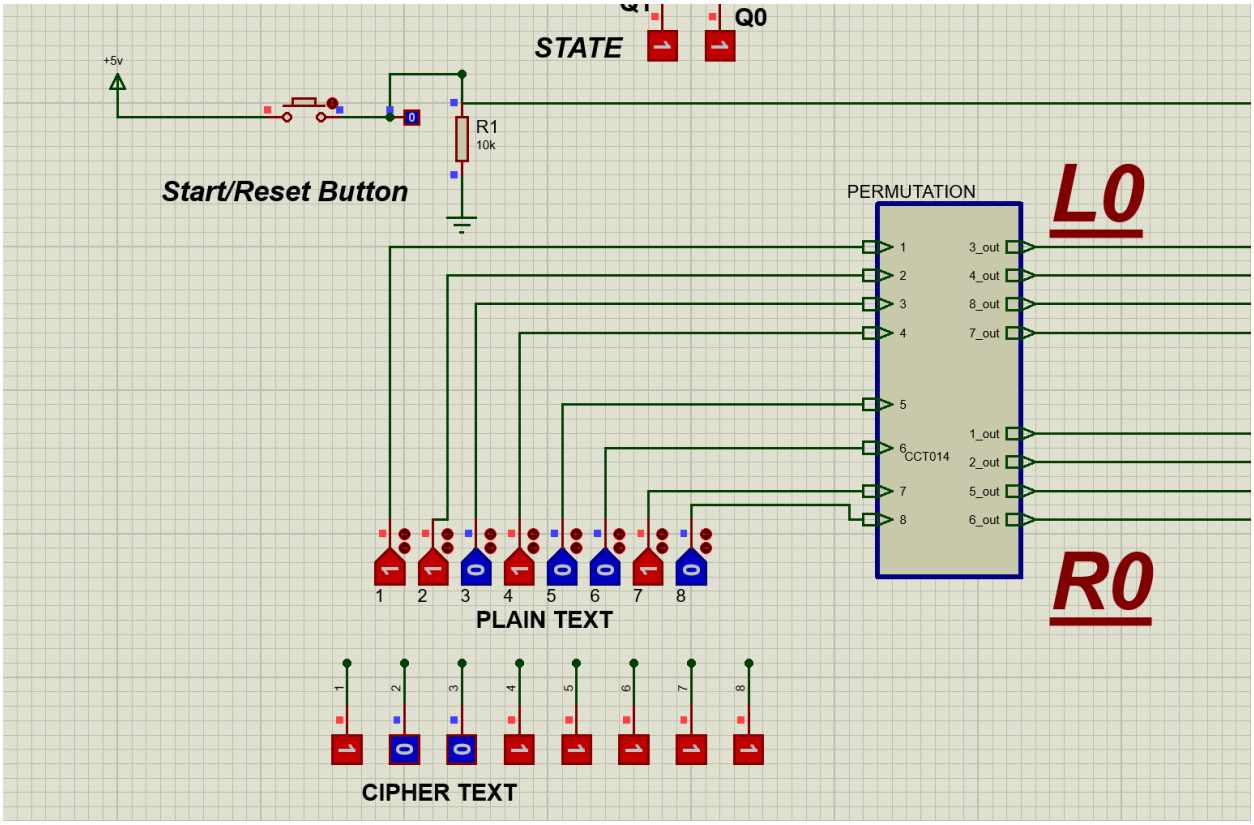
DIGISIM PS-1

Team Name: The Hawks

Sequential Circuit:

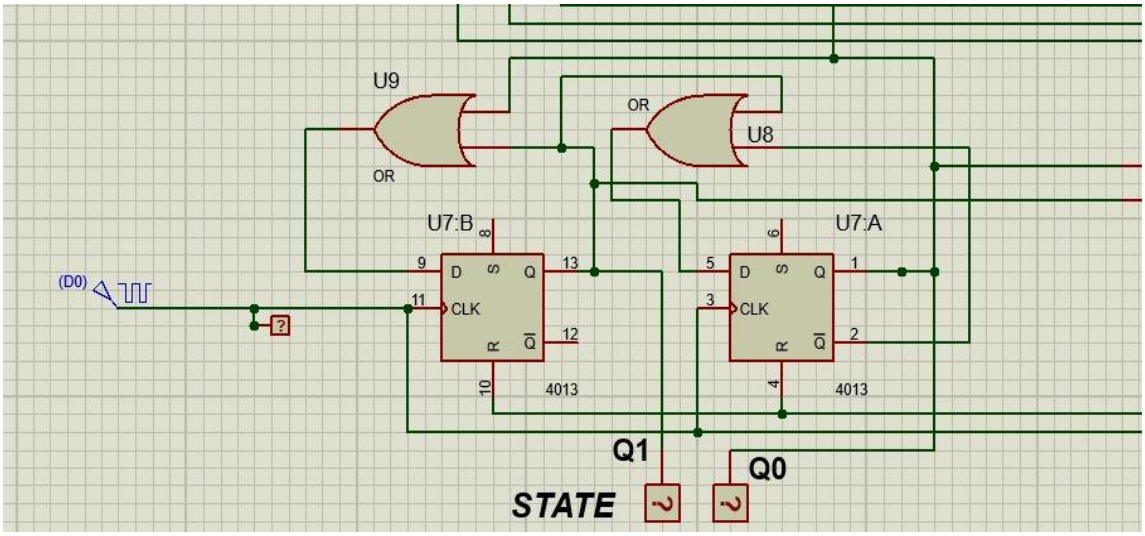
Part 1 (Encryption): **Total Cost = 68.5**

1. **INPUT METHOD:**

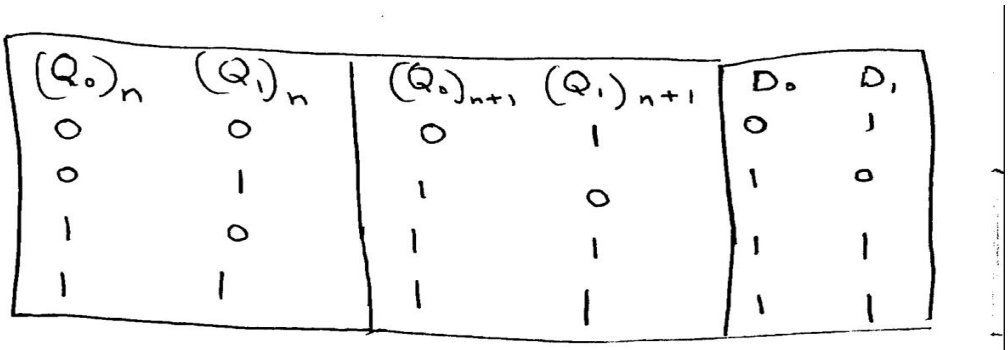


After you start the simulation, enter the plain text and then trigger the start button once. After the state 11 is reached through FSM, the cipher text is generated. On triggering the PUSH button, the state is set to 00.

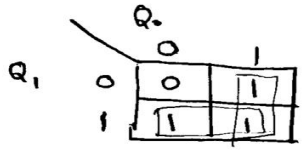
2. FSM:



Displayed above is the Finite State Machine (FSM) circuit utilized for the implementation of round-wise key generation, alongside the use of the f function and XOR gates in each instance. The circuit comprises four states. Specifically, Q1 Q0 (00) denotes the completion of the initial encryption round, whereas 01, 10, and 11 correspondingly indicate the fulfillment of the 2nd, 3rd, and 4th rounds, culminating in the termination of the encryption process. This termination is facilitated by maintaining the state value at 11 once it has been reached. Following is the state diagram depicting the FSM:

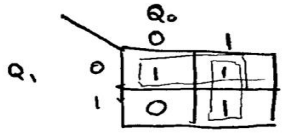


K-map For D_0 :-



$D_0 = Q_0 + Q_1$

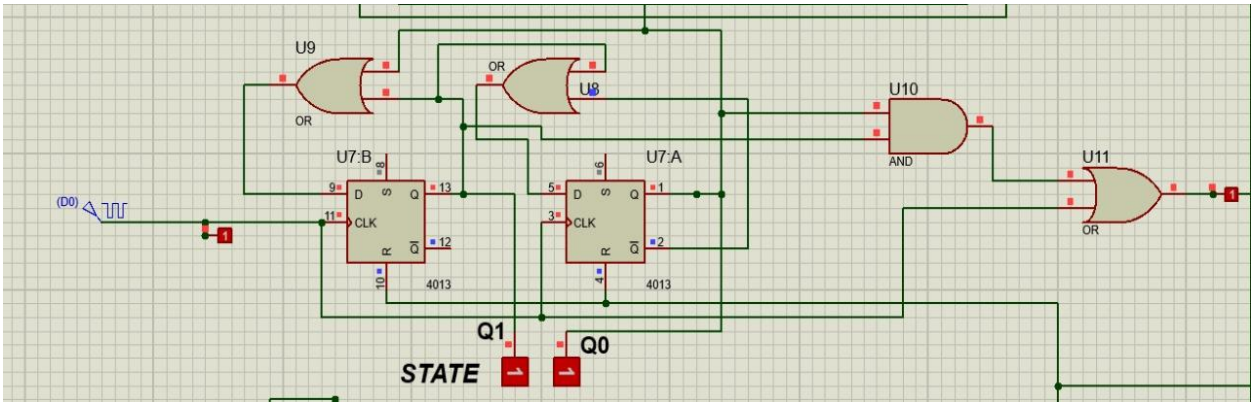
K-map For D_1 :-



$D_1 = Q_0 + \overline{Q_1}$

3. **CLOCK GATING:**

Clock gating is a power-saving technique in digital circuit design that selectively disables the clock signal to idle circuit blocks to reduce power consumption.

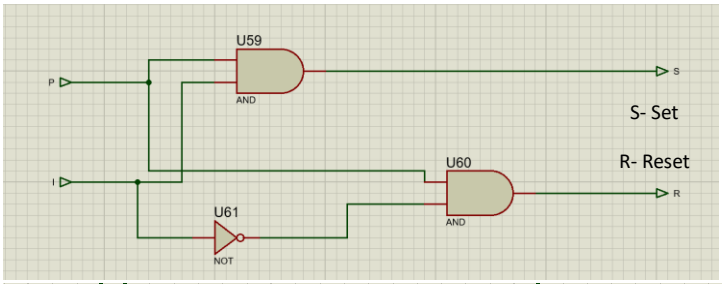


Output = Q_1Q_0 + clk

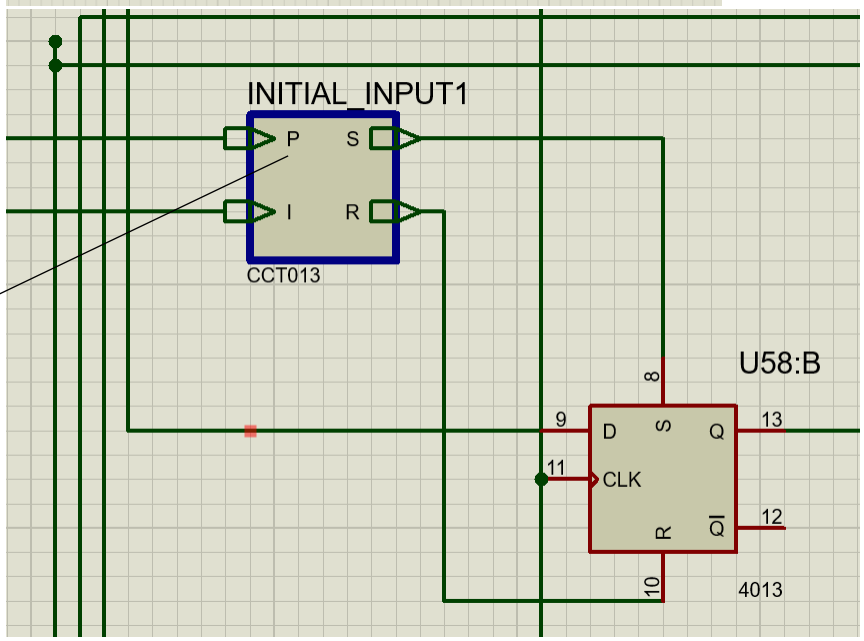
This output generated is being used in every sequential component of the circuit as clock.

