SIMPLIFIED DATA ENCRYPTION STANDARD

S-DES is a simplified version of DES, developed for beginners to learn the basic concept of DES. It was developed in 1996 by Prof. Edward Schaefer at Santa Clara University. The S-DES has all significantly reduced parameters of DES with safeguarding the structure of DES. It is only for educational purposes and not suitable for practical purposes due to security issues.

It is a block cipher that takes 8 bits plaintext block and converts it to 8 bits block of ciphertext with the help of encryption key of size 10 bits. Decryption uses the same key to produce 8 bits of original plaintext from 8 bits of ciphertext. The S-DES scheme is shown in Figure 1. Let us first discuss how to generate the 10 bits of the encryption key, before going in the depth of encryption and decryption process in S-DES.

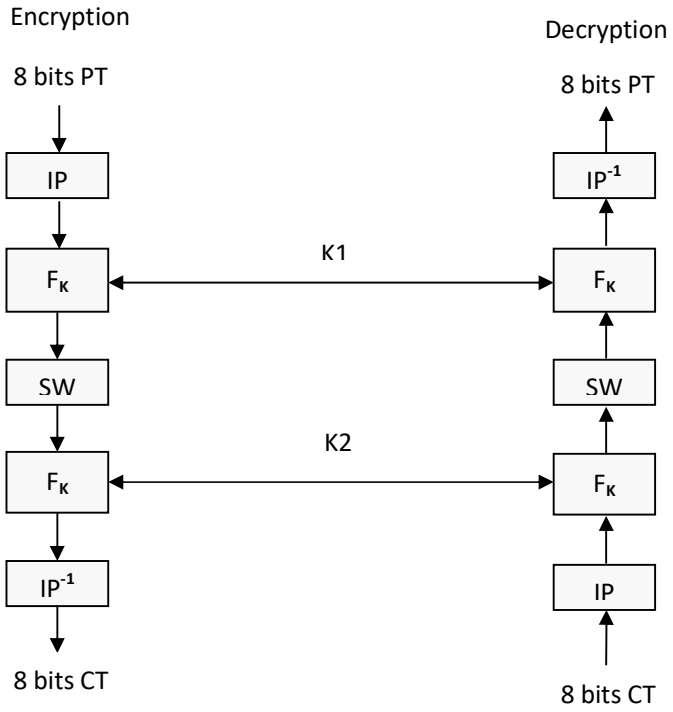

Figure S-DES Scheme

KEY GENERATION PROCESS

There are two rounds in S-DES and for each round one key is used. So two keys K1 and K2 are generated which are used in encryption and decryption as well. Only in decryption the order of keys is reversed. Key generation process is depicted in Figure and discussed below with the help of an example.

Step 1:

Any random 10 bits number is selected. This is a random key which should be shared only between sender and receiver.

