1 1 1 0
- XOR 0 1 1 1
- =1 0 0 1 0 1 0 0
- Swap nibble
- = 0 1 0 0 1 0 0 1

- Swap nibble
- = 0 1 0 0 1 0 0 1
- 1 2 3 4
- Apply E/P =41232341
- 1 1 0 0 0 0 1 1
- XoR K2 1 1 1 0 1 0 1 0=key2
- 0 0 1 0 1 0 0 1
- Apply S-box substitution
- S0 box 00 Row and 01 coln = 00
- S1 box 11 Row and 00 coln = 10
- Substitution = 0 0 1 0
- 1 2 3 4
- Apply P4= 2 4 3 1
- = 0 0 1 0
- XoR 0 1 0 0
- 0 1 1 0 1 0 0 1
- 1 2 3 4 5 6 7 8
- Apply Inverse IP IP inverse= 4 1 3 5 7 2 8 6
- = 0 0 1 1 0 1 1 0
- Cipher Text