**Simplified DES(S-DES)**

**Simplified Data Encryption Standard (S-DES) is a simple version of the DES Algorithm. similar to the DES algorithm but is a smaller algorithm and has fewer parameters than DES. It was made for educational purposes so that understanding DES would become simpler.  It is a block cipher that takes a block of plain text and converts it into ciphertext.  It takes a block of 8 bit.**

**It is a symmetric key cipher i.e. they use the same key for both encryption and decryption.**

**Demonstration of Key Generation for S-DES encryption and decryption algorithm shown below.**

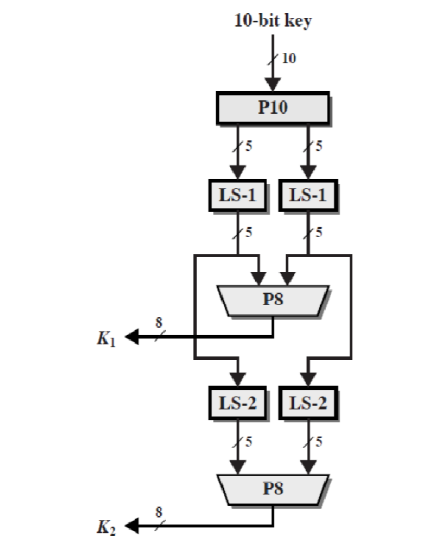
**We take a random 10-bit key and produce two 8-bit keys which will be used for encryption and decryption.**

**Key Generation Concept:**

**In the key generation algorithm, we accept the 10-bit key and convert it into two 8-bit keys. This key is shared between both sender and receiver.**

**As shown in the below figure, random 10 bit key is used then permutation-p(10)—( Which is nothing but how the 10 bits are rearranged into 10 bits by using p(10)) is used. Then it is divided into 5bits each and then left shifted. After left shifting p(8)—( Which is nothing but how the 10 bits are rearranged into 8 bits by using p(8)) is applied.**

**Then k1 and k2 are determined.**



**Fig 1: S-DES Key Generation**

Generate two 8-bit subkeys from the original 10-bit key

• The key is first subjected to a permutation (P10).

• Divide the output of P10 in to two halves and perform circular left shift one bit position (LS-1) on the two halves and then passes through a permutation function (P8) that produces an 8-bit output for the first subkey(K1).

• The output of the shift operation is given as input into another shift(LS2) (left shift by 2 bits on the two halves of the data) and another instance of (P8) to produce the second subkey(K2)

K1=P8(Shift(P10(key)))

K2=P8(Shift(Shift(P10(key)

