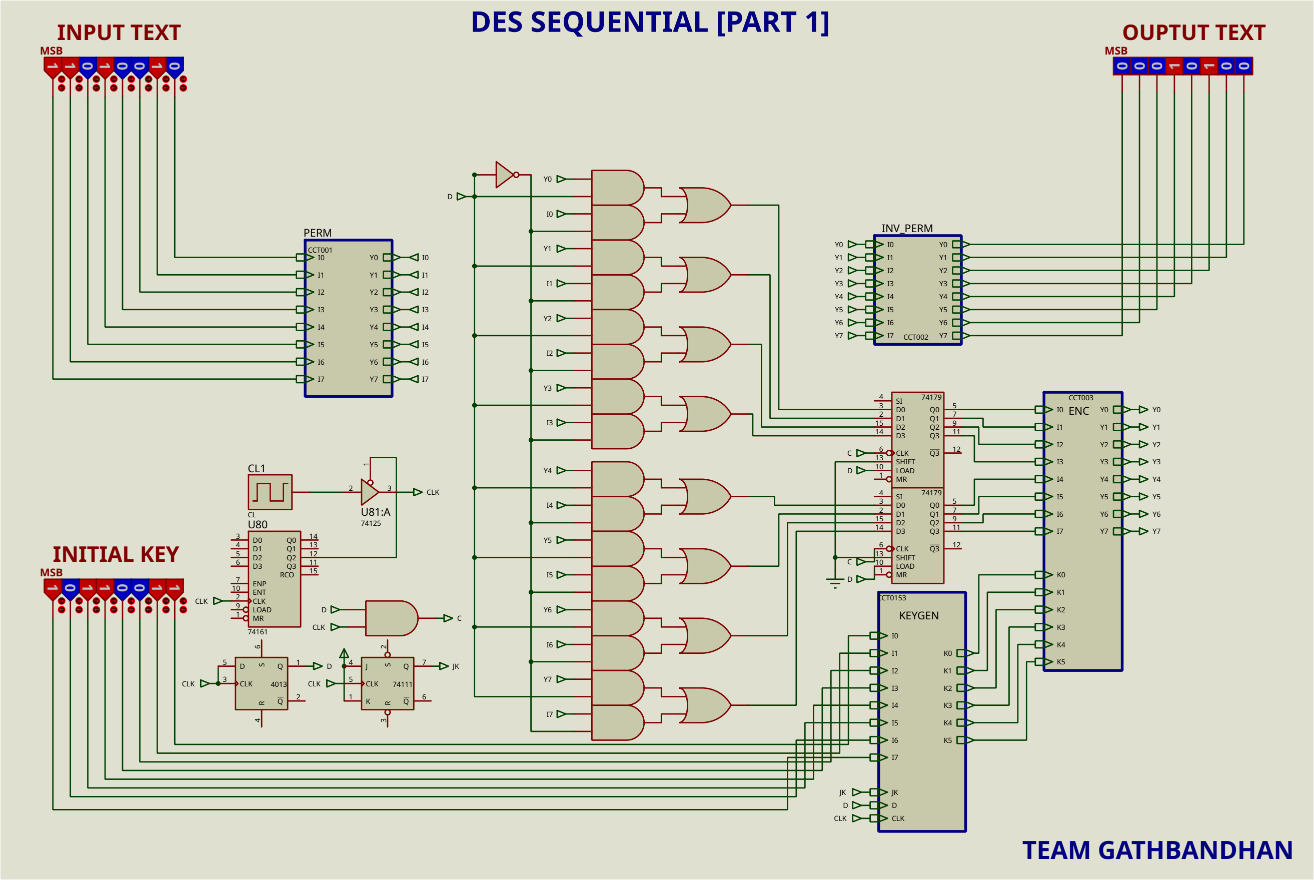
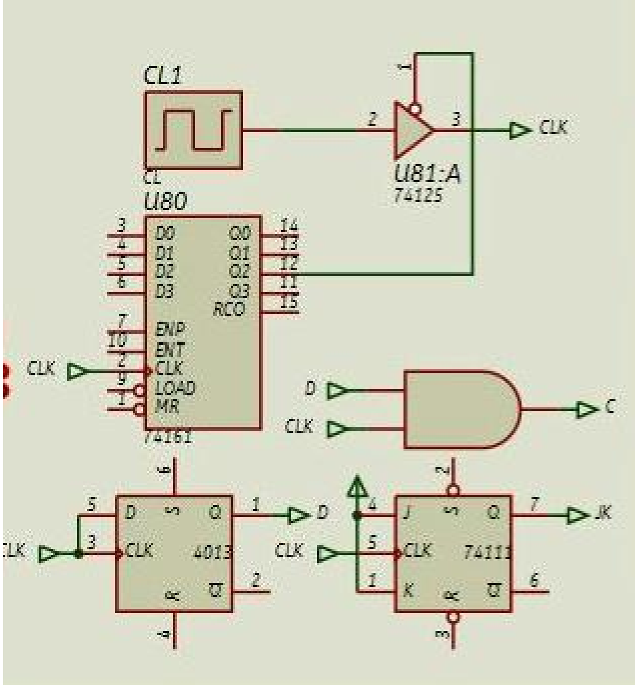
DIGISIM PS1 - SEQUENTIAL ENCRYPTION-ONLY CIRCUIT [PART 1]



This is the Encryption-only Sequential Circuit for DES Algorithm. Here, instead of cascading multiple blocks for each round, the clock changes rounds with the same set of blocks.
A counter[IC7461] is used to stop the encryption and decryption processes at 4 rounds.

