UDYAM’24

✻Digism Problem Statement✻

Team : Karanam Srimayi (22095051) ,
Samruddhi Deshmukh (22095099)

Problem Statement :

Encryption and Decryption of a 8-bit binary value using des algorithm implementation in digital logics and circuit .

DES Algorithm (Combinational Solution) :

1) Data Encryption Standard (DES) is a block cipher with a 56-bit key length that has played a significant role in data security. Here in our PS , we have to deal with just 8-bit binary input .

2) There are a total of 4 Rounds in the encryption algorithm .The initial input is permuted accordingly as given . At each round several operations are performed . And each round has its own round key .

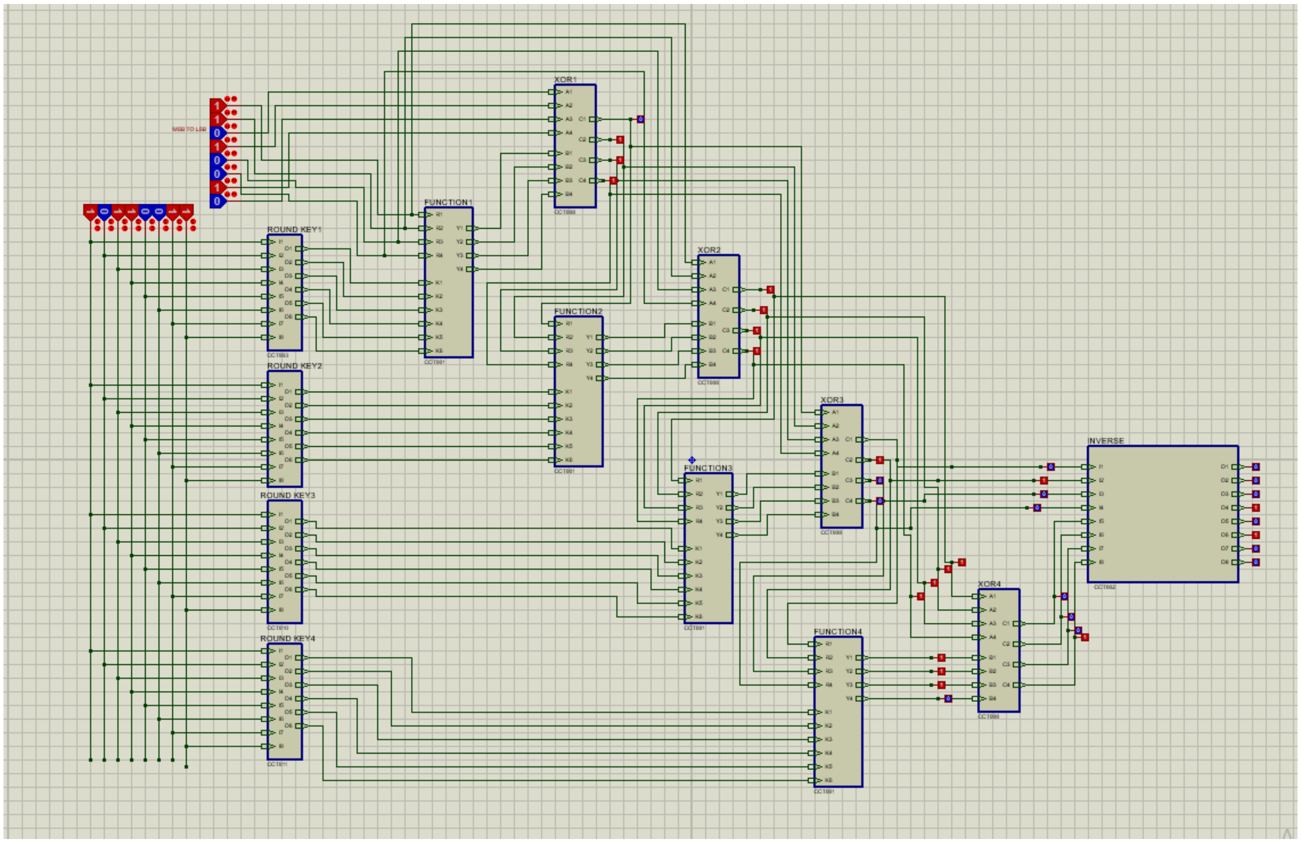
3) The initial key is provided at the input . At each round , the key is circular left shifted by 1 or 2 bits and then merged and compressed for further operations .

