**NIRMA UNIVERSITY**

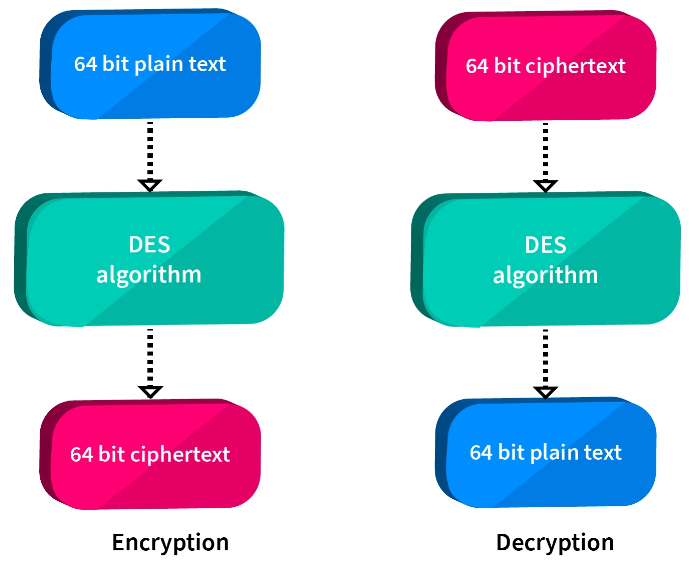
**Institute of Technology**

**B.Tech. Computer Science and Engineering**

**2CSDE54 Information and Network Security**

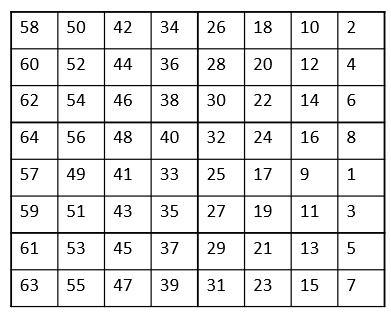
**Perform encryption and decryption using Data Encryption Standard**

The Data Encryption Standard algorithm is a block cipher algorithm that takes in 64-bit blocks of plaintext at a time as input and produces 64-bit blocks of cipher text at a time, using a 48-bit key for each input. In block cipher algorithms, the text to be encrypted is broken into ‘blocks’ of text, and each block is encrypted separately using the key.

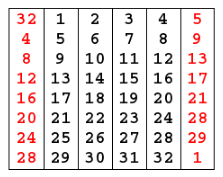


**Steps to perform Two rounds of DES**

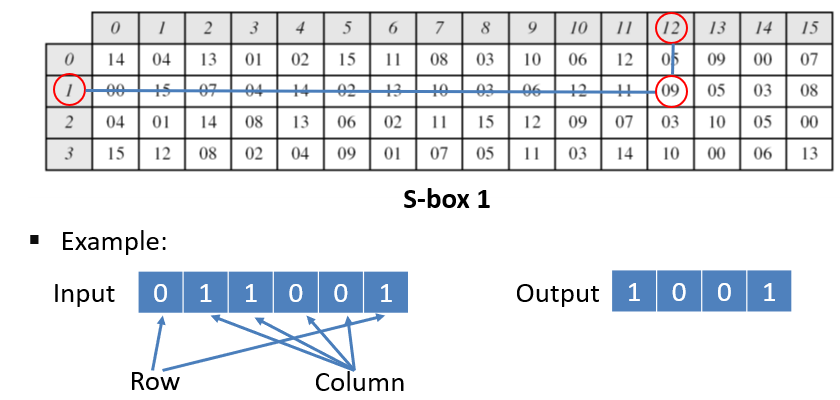
1. Take the 6 characters at a time from the file for encryption i.e. [8bitX6=64 bit block size]
2. Call a function that converts each character to ASCII and returns the binary of that character
3. Now we have 64 bit, call initial permutation function that changes the position of the bits.



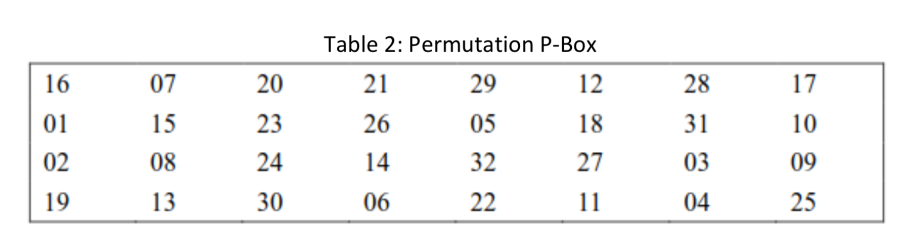
1. Take 56 bit key and create two round key K1 and K2 by left shifting both Left half and Right half[consider only first 48 bit from 56 bit for round key]
2. Expansion Permutation (E-table), Right half is expanded from 32-bits to 48-bits



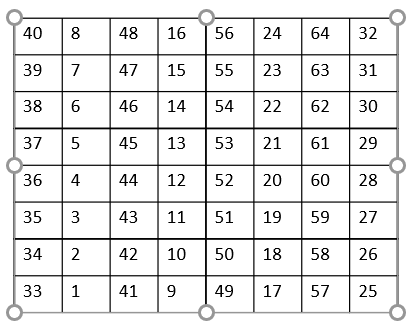
1. S-box Substitution: Accepts 48-bits from XOR operation and produces 32-bits using 8 substitution boxes (each S-box has a 6-bit i/p and 4-bit o/p).



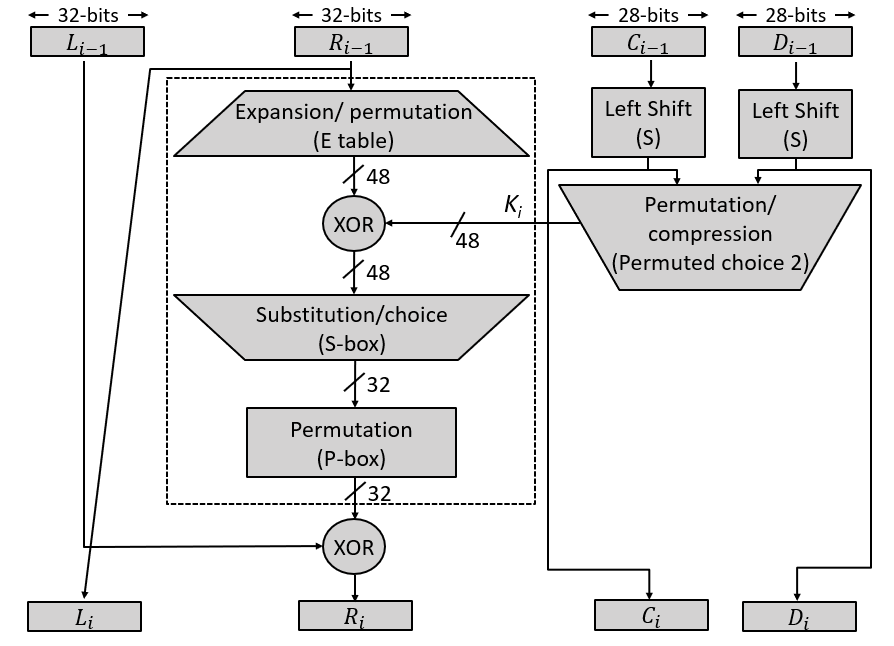
1. P-Box Permutation: rearrange the 32 bits in this fashion and read it again



1. XOR and Swap: Apply XOR Left portion and output of P-Box will be used as right portion for next round
2. Apply inverse initial permutation:



**Single round DES**



**DES Algorithm**