In addition to this, a few other small elements are added for the functioning of the circuit:

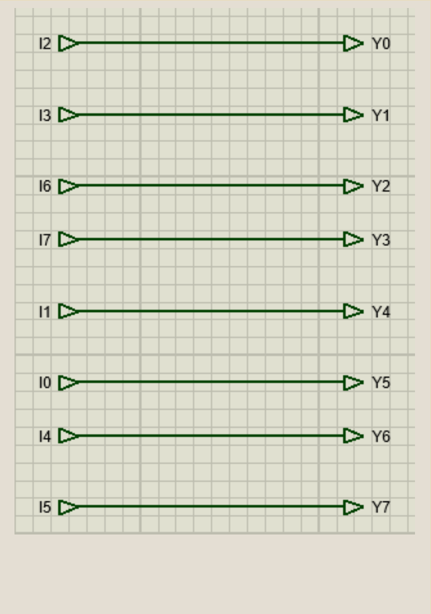
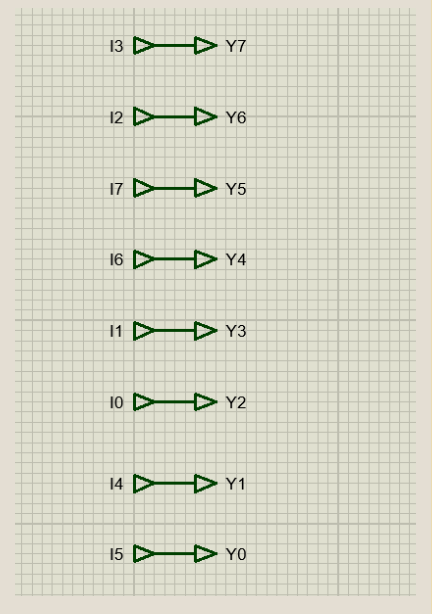
1. **D-LATCH** : This latch is initially **LOW**, and then switches to **HIGH** with the clock's first positive edge. This serves to first use the initial input, and then use the generated output as the input for subsequent rounds.
2. **JK MASTER-SLAVE FLIP-FLOP** : This flip-flop serves as a frequency divider and outputs a pulse with half the clock frequency.
3. **AND GATE B/W D AND CLK** : This functions as a switch to only take input when the latch is on. In other words, it adds a delay to the clock for the **ENC** block.



We have divided the rest of the circuit into several sub-circuits. These are :

PERM and INV_PERM

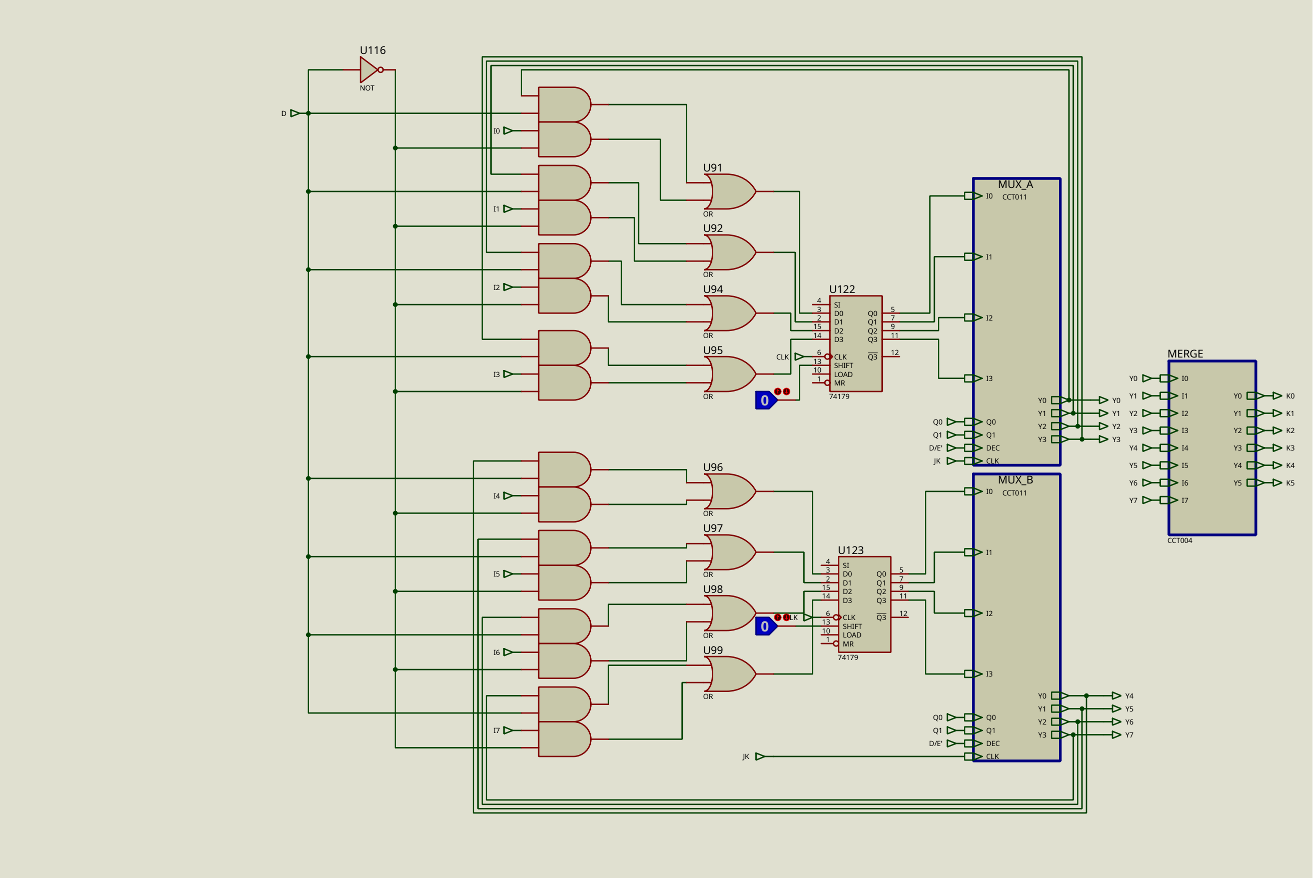
These are the sub circuits for permutations that are carried at the beginning and end of the encryption chain.

 I2 Y0 I3 Y1 I6 Y2 I7 Y3 I1 Y4 I0 Y5 I4 Y6 I5 Y7	 I3 Y7 I2 Y6 I7 Y5 I6 Y4 I1 Y3 I0 Y2 I4 Y1 I5 Y0
PERM	INV-PERM

We have implemented these permutations by simply connecting the inputs and outputs in the required order.

