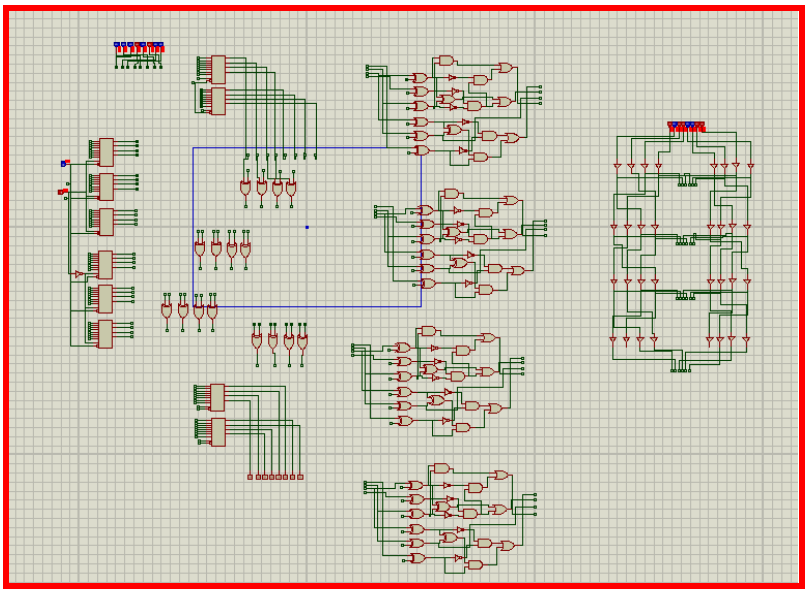
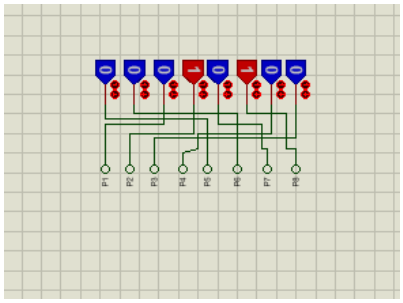
DIGISIM-PS-1