4) There is also a special function ‘f’ which carries out many operations like expansion , XOR , S-box substitution and permutation .

5) The output of XOR of function output and 4 left bits of the current round is carried onto the next round as right 4 bits . While the current right bits move to the next left 4 bits .

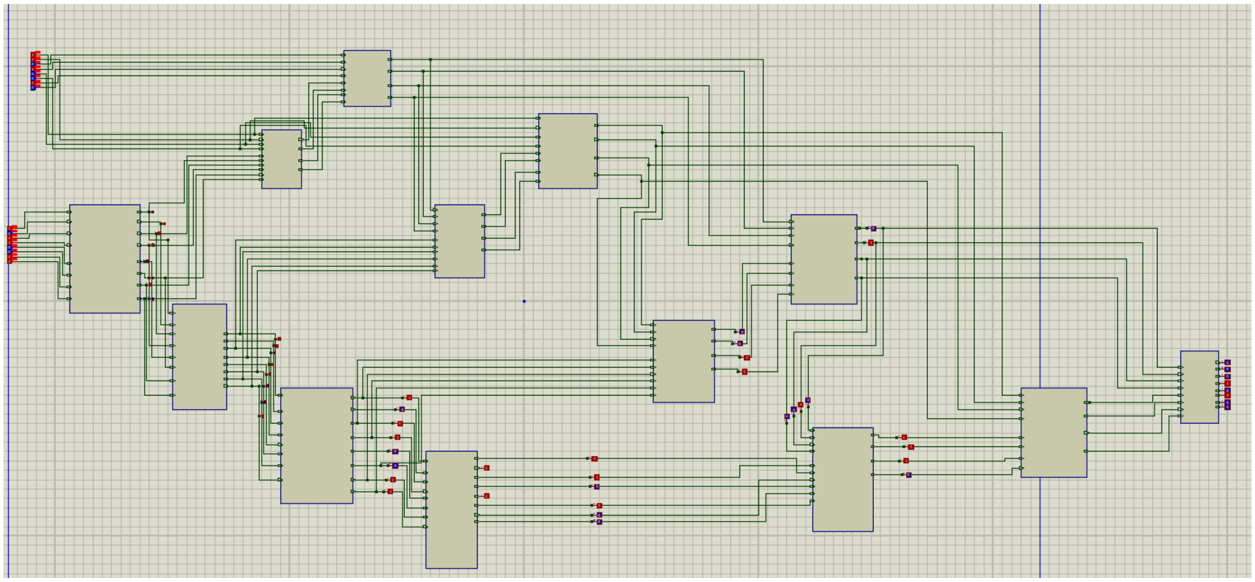
6) After the completion of 4 rounds , the output is inverse permuted to get our encrypted text or cipher text .

Encryption implementation on Proteus (Only Combinational Solution) :



DES Algorithm (Sequential + Combinational Solution) :

For the Sequential solution we have used a circular shifting register in each round key by which , every time we don’t need to shift the bits manually and the circuit itself stores the bits and shifts it for the next round .
All the clocks used in the registers are according to our given needs of one bit or two bit shifting .
Rest all the circuit is same as the combinational one .



Circuit implementation on Proteus

Sequential Logic :

The sequential logic is found in the round key . As there are 4 round keys , and each time there is a left circular shifting in the bits . For this purpose , we have used bidirectional shift registers with parallel input and parallel output .