KEYGEN

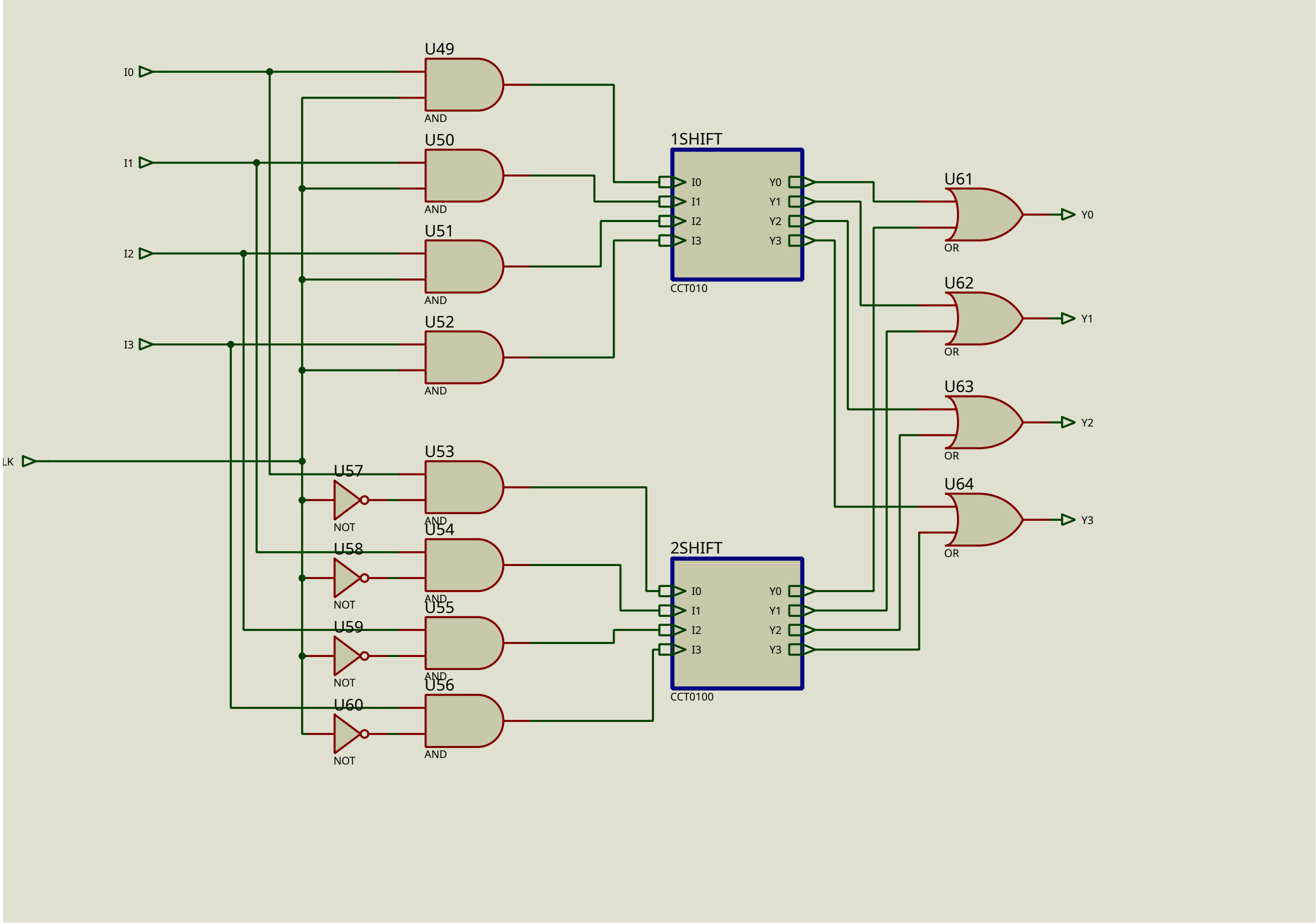
This sub-circuit sees the most variation from Combinational to Sequential Logic.



Here, a switch is added to take the initial input while the latch is OFF, and then switch to the generated output as input for the next round as soon as the latch turns ON. After this, a register is added for each half of the 8 bit input, this helps prevent racing by making the rest of the combinational circuit edge-triggered.
The register then outputs into the MUX ICs.

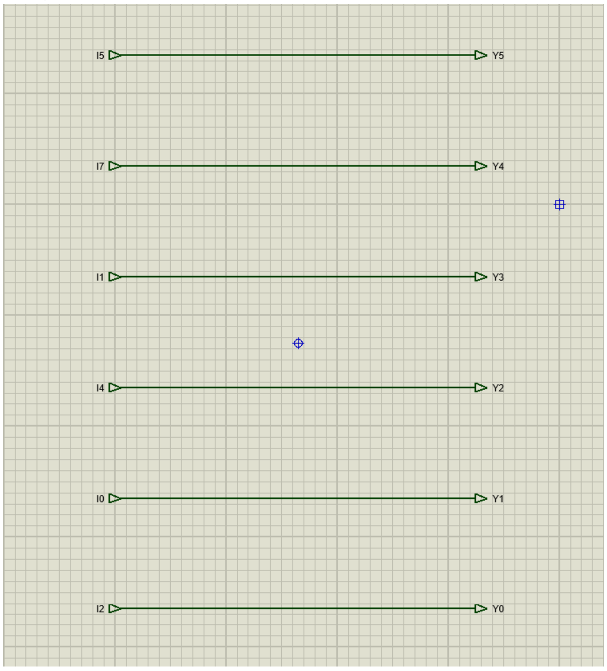
MUX_A AND MUX_B

These IC's handle the actual shifting of the input. In the encryptor-only circuit, a mux-like design is used to switch between 1 and 2 bit circular left shifts. The output is then OR'ed and outputted.



