DIGISIM PS-1
(SEQUENTIAL CIRCUIT)

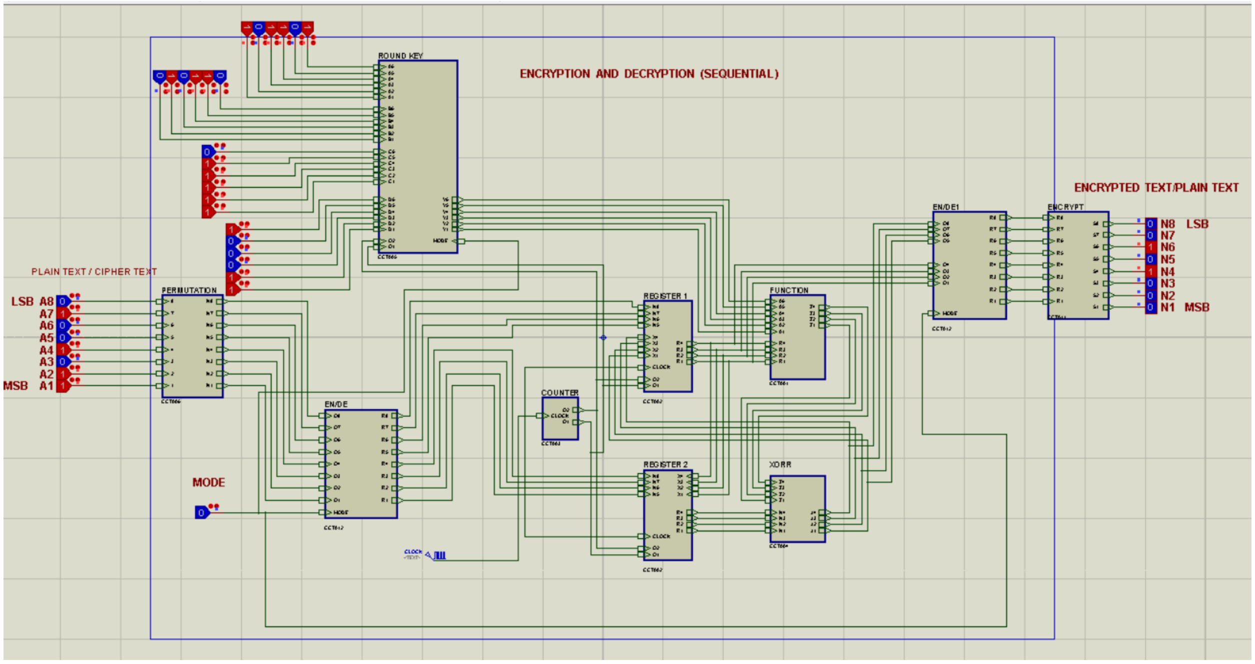
TEAM MEMBERS

1.AYUSHI KUMARI(22095020)
2.ALLU DEEKSHITA(22095009)

PROBLEM STATEMENT

To design and simulate a digital circuit that encrypts a given digital input using a simplified version of the DES algorithm.

CIRCUIT DIAGRAM



COMPONENTS USED

1. 6 4x1 mux
2. 2 jk flip flop
3. 8 d flip flop
4. 8 2x1 mux
5. Logic gates (2+17+4)

Total cost of the circuit=50.3(encryption+decryption)
cost=18.1(only encryption)

APPROACH

1.TO GENERATE ROUND KEYS→ round keys are generated using the same combinational circuit and the four round keys generated are given as input. Now 6 4x1 mux are used. The bits of 1st round key (A1 A2 A3 A4 A5 A6) is given as 1st input of the every mux(A1 to 1st mux, A2 to 2nd and so on).similarly bits of 2nd round key is given as input to 2nd input of every mux and so on. Now a common counter is connected to the select lines of all the mux s.t. When counter is 00, round key one is given as output, when counter is 01, round key 2 is given as output and so on

For incorporating description , we will take input mode.
Mode 0→encryption
Mode 1→ decryption
Mode is taken xor with the output of the counter in the generation of round key s.t. When mode mode is 0. Output of counter remains same but when mode is 1, output is reversed(goes 11 10 01 00). Then round key 4 is given as output first, then 3rd round key and so on.

2. EN/DE BLOCK FOR SWAPPING LEFT AND RIGHT PART→ when mode is 0 output from the permutation block(which performs permutation on initial plain text) is given as input. But when mode is 1, left and right halves of the permuted text are swapped.

3. REGISTER1 and 2→ made a PIPO register using d flip flop, input of the d flip flops in register 1 is output from the xor block. The output of the d flip flops is given as 2nd input of 4 2x1 mux, the 1st input of the mux will the right half part of the permuted text. The OR of the output bits of the counter is given to select line, when counter is 00, its OR will be 0 and right part of permuted text is given as input once, after that OR of the counter will be one nad the output of the XOR block will be given as output of the register 1.

The output of the register 1 is given as input to FUNCTION block along with the round keys.

In 2nd register, the same procedure is used except that when the counter gives 00, the left part of the permuted text is given as output and for the rest of the counts, the output is the previous input to the function.

The output of the register 2 and the output of the function block goes as input to xor block.

After 3 clock pulses the output L4 and R4 produced are taken to EN/DE block which swaps left and right part is case of decryption and passes the same in case of encryption. Its output is inverse permuted and given as output.

The internal circuit of the function block, xor block and blocks doing permutation and inverse permutation remains same as in case of combinational.