4. **Input Loading in flip flops:**

The input (plain-text and initial key) is loaded in the flips-flops using the push button. This is achieved using the SET and RESET inputs of the flip flops.

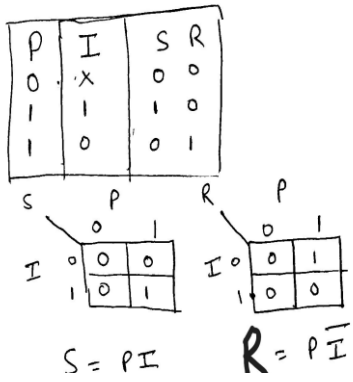


Child sheet of the initial input box



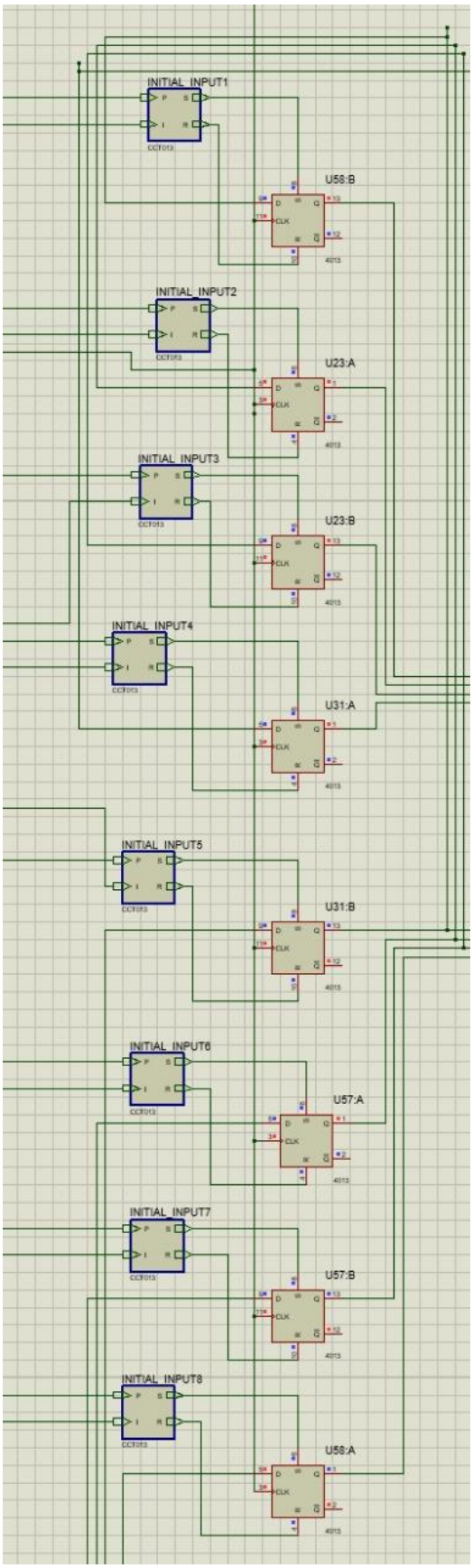
Here, P is connected to the output of the PUSH button whereas I is plain text bit.