MERGE

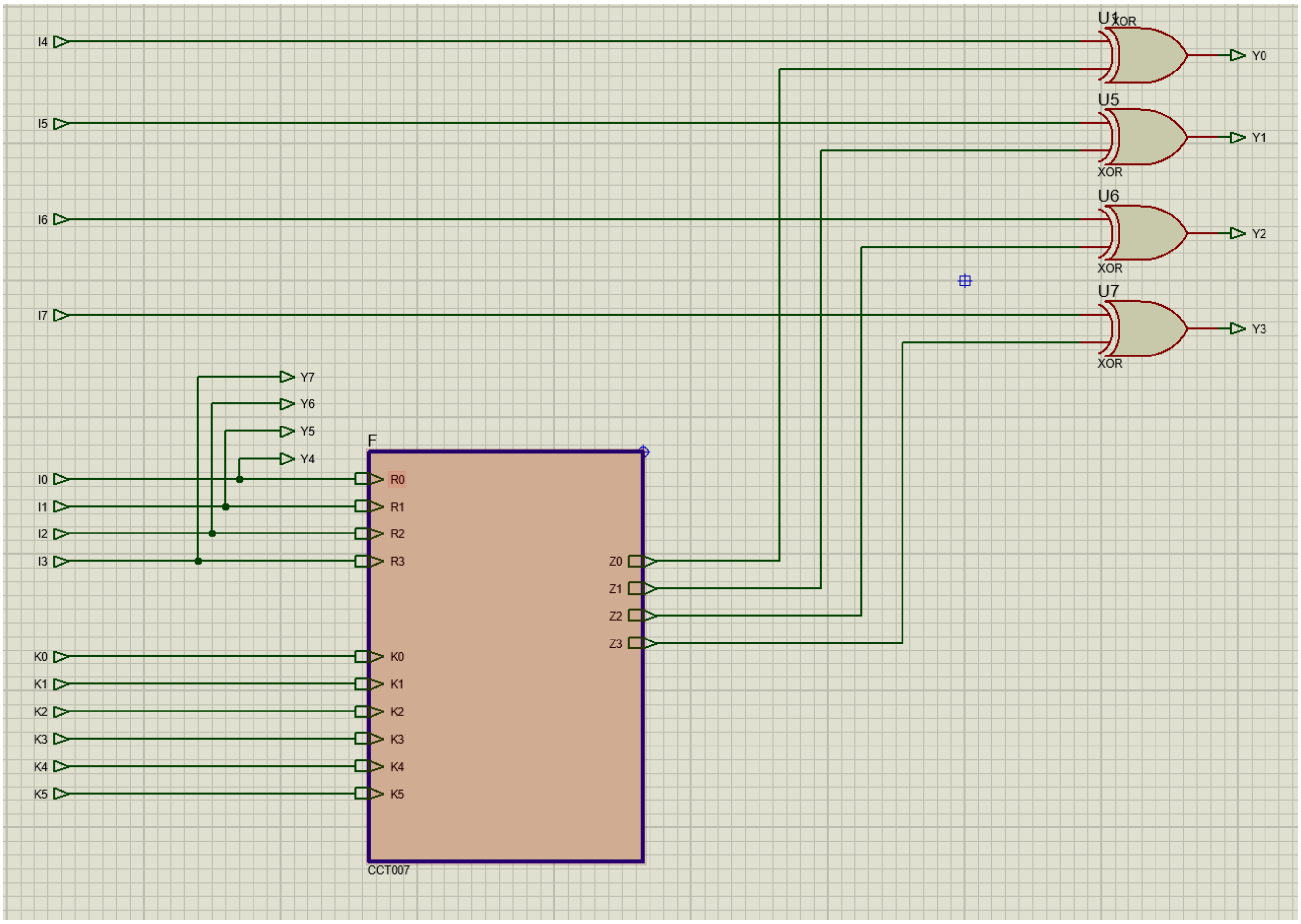
This sub-circuit implements the merge and compress function for key generation. It works by simply taking the required inputs and then permuting them. The ouptut is passed on as the round key



ENC

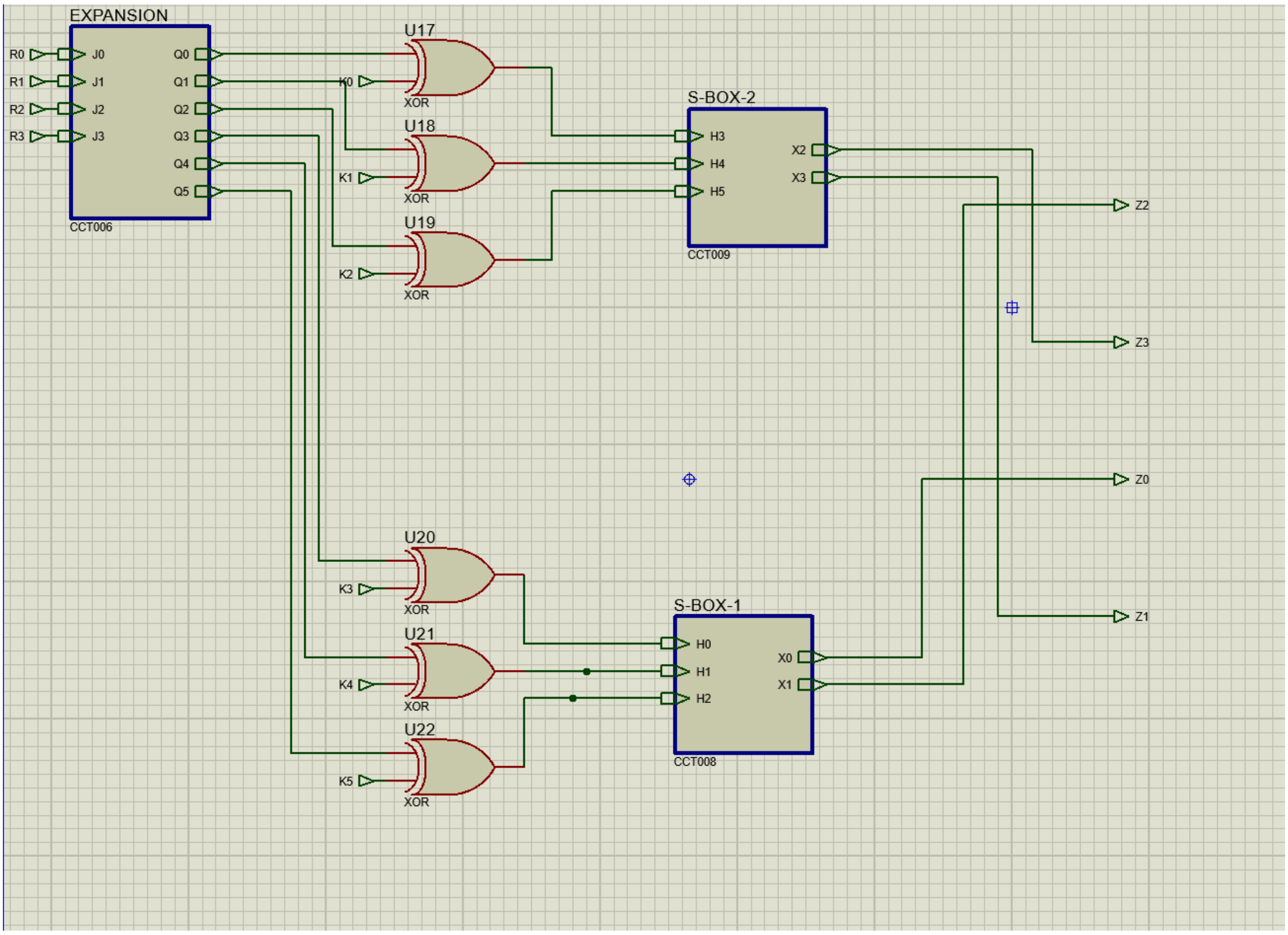
This sub-circuit is where the actual encryption takes place. Here, the right-half [4 bits] (left-half of the next round's input) of the input is passed into the F sub-circuit, along