e.g. Selected key : 1010101010

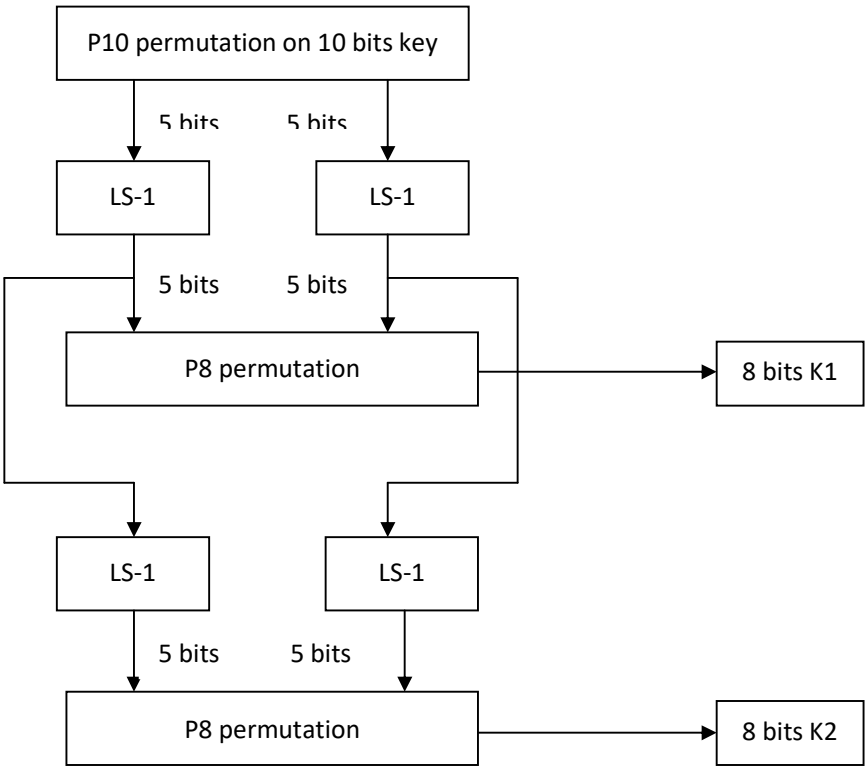

Figure Key generation process

Step 2:

This selected key undergoes the P10 permutation. P10 permutation is shown in Figure. Output of the selected key after permutation (P10) is {1101001100}.

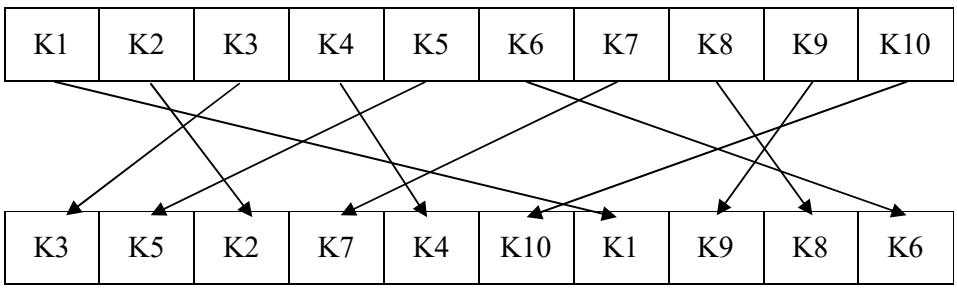

Figure P10 permutation

Step 3:

The permutated key is divided into two halves, left half and right half.

Left half : (11010) and Right half : (01100)

Step 4:

Left circular shift by 1 bit on each half is performed.

After left circular shift by 1 bit sesperately on each half , output is : {(10101) (11000)}

Step 5:

Both the halves, left half and right half are merged together and passes through P8 permutation (Figure). The output of this step is the generated first key i.e. K1.

Generated Key K1: **{11100100}**

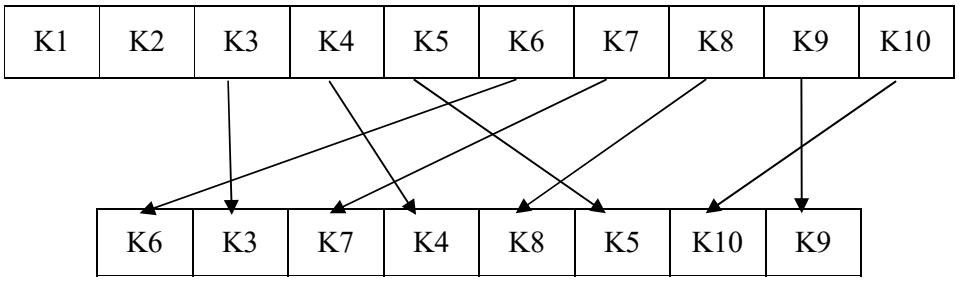

Figure P8 permutation

Step 6:

The key generation algorithm proceeds futher to generate second key i.e. K2. The output of step 4, two halves (5 bits each) are considered for the next step.

Left half : (11010) and Right half : (01100)

Step 7:

Bits in each half undergo circular left shift by 2 bits, separately.

After circular left shift by 2 bits we get: {(01011) (10001)}

Step 8:

The output of each half is combined together and P8 permutation is carried out on them. This generates second key i.e. K2 which is of 8 bits.

The generated key K2 : **(10010110)**.

ENCRYPTION

Encryption process of simplified DES is divided into following five functions.

1. IP-Initial permutation
2. F_k - 2 input function
3. SW-Swapping of 2 nibles

4. F_k – 2 input function
5. IP^{-1}- Inverse permutation

The encryption process is shown in Figure 2 and elaborated in detail with an example as follows.