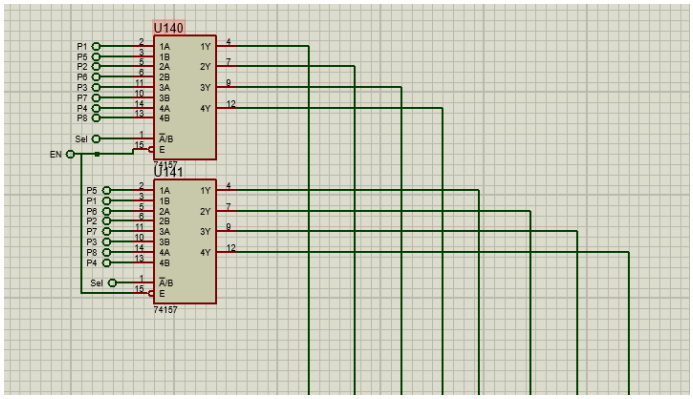
Combinational Approach



Input

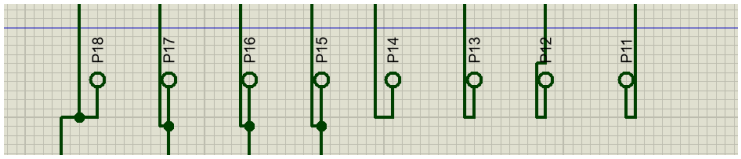


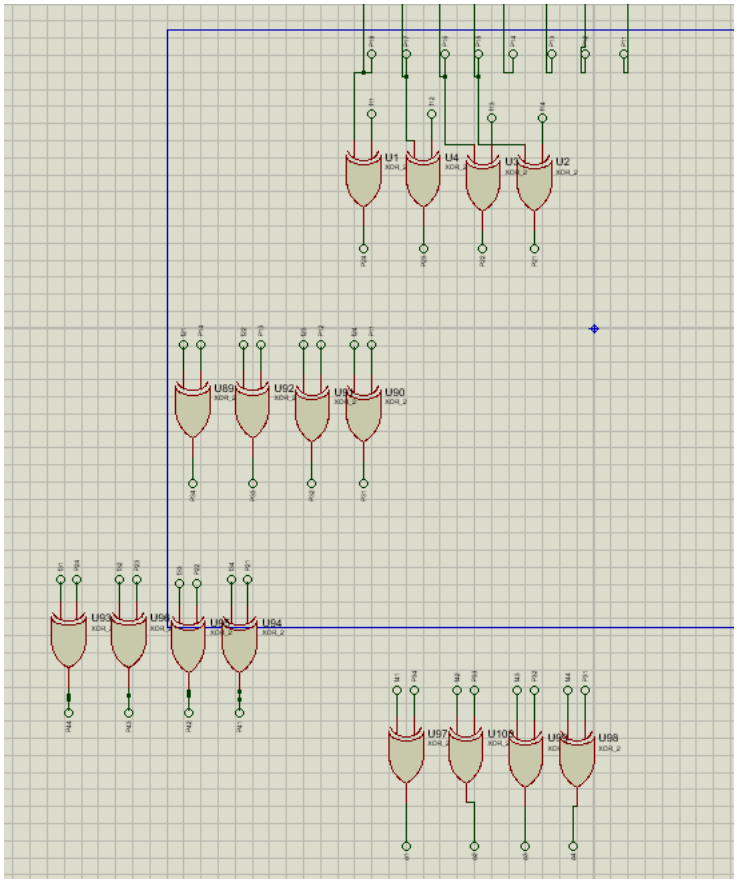
Permutation



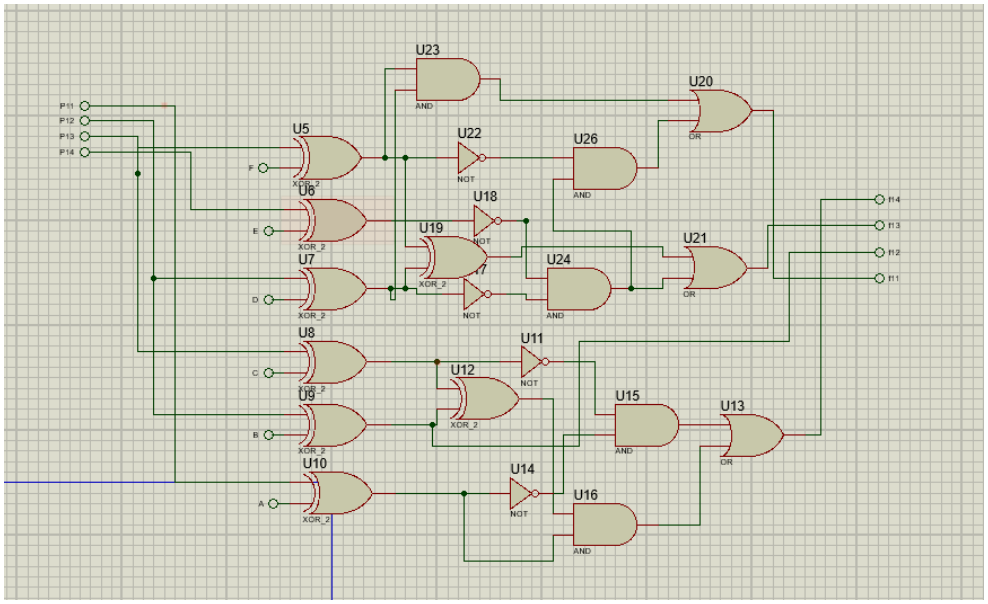
→ In this part multiplexer is used for Swapping purpose of R4 and L4 In decryption .
→ In encryption the Sel bit will be 0 and in Decryption Sel bit will be 1 .
→ Then the output going forward with permutations given in PS .

