Akshay S. Chavan

S-DES Algorithm

Basic Functions:

- P10 (permute)

Input :	1	2	3	4	5	6	7	8	9	10
Output :	3	5	2	7	4	10	1	9	8	6

- P8 (Select and permutate)

Input:	1	2	3	4	5	6	7	8	9	10
Output:	6	3	7	4	8	5	10	9		

- P4 (permute)

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

- Initial permutation (IP):

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

- Expand and permute (EP):

Input :	1	2	3	4				
output:	4	1	2	3	2	3	4	1

- Inverse Initial permutation (IP^{-1}):
  - reverse of Ip.

- Left-Shift 1 (LS-1)
  - left shift by 1 position

- Left-shift 2 (LS-2)
  - left Shift by 2 positions

- S-Boxes:
  - 4-bit input : bit1, bit2, bit3, bit4
  - bit1, bit4 Specifies row.
  - bit2, bit3 Specifies Column.
  - 2 bit output.

$$S_0 = \begin{array}{c|cccc|} & 0 & 1 & 2 & 3 \\ \hline 0 & 01 & 00 & 11 & 10 \\ 1 & 11 & 10 & 01 & 00 \\ 2 & 00 & 10 & 01 & 11 \\ 3 & 11 & 01 & 11 & 10 \\ \hline \end{array} \qquad S_1 = \begin{array}{c|cccc} & 0 & 1 & 2 & 3 \\ \hline 0 & 00 & 01 & 10 & 11 \\ 1 & 10 & 00 & 01 & 11 \\ 2 & 11 & 00 & 01 & 00 \\ 3 & 10 & 01 & 00 & 11 \end{array}$$

* KEY-GENERATION PROCESS :

Input Key : 1010 000010
1 2 3 4 5 6 7 8 9 10

1) P10 : $\underbrace{1\ 0\ 0\ 0\ 0}_{\text{left half}} \mid \underbrace{0\ 1\ 1\ 0\ 0}_{\text{right half}}$

2) LS-1 on both left half & right half :
O/P : 00001 | 11000

3) P8 : Input: 00001 11000 (1 2 3 4 5 6 7 8 9 10)
Output: 10100100 ⇐ key-1

FOR GENERATION OF KEY-2 :

4) LS-2 on output of step ②

Input : 00001 | 11000

Output: 00100 | 00011

5) P.8 : Input: 00100 00011
Output: 01000011 ⇐ key-2

• **EXAMPLE :**

plain-text : 0 1 1 1 0 0 1 0
key : 1 0 1 0 0 0 0 0 1 0

ENCRYPTION : $\overset{1}{0}\ \overset{2}{1}\ \overset{3}{1}\ \overset{4}{1}\ \overset{5}{0}\ \overset{6}{0}\ \overset{7}{1}\ \overset{8}{0}$

ROUND-1

1) IP :

$\underbrace{1\ 0\ 1\ 0}_{\text{Left-Half}}\quad \underbrace{1\ 0\ 0\ 1}_{\text{Right-Half}}$

⇓

2) $\overset{1}{1}\ \overset{2}{0}\ \overset{3}{0}\ \overset{4}{1}$

Ep: 1 1 0 0 0 0 1 1

3) EXOR Expanded Right-Half with key-1

1 1 0 0 0 0 1 1 ← Expanded R.H.
EXOR 1 0 1 0 0 1 0 0 ← key1
0 1 1 0 0 1 1 1

4) $\underbrace{0\ 1\ 1\ 0}_{\Downarrow\ S_0}\quad \underbrace{0\ 1\ 1\ 1}_{\Downarrow\ S_1}$

0 1 1 0 row = 00 col = 11

0 1 1 0 row = 00 col = 11

Refer S-Box Matrix

$$\begin{array}{lcc} & S_0 & S_1 \\ \text{Output:} & 10 & 11 \end{array}$$

⇓

5) P4: $\overset{1}{1}\ \overset{}{\underset{2}{0}}\ \underset{3}{1}\ \underset{4}{1}$

Output: 0111

6) EXOR Step ⑤ output with left-half of Step ①

$$\begin{array}{lcccc l} & 0 & 1 & 1 & 1 & \Leftarrow \text{Step ⑤ O/p} \\ \text{EXOR} & 1 & 0 & 1 & 0 & \Leftarrow \text{left-half from Step ①} \\ \hline & 1 & 1 & 0 & 1 & \end{array}$$