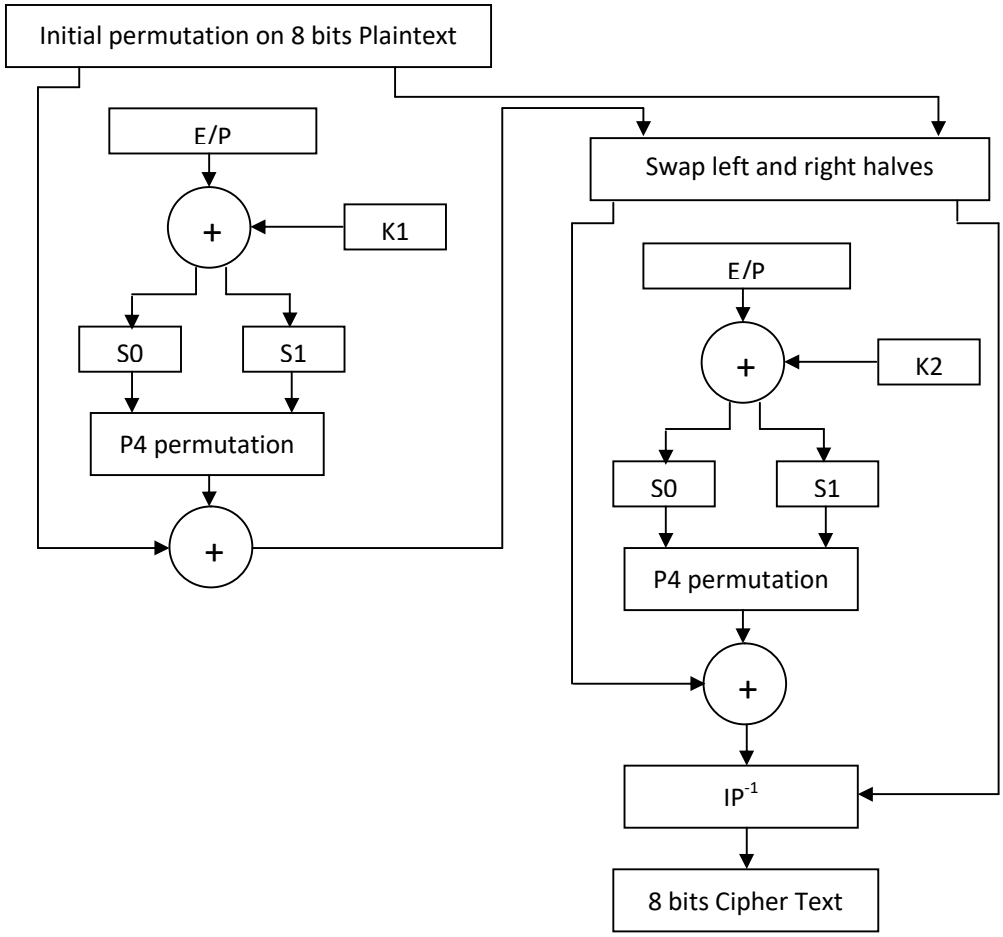

Figure S-DES encryption process

Step 1: Block size of plaintext is of 8 bits in S-DES.

Consider Plaintext as **11110000.**

Step 2: Initial permutation is applied on the block of 8 bits plaintext using Figure 2.

- 10111000

Divide the permuted bits into 2 halves, each of 4 bits which gives left half (1011) and right half (1000).

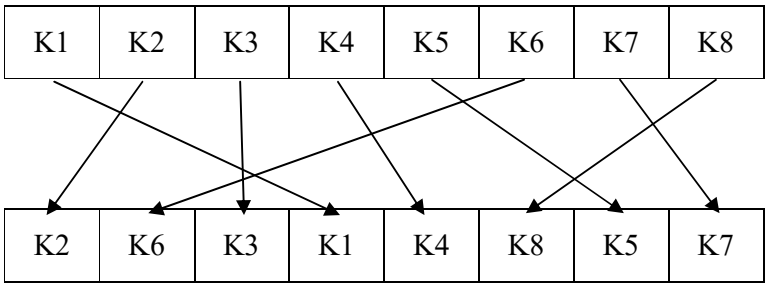

Figure Initial permutation

Step 3:The right half is permuted using Expansion/Permutaton (E/P) as given in Figure 3 which gives 8 bits as output.