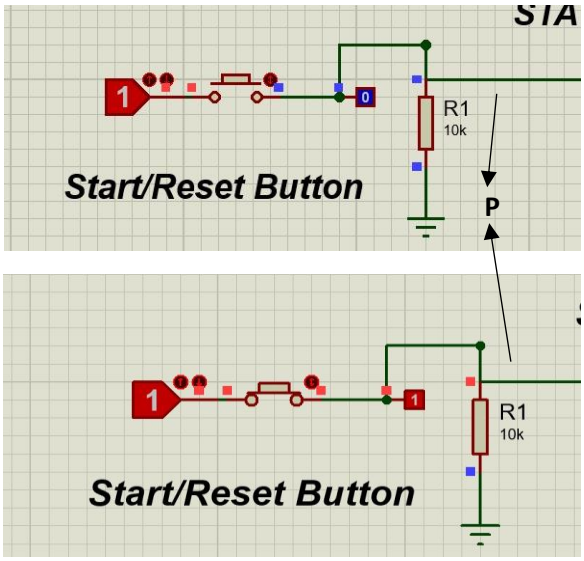
Here, when P is low, input is taken from D (i.e. output of the previous encryption round) that's why S,R = 0,0.



K-map for RESET and SET

Same input mechanism is used in loading of initial key.





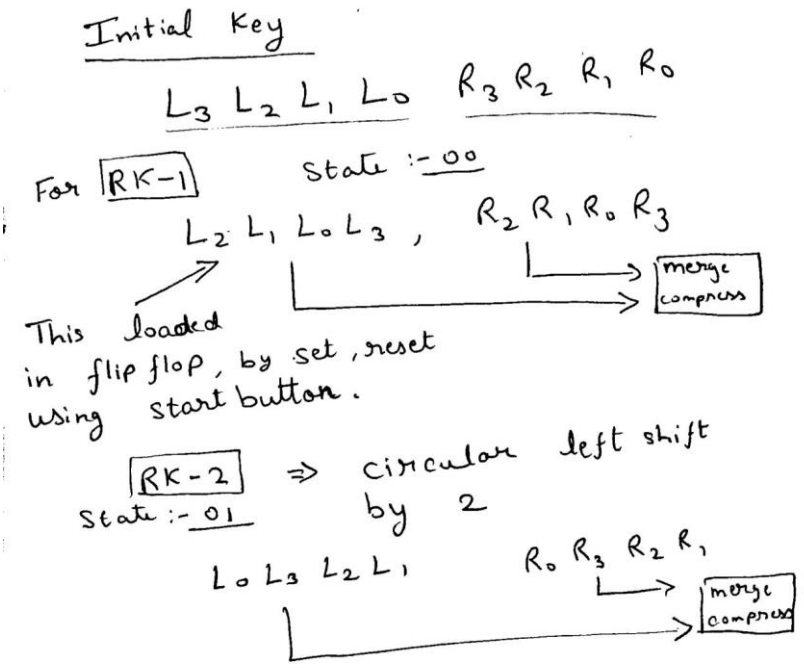
As P become high, it loads plain text, initial key to its respective flip flop. Also the state become 00.

These are the 8 D-flip flops used to store result of each round of encryption.

Each flip flop have its initial box whose output is connected to S, R of flip flop, used to load plain text

5. Round Key Generation:

Round key 1 is given as input manually (i.e. is it not generated by left-shifting, instead it is given using wire manipulations. However, all round keys after the 1st key are generated by using a left circular shifting circuit made of flip-flops.