7) Merge right half from Step ① to output of Step ⑥

1101 $\underbrace{1001}$ ← Right-Half from Step ①

8) Swap

1001 1101 ⇐ Round 1 output

ROUND-2

Input: $\underbrace{1001}_{\text{left}}$ $\underbrace{1101}_{\text{right}}$

1) Ep:

1 1 0 1
1 2 3 4

Output: 1110 1011

2) EXOR with Key 2

EXOR

$$\begin{array}{l} 1\,1\,1\,0\,1\,0\,1\,1 \\ 0\,1\,0\,0\,0\,0\,1\,1 \quad \leftarrow \text{Key-2} \\ \hline 1\,0\,1\,0\,1\,0\,0\,0 \end{array}$$

3)

$$\underbrace{1\,0\,1\,0}_{\downarrow\downarrow} \qquad \underbrace{1\,0\,0\,0}_{\downarrow\downarrow}$$

S0 S1
↓ ↓
row=10 10 11 row=10
Col = 01 Col = 00

Output: 1011

4) P4:

1 0 1 1
1 2 3 4

Output: 0 1 1 1

5) EXOR with left-half from ~~Key~~ Step-1 (before Ep)

$$\begin{array}{l} 0\,1\,1\,1 \\ 1\,0\,0\,1 \quad \leftarrow \text{left half of Step ①} \\ \hline 1\,1\,1\,0 \end{array}$$

6) Merge with right-half from step ①

1110 1101

* Output of round-2 : 1110 1101

- After performing all rounds perform Ip^{-1}

Input: $\overset{1}{1}\ \overset{2}{1}\ \overset{3}{1}\ \overset{4}{0}\ \ \overset{5}{1}\ \overset{6}{1}\ \overset{7}{0}\ \overset{8}{1}$

Output: 0111 0111

Thus, Ciphertext we get is 01110111

* <u>DECRYPTION</u> :

- perform Same steps as encryption but use keys in Reverse order as they are used for encryption (ie. key2 then key1 ...)

<u>ROUND-1</u>

1) Ciphertext Input: $\underset{1}{0}\,\underset{2}{1}\,\underset{3}{1}\,\underset{4}{1}\,\underset{5}{0}\,\underset{6}{1}\,\underset{7}{1}\,\underset{8}{1}$

Ip: $\underbrace{1110}_{\text{left half}}\quad\underbrace{1101}_{\text{right half}}$ $\downarrow$

2) Ep:

Input: $\overset{1}{1}\,\overset{2}{1}\,\overset{3}{0}\,\overset{4}{1}$

Output: 11101011

3) EXOR with key-2

11101011

01000011 ← key2

10101000

$\underbrace{1010}_{S_0}\ \underbrace{1000}_{S_1}$

4)

row= 10 ↓ S0 ↓ S1 row= 10

col= 01 10 11 col= 00

Output: 1011

5) P4: Input: 1 0 1 1 (1 2 3 4)

Output: 0 1 1 1

6) EXOR with left-half of step ①

0111

1110

1001

7) Merge with right-half from step ①

1001 1101

8) Swap:

1101 1001

ROUND - 2

Input: $\underbrace{1101}_{\text{left half}}$ $\underbrace{1001}_{\text{right half}}$

1) Ep:

Input: $\overset{1}{1}\,\overset{2}{0}\,\overset{3}{0}\,\overset{4}{1}$

Output: 1100 0011

2) EXOR with key-1

$$\begin{array}{rl} & 1100\ 0011 \\ \text{EXOR} & 1010.0100 \\ \hline & \underbrace{0110}\ \underbrace{0111} \end{array}$$

3)

	$\Downarrow$	$\Downarrow$	
	S_0	S_1	
row = 00	↓	↓	row = 01
col = 11	10	11	col = 11

4) P4: Input: $\overset{1}{1}\,\overset{2}{0}\,\overset{3}{1}\,\overset{4}{1}$

Output: 0111

5) EXOR with left-half

$$\begin{array}{rl} & 0111 \\ \text{EXOR} & 1101 \\ \hline & 1010 \end{array}$$

6) Merge with right half

1010 1001

Output of Round-2 : 10101001

Finally perform IP^{-1} on output of Round-2

- IP^{-1} :

	1	2	3	4	5	6	7	8
Input:	1	0	1	0	1	0	0	1
Output:	0	1	1	1	0	0	1	0

∴ Decrypted text : 01110010