- 01000001

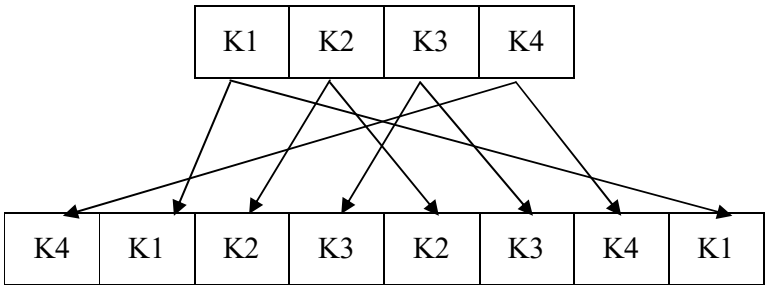

Figure Expansion/Permutation

Step 4: These 8 bits are XORed with the first key (K1).

- 10100101

Step 5: The XORed output is again divided into two halves , left half and right half.

Step 6: Next we apply S-box substitution. There are 2 S-boxes, S0 and S1. The S-box takes input as 4 bits and produces output as 2 bits. The S0 and S1 S-boxes are given in Table 1. Select first and last bit (underlined digits) of the input group and take decimal equivalent number of it . This will be the row number of S-box. Then pck up middle (2) bits (Italic digits) , convert it to its decimal equivalent number, which will produce the column number. Take intersection of this row and column numbers that will give the ouput of S-box. For left half use S0 and for right half use S1 and take binary equivalent of the decimal number of S-box.

Input group	Row no.	Column no.	S-Box substitution
1*01*0	2	1	2
0*10*1	1	2	1

Table S-Box Structure

S0

R/C	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

R/C	0	1	2	3
0	0	1	2	3
1	2	0	1	3
2	3	0	1	0
3	2	1	0	3

Step 7: The output of both S-boxes are combined together which forms 4 bits number will be given to the P4 permutation. P4 permutation is described in Figure 4.

- 0101

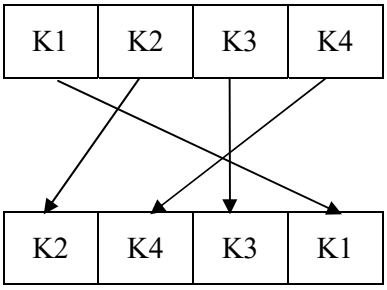

Figure P4 Permutation

Step 8: Output of step 7 is XORed with Left half of the initial permuation step.

- 1110

Step 9: This will be applied to SW as left of the input. The right half of input to SW is the right half (4 bits) of initial permutation step.

- { 11101000}

Step 10: SW operation swaps thease two halves. Consider swapped halves as left half and right half and repeat the same procedure from step 3 to step 9 with key K2 instead of K1. Then feed this output into IP^{-1} table as left half which will be combined with the right half of the initial permutation. Inverse permutation is given in Figure 5. Output of this will be the generated chipher text of the plaintext.

- Cipher text: **10011101**

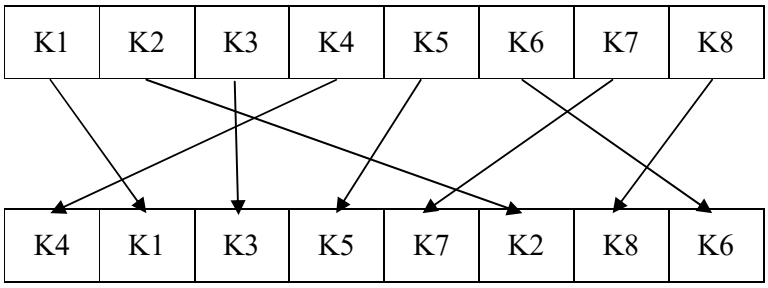

Figure 5 Inverse initial permutation

DECRYPTION

Decryption process S-DES is similar to encryption process with only difference in using the keys. Keys are used in reverse order. After decryption original message will be generated.