State 00: circular left shift by 1 bit

Key loaded

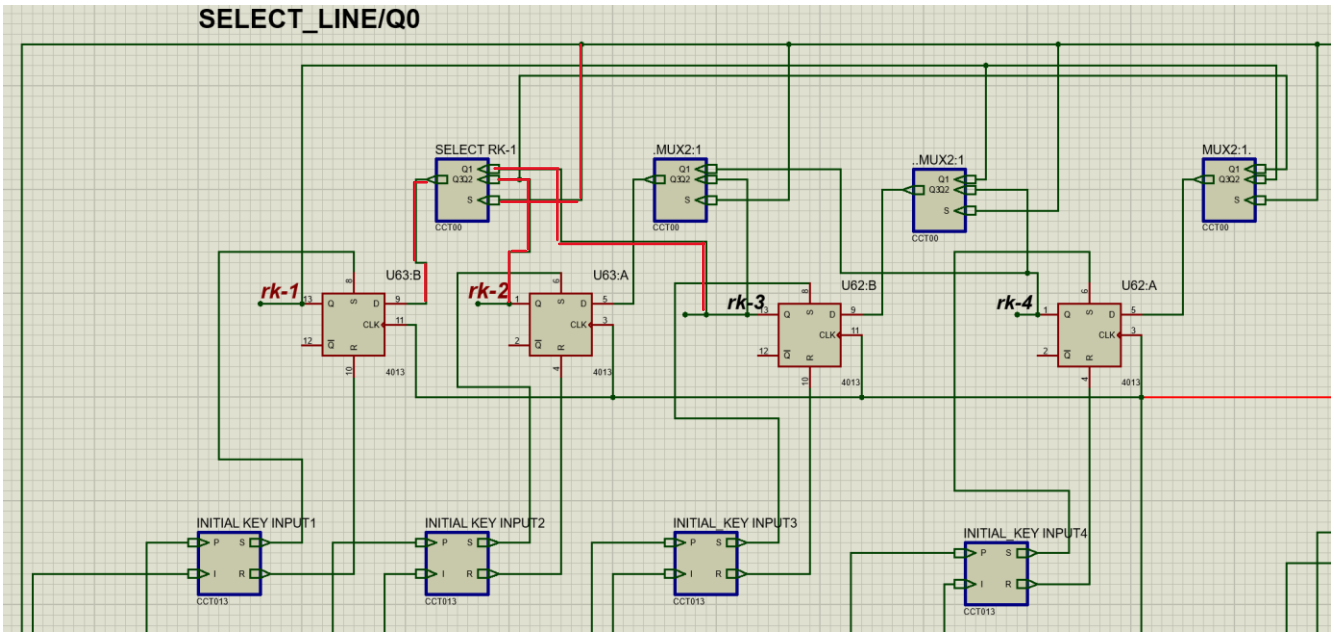
State 01: circular left shift by 2 bit

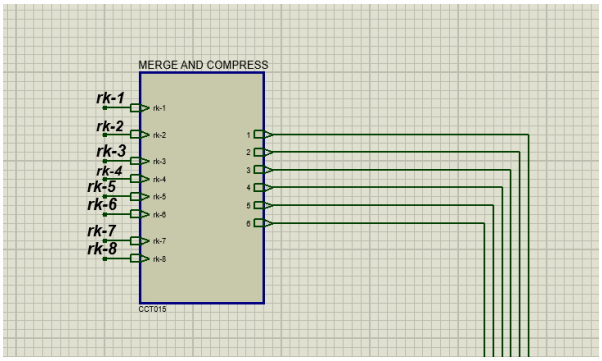
State 10: circular left shift by 1 bit

State 11: circular left shift by 2 bit

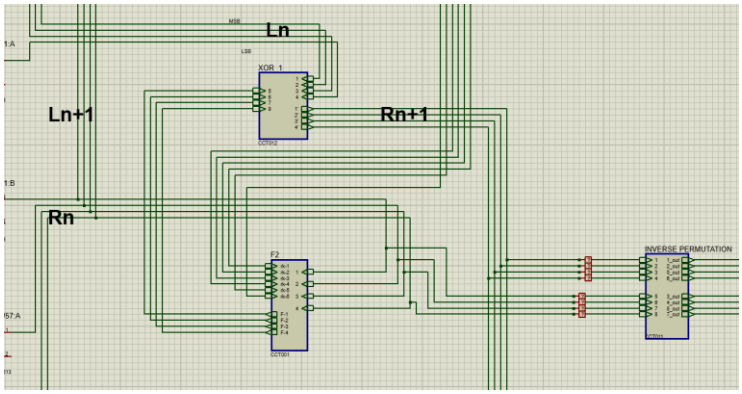
Here circular left shift is done twice in even state and once in odd state.

Therefore Q0 is used as select line for all the MUX.





This box merges and compresses round keys



This is same as that of combinational