Permuted text data

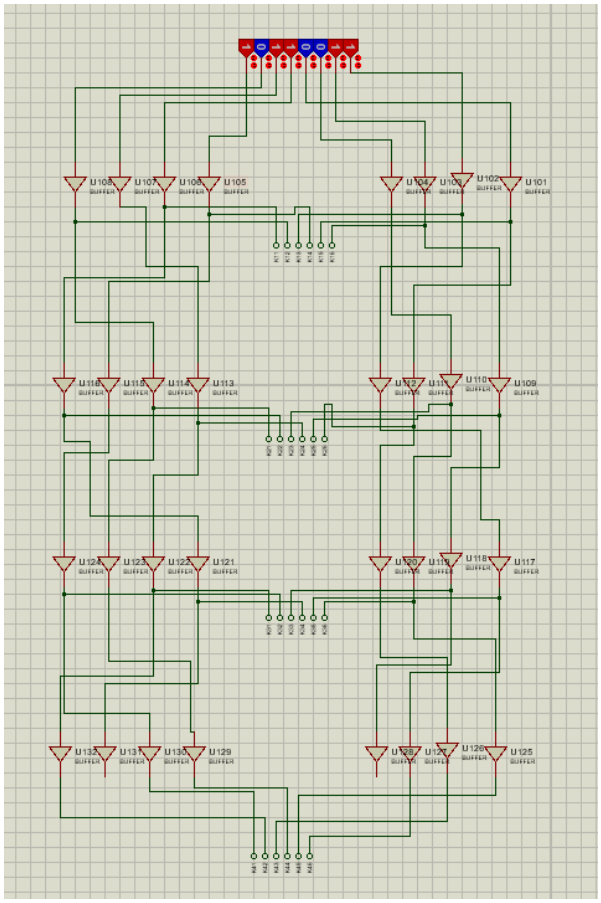




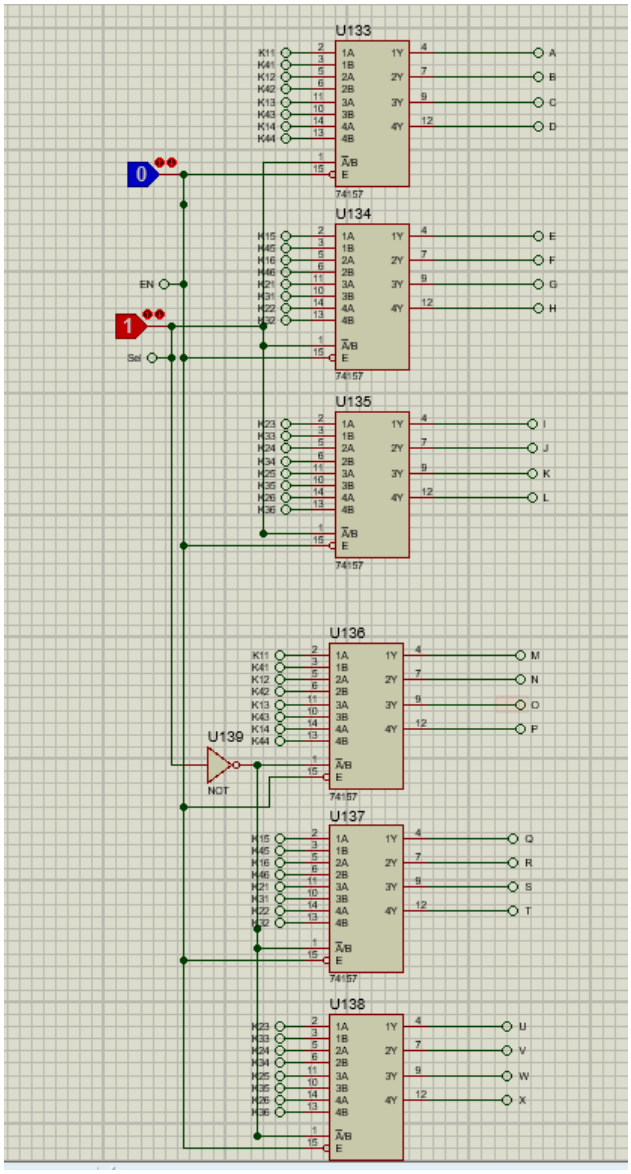
→ This is four step xor of left four bits with the output of function of right four bit and 6 bit generated round Key .



This is combinational circuit for the function in between LSB 4 bits and 6 bit round key .