with the round keys.
The output is then XOR'ed with the permuted left-half of the input to get the right-half of the next round's input.

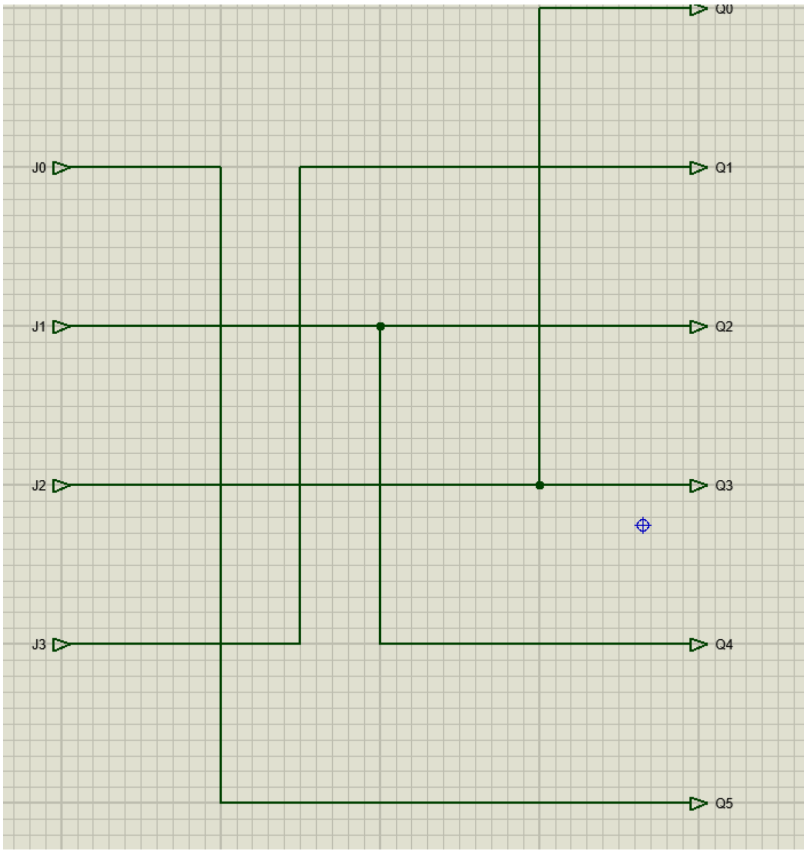


F

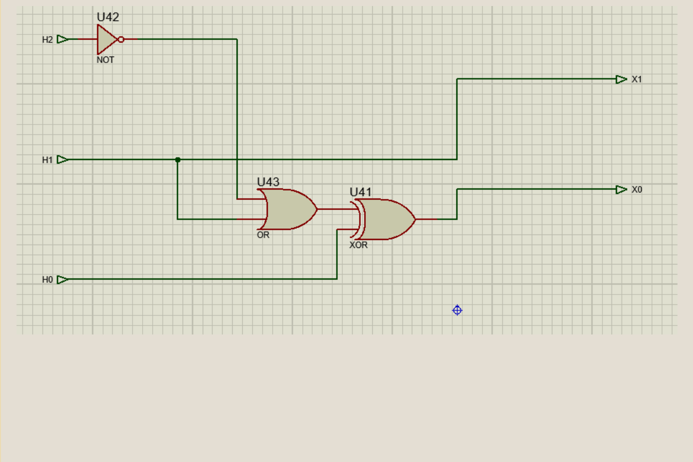
This sub-circuit implements function *"f"*. Here, the input[4-bits] is expanded to 6 bits, which is then bitwise XOR'ed with the round key. The output is then split into halves and then fed into the S-BOXES. The 2-bit outputs are then permuted and outputted.



