S-DES

PART-1

S-DES ALGORITHM

1) S-DES stands for Simplified Data Encryption Standard
2) S-DES is symmetric cipher
3) The size of plain text is 8 bits
4) The size of key is initially 10 bits
5) It's a 2-round process

Functions or tables:

P-10

I/P	1	2	3	4	5	6	7	8	9	10
O/P	3	5	2	7	4	10	1	9	8	6

P-8

I/P	1	2	3	4	5	6	7	8	9	10
O/P	6	3	7	4	8	5	10	9		

IP-8

I/P	1	2	3	4	5	6	7	8
O/P	2	6	3	1	4	8	5	7

EP

I/P	1	2	3	4				
O/P	4	1	2	3	2	3	4	1

XOR Truth Table

A	B	A XOR B
1	1	0
1	0	1
0	1	1
0	0	0

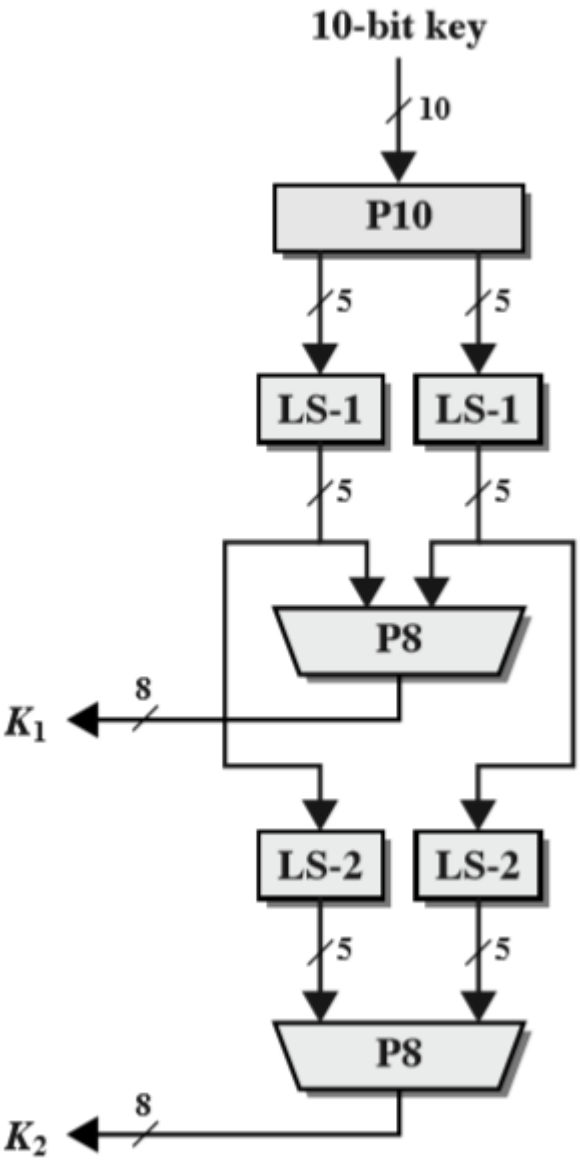
P-4

I/P	1	2	3	4
O/P	2	4	3	1

IP^{-1}

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

Key-Generation:



Step 1:

Just select a random key of 10-bits, which only should be shared between both parties which means sender and receiver.
As I selected below!

Select key:1010000010

Step 2:

Put this key into P.10 Table and permute the bits.

P-10 table

I/P	1	2	3	4	5	6	7	8	9	10
O/P	3	5	2	7	4	10	1	9	8	6

As I put key into P.10 Table

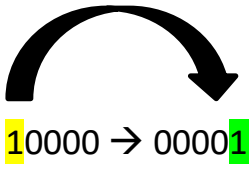
	1	2	3	4	5	6	7	8	9	10
I/P	1	0	1	0	0	0	0	0	1	0
O/P	1	0	0	0	0	0	0	1	1	0

Step 3:

Divide the key into two halves, left half and right half;
{1 0 0 0 0} | {0 1 1 0 0}

Step 4:

Now apply the one-bit left shift on each half:
Before left shift: {10000} | {01100}
After left shift: {00001} | {11000}
The output will be:
{0 0 0 0 1} {1 1 0 0 0}



Step 5:

Now once again combine both halve of the bits, right and left. Put them into the P8 table. What you get, that will be the K1 or First key.
Combine: 0 0 0 0 1 1 1 0 0 0

P-8 Table

I/P	1	2	3	4	5	6	7	8	9	10
O/P	6	3	7	4	8	5	10	9		

As I put key into P.8 Table

	1	2	3	4	5	6	7	8	9	10
I/P	0	0	0	0	1	1	1	0	0	0
O/P	1	0	1	0	0	1	0	0		

K1=1 0 1 0 0 1 0 0

Step6:

As we know S-DES has two round and for that **we also need two keys**, one key we generate in the above steps (step 1 to step 5). Now we need to **generate a second** bit and after that we will move to encrypt the plain text or message.

It is simple to generate the second key. Simply, go in **step 4** copy both halves, each one consists of 5 bits. But be careful on the taking of bits. Select those halves which are output of first round shift, don't take the bits which are not used in the first round. In simple words, take the output of first round shift in above **step 4.**

Which are: {00001} | {11000}

Step 7:

Now just apply two left shift circulate on each half of the bits, which means to change the position of two bits of each halves.
left half: 00001
Right half: 11000

00001 → 00100

After the two rounds of left shift on each half out-put of each half will be.

Left half: 00100
Right half: 00011
Combine both together: As: 0 0 1 0 0 – 0 0 0 1 1

Step 8:
Now put the bits into P-8 Table, what you get, that will be your second key. Table is also given in **step 5**.

But here the combinations of bits are changed because of two left round shift from step 5. Check it in depth.
Combine bits: 0 0 1 0 0 0 0 0 1 1

P-8 :

I/P	1	2	3	4	5	6	7	8	9	10
O/P	6	3	7	4	8	5	10	9		

	1	2	3	4	5	6	7	8	9	10
I/P	0	0	1	0	0	0	0	0	1	1
O/P	0	1	0	0	0	0	1	1		

K2= 01000011

Finally, we created both key

Key-1 = 1 0 1 0 0 1 0 0

Key-2 = 0 1 0 0 0 0 1 1

THANK YOU