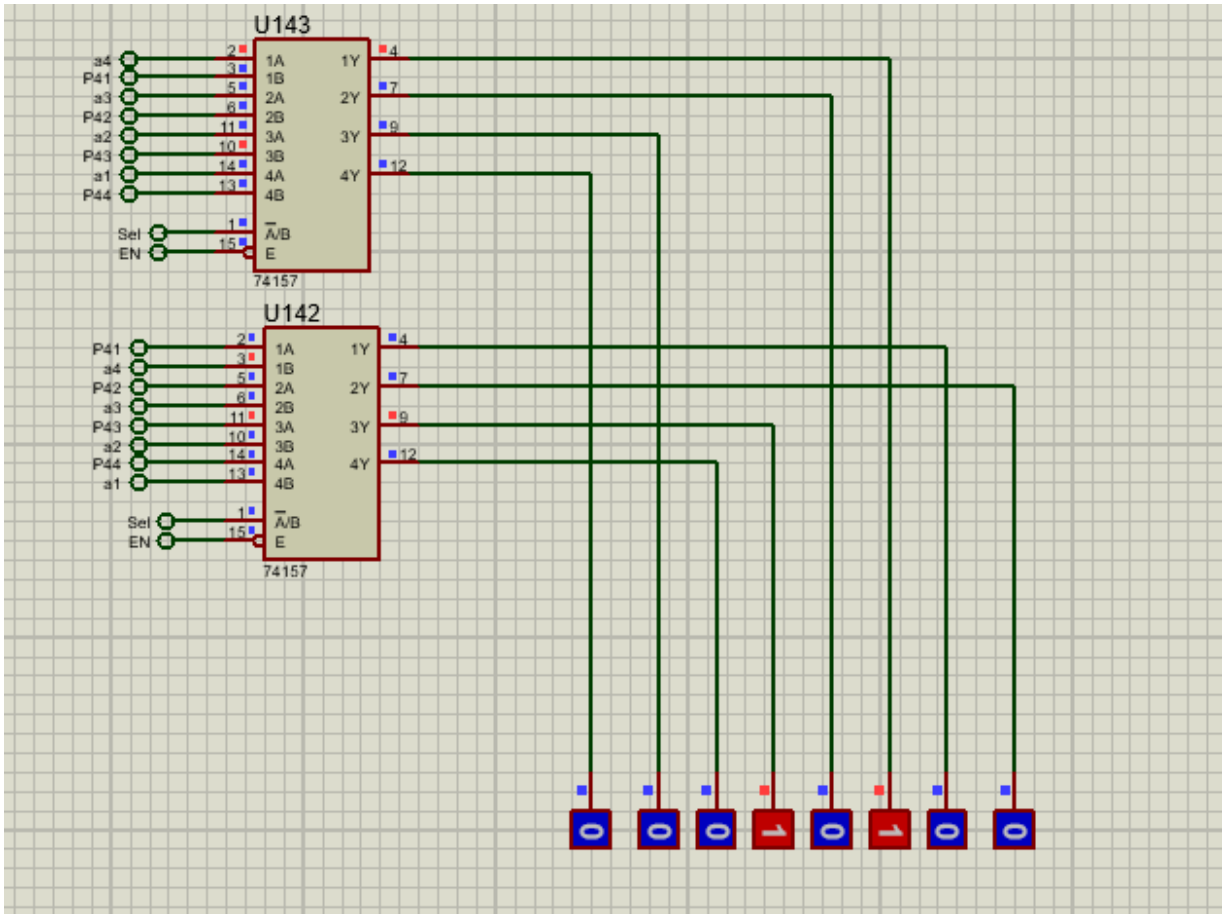


→This is four step round key generation



→This part of the circuit is for multiplexing the 4 round keys according to decryption and encryption .

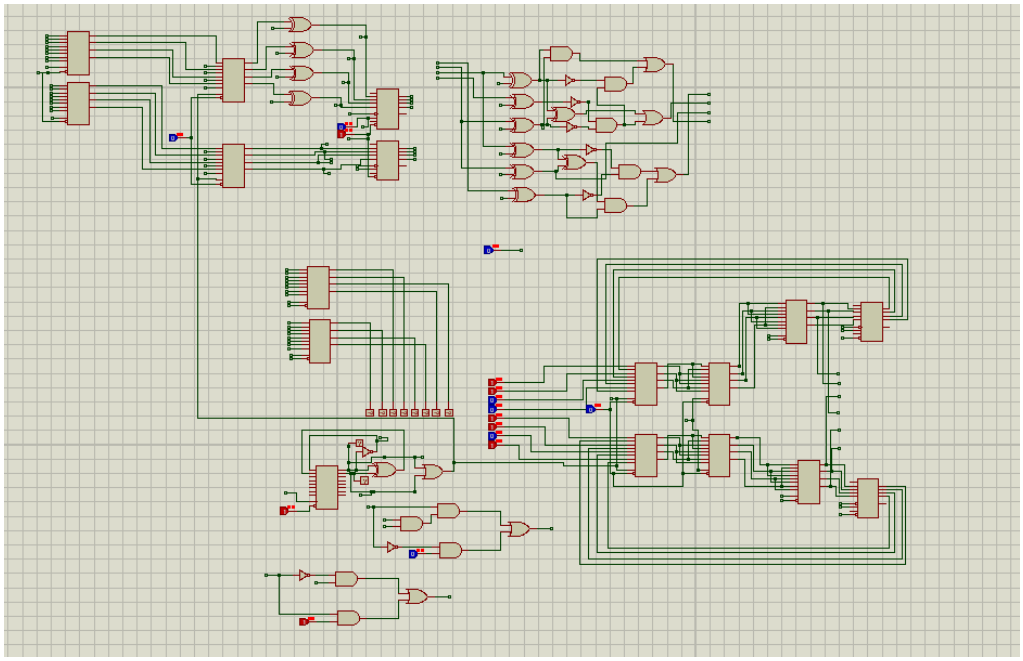
→ Bit 0 for encryption and bit 1 for decryption