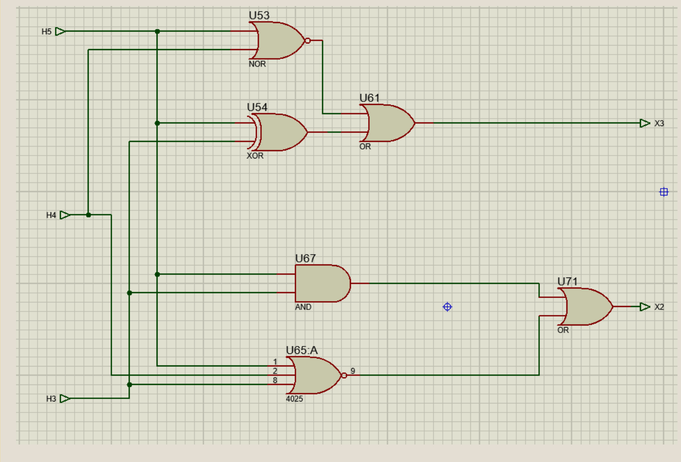
EXPANSION



S-BOXES

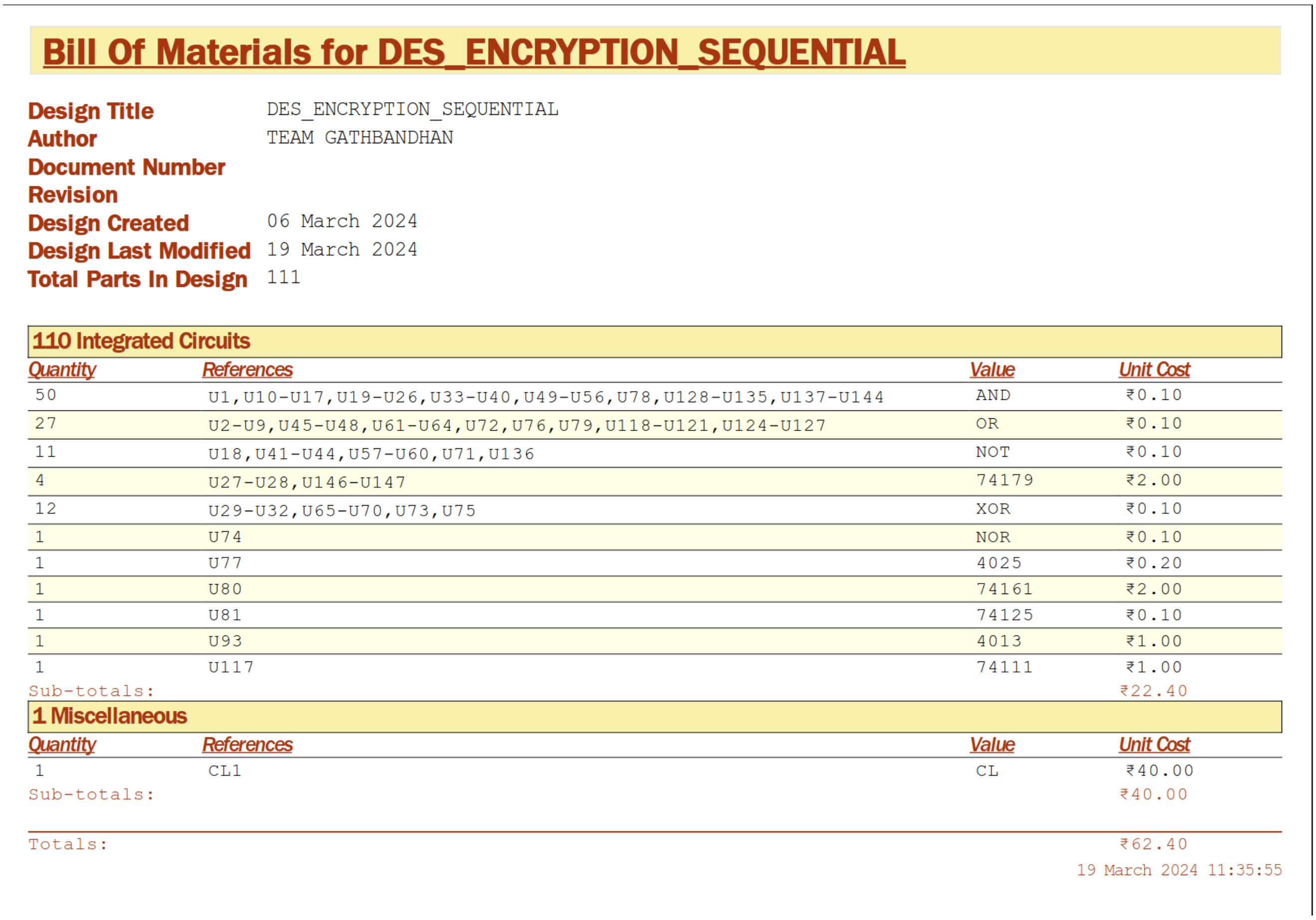


S-BOX-1



S-BOX-2

BILL OF MATERIALS FOR PART 1 [SEQUENTIAL]



Bill Of Materials for DES_ENCRYPTION_SEQUENTIAL

Design Title	DES_ENCRYPTION_SEQUENTIAL
Author	TEAM GATHBANDHAN
Document Number	
Revision	
Design Created	06 March 2024
Design Last Modified	19 March 2024
Total Parts In Design	111

110 Integrated Circuits

Quantity	References	Value	Unit Cost
50	U1,U10-U17,U19-U26,U33-U40,U49-U56,U78,U128-U135,U137-U144	AND	₹0.10
27	U2-U9,U45-U48,U61-U64,U72,U76,U79,U118-U121,U124-U127	OR	₹0.10
11	U18,U41-U44,U57-U60,U71,U136	NOT	₹0.10
4	U27-U28,U146-U147	74179	₹2.00
12	U29-U32,U65-U70,U73,U75	XOR	₹0.10
1	U74	NOR	₹0.10
1	U77	4025	₹0.20
1	U80	74161	₹2.00
1	U81	74125	₹0.10
1	U93	4013	₹1.00
1	U117	74111	₹1.00
Sub-totals:			₹22.40