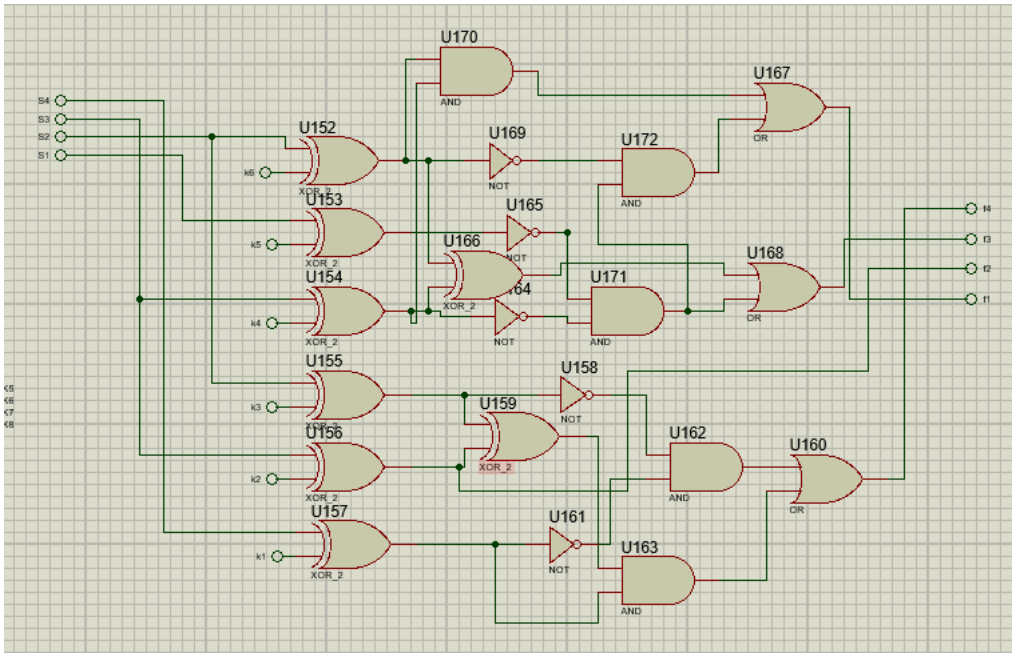


→ Output with permutations

Sequential Approach

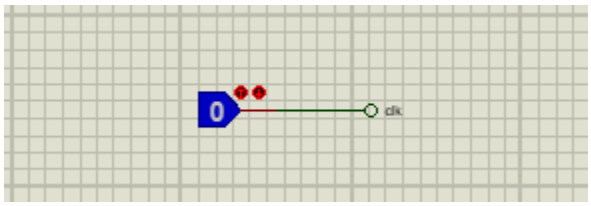
→ The Input for both sequential and combinational circuit is same .