1 Miscellaneous

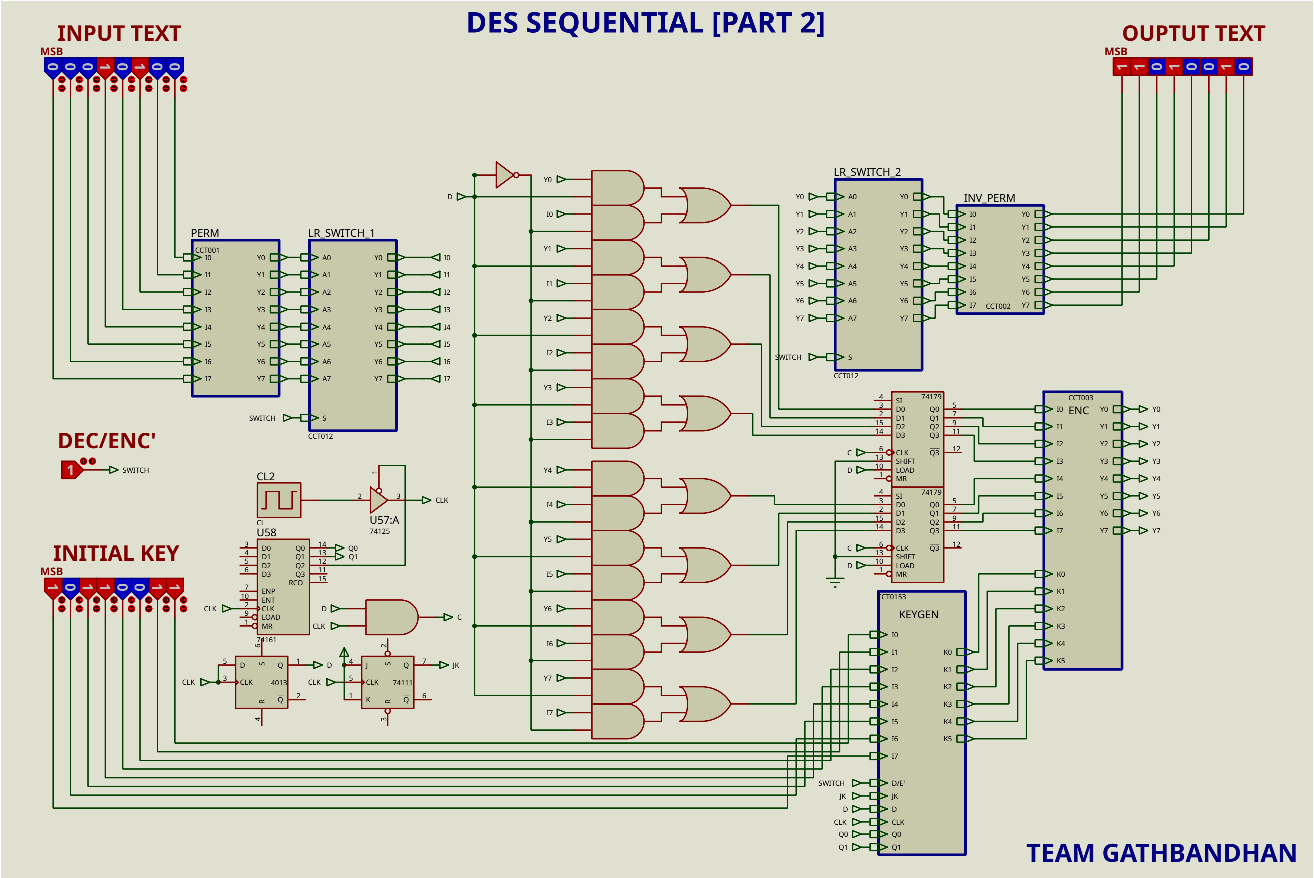
Quantity	References	Value	Unit Cost
1	CL1	CL	₹40.00
Sub-totals:			₹40.00

Totals: ₹62.40

19 March 2024 11:35:55

TOTAL COST : RS 62.40

COMPLETE 4-BIT DES [SEQUENTIAL]



This circuit builds upon the encryption-only circuit in the way that it can also decrypt encrypted text when put in the decryption mode.
This can be selected by switching the **DEC/ENC'** button from 0 to 1.

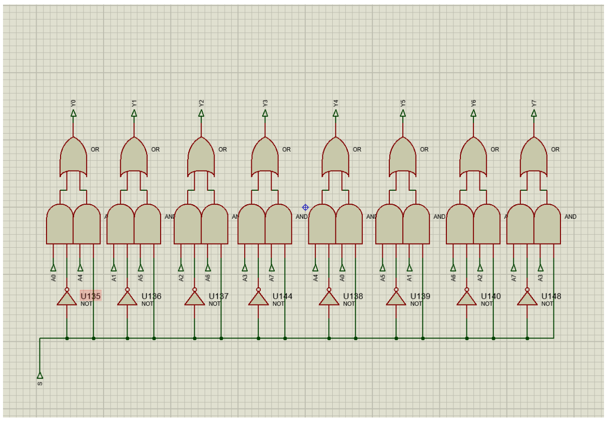
Logically, it differs from the encryption-only circuit in a number of ways:

1. The input and output have left and right halves switched.
2. The round keys are used in opposite order.

This is implemented schematically by adding two new sub-circuits:

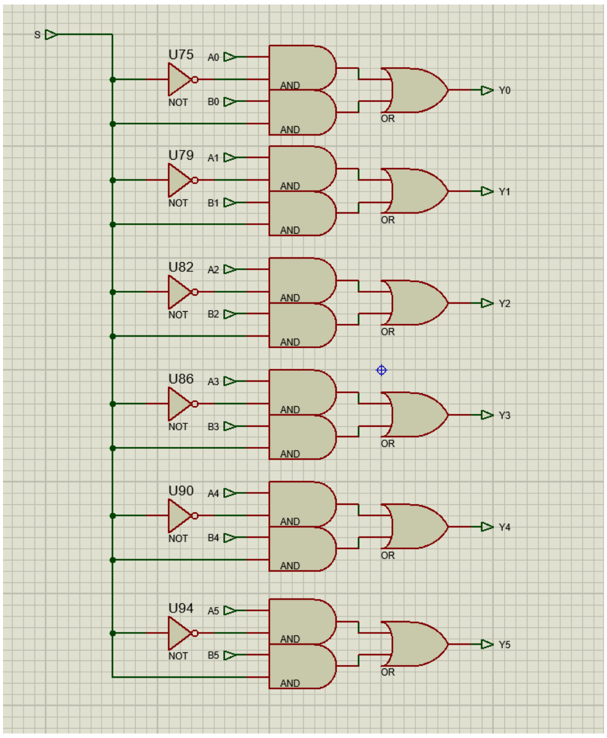
1. LR_SWITCH

This is a simple sub-circuit that switched the left and right halves when **DEC/ENC'** is HIGH.