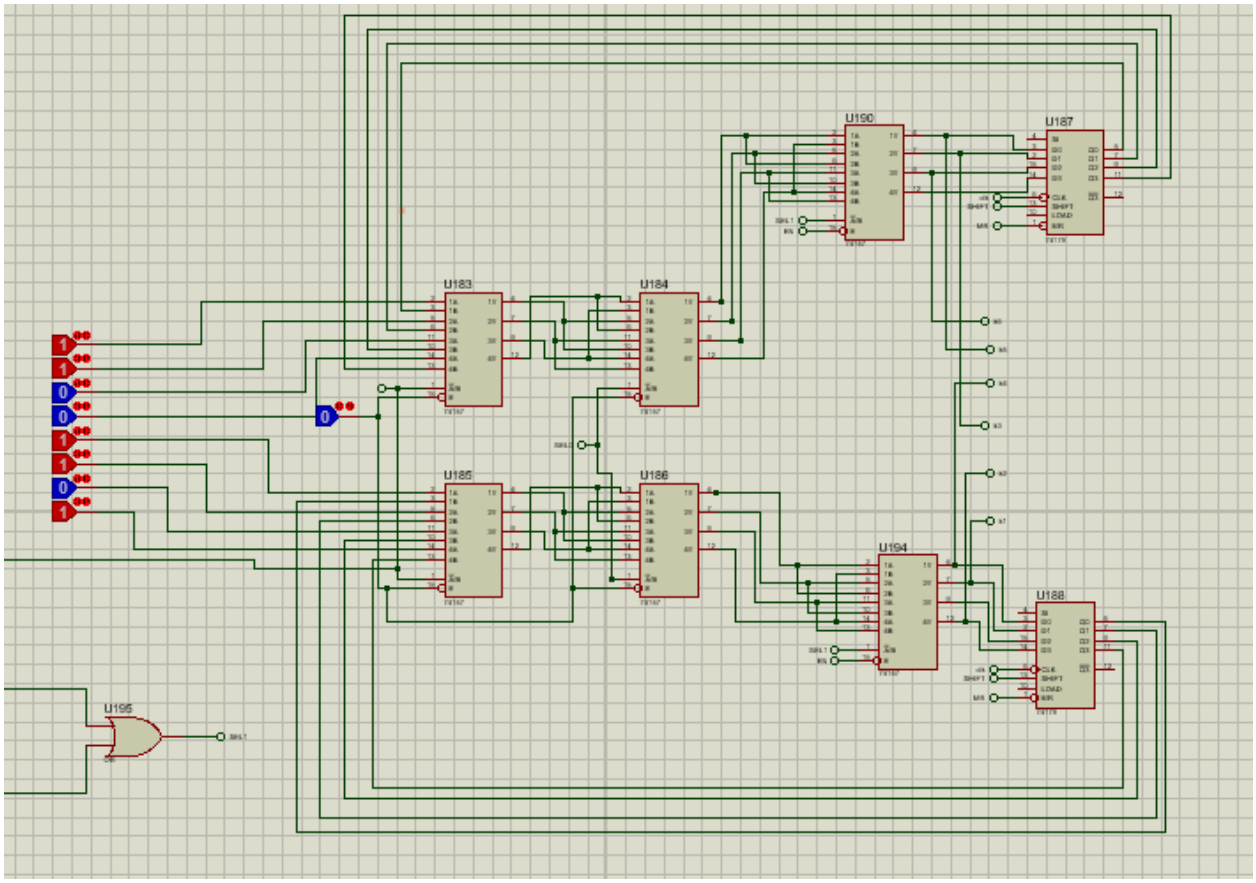




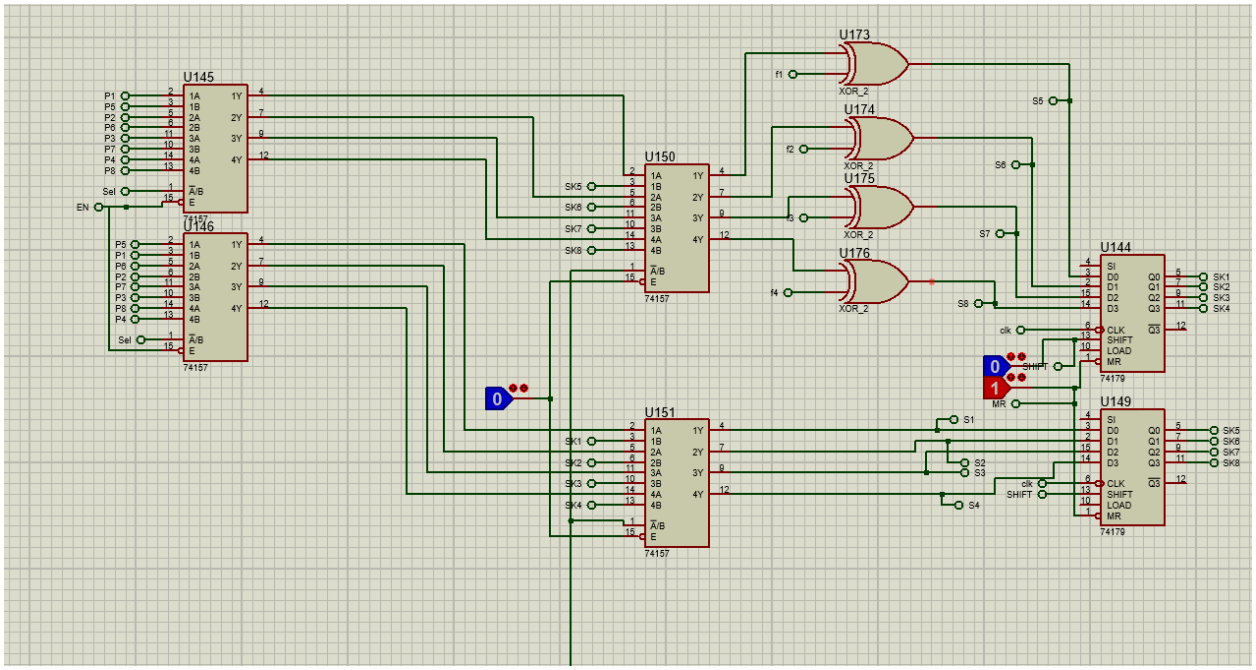
→ This part is for the function between the 6 bit round key and 4 bit LSB .

→This is for clk . And for running the sequential circuit we have to toggle rising 3 times after running the simulation

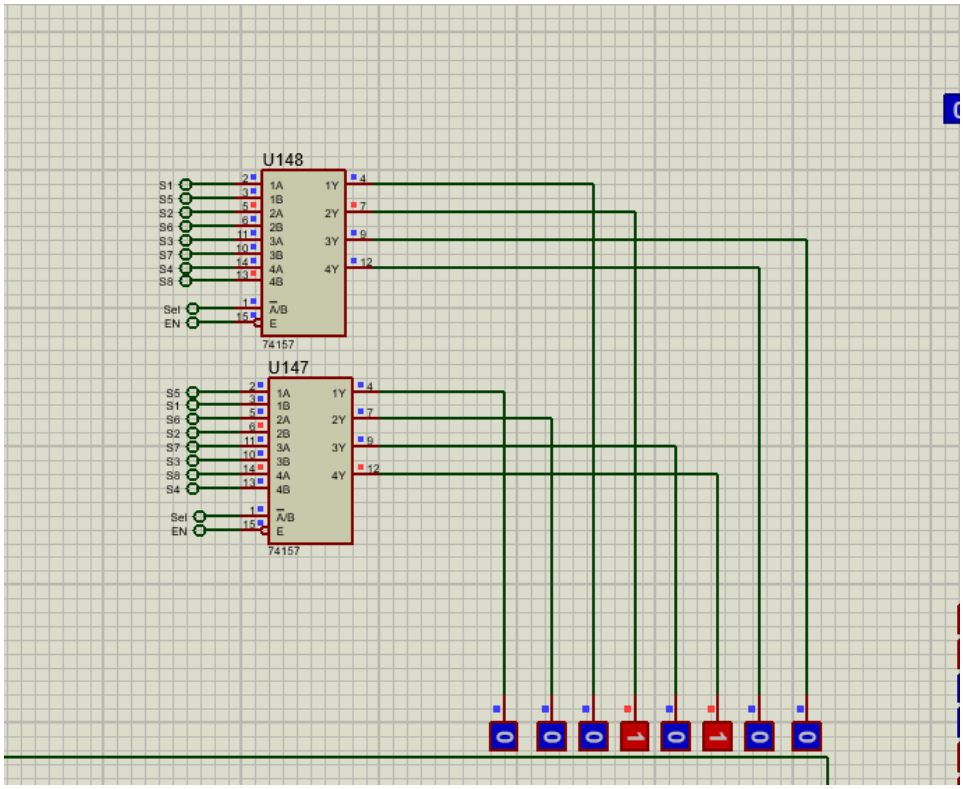




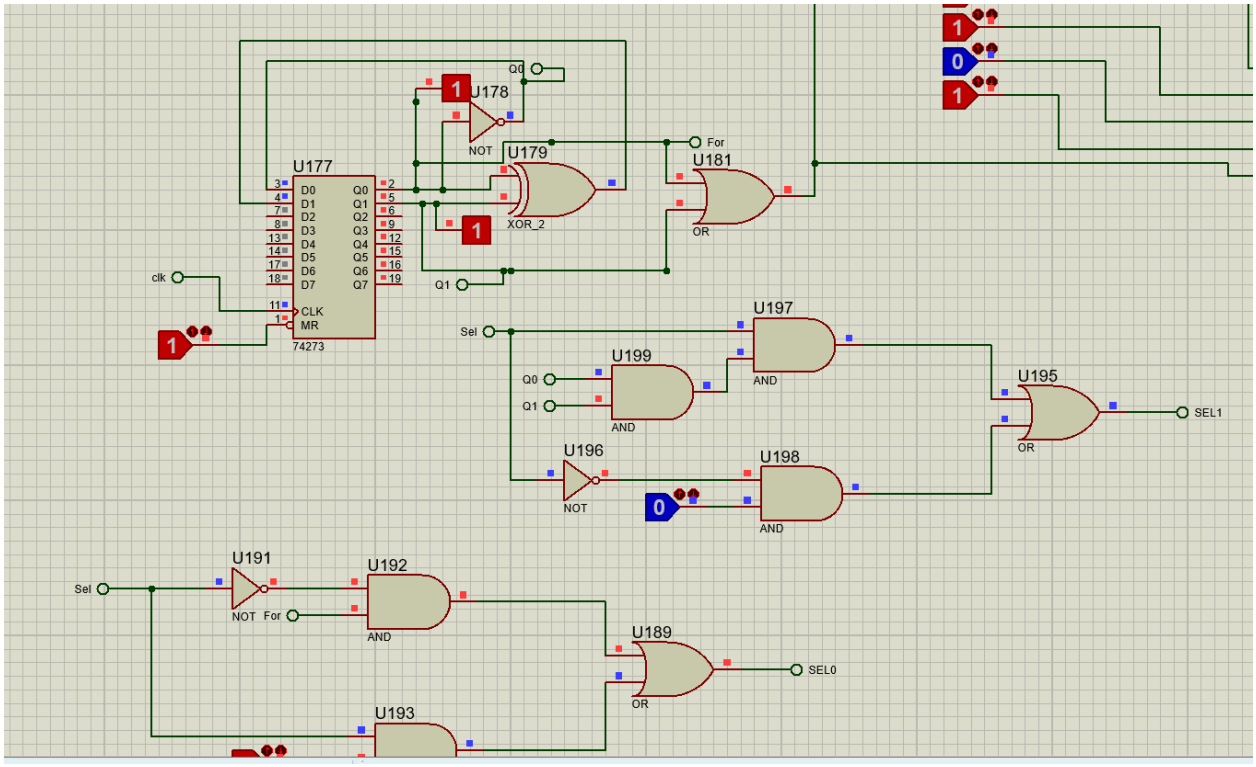
→ This part is for round key generating



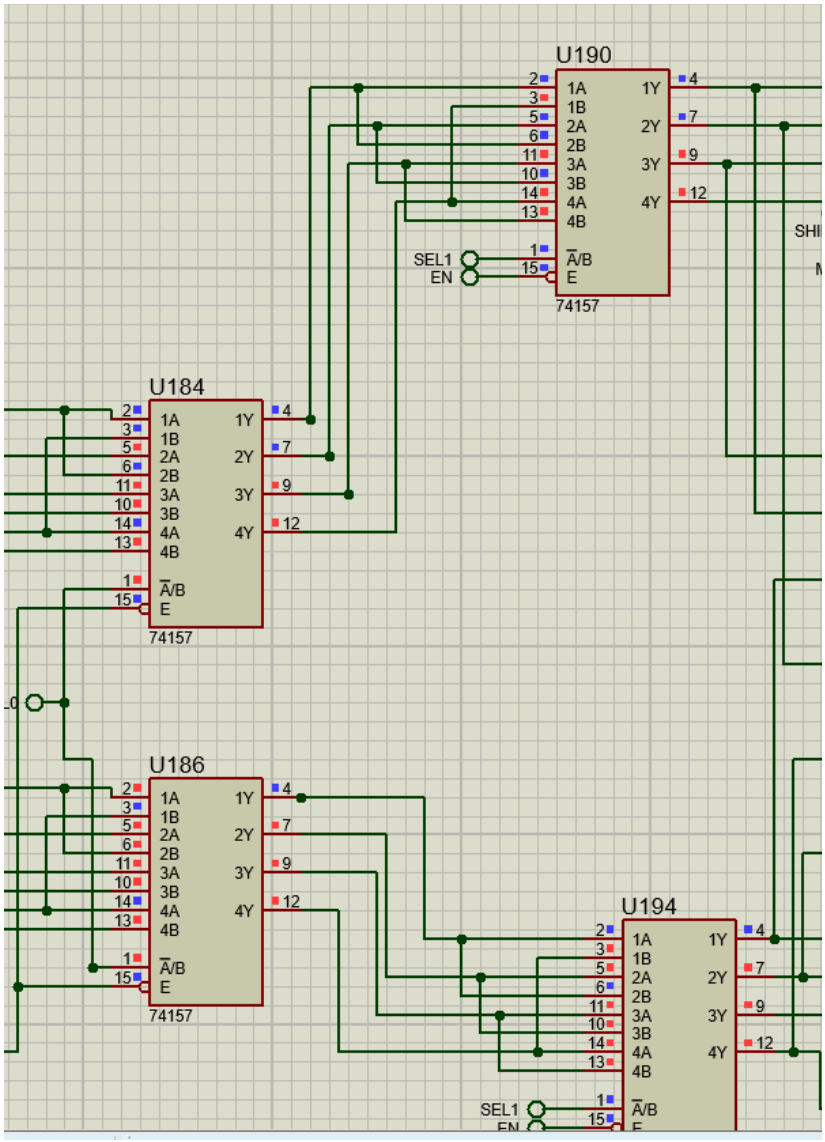
→ This part is for to get every round of 8 bit text data



→ This is output after three clock cycles



→ This part is for generating control signals to get desired shifting of bits



→ This is a kind of Barrel shifter which shifts differently in different cycles .