2. HEX_SELECTOR

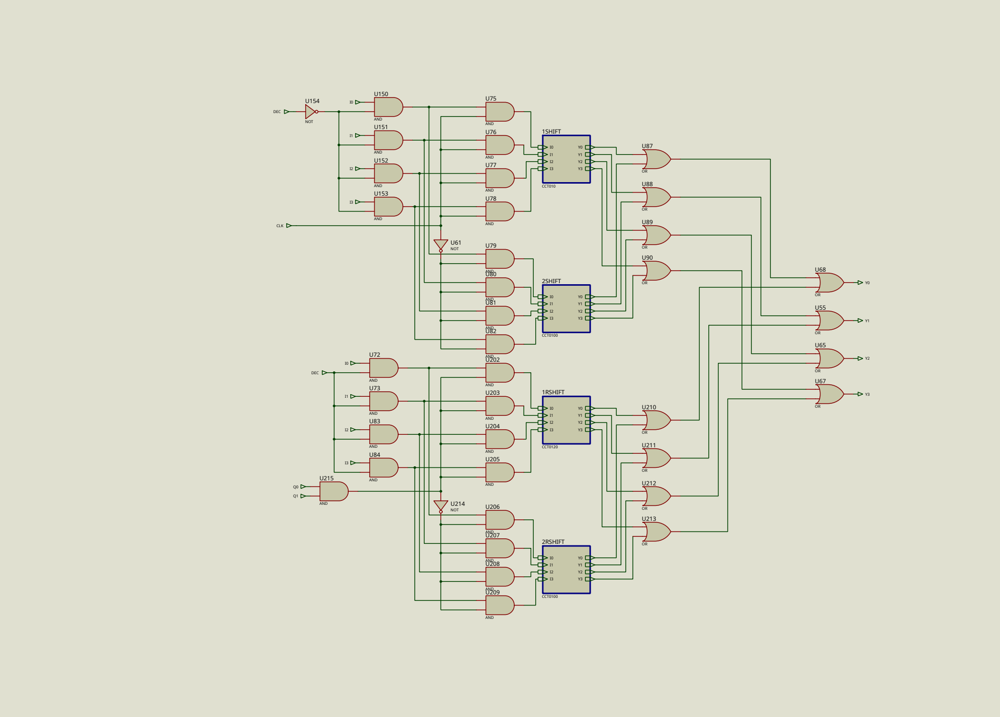
This subcircuits switches between the normal round-key order and the reverse order if **DEC/ENC'** is set to HIGH.



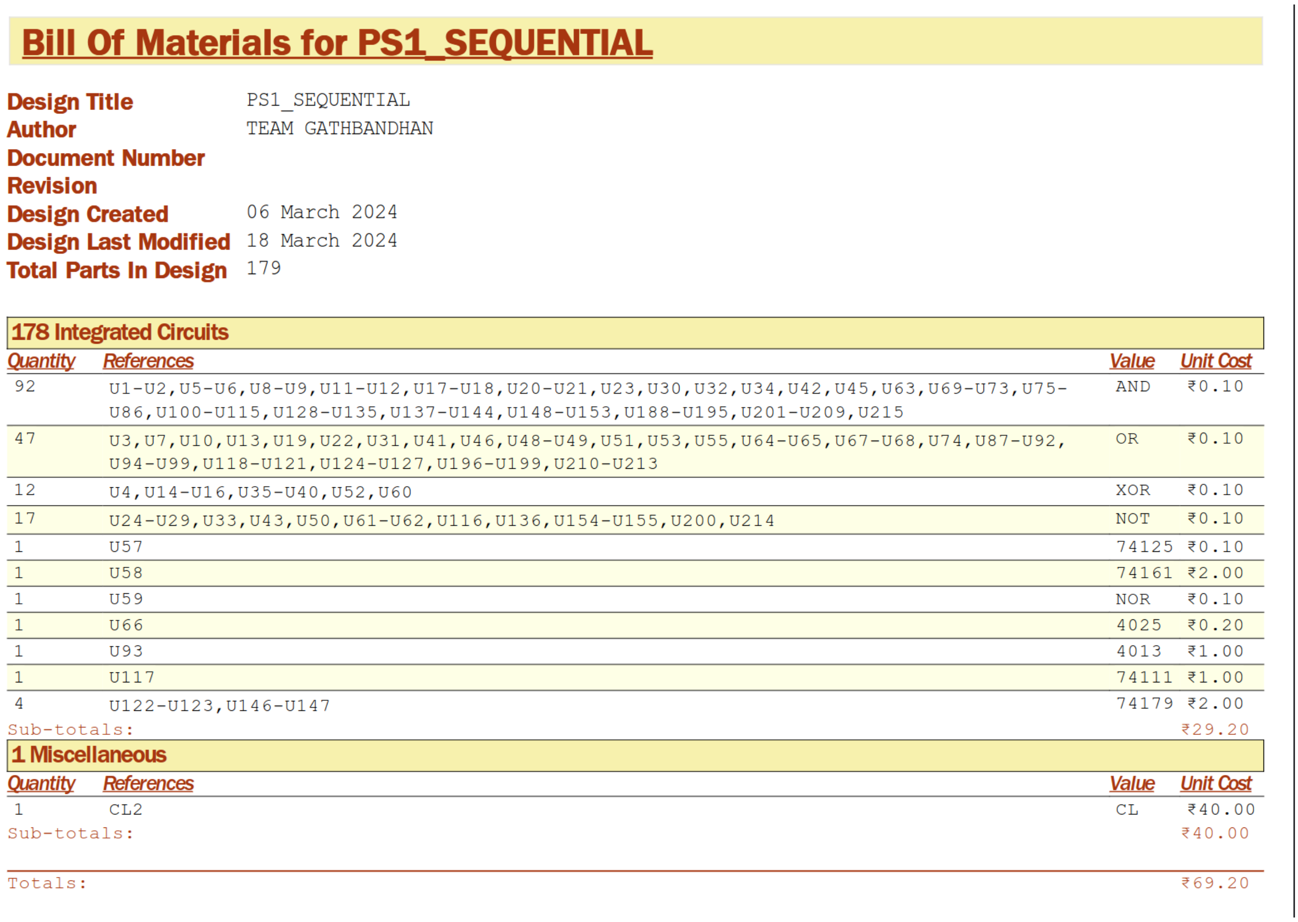
In addition to this, the following changes are also made to implement decryption :

MUX_A AND MUX_B

Here, a new Decryption half is added, with the help of another mux-like design using the **DEC/ENC'** switch.
In the Decryption half, the input is shifted twice except for the third round. Here, the input is right-shifted by 1 bit.
Lastly, the outputs are OR'ed and then fed into **MERGE**, which remains unchanged.



BILL OF MATERIALS FOR PART 2 [SEQUENTIAL]



Bill Of Materials for PS1_SEQUENTIAL

Design Title	PS1_SEQUENTIAL
Author	TEAM GATHBANDHAN
Document Number	
Revision	
Design Created	06 March 2024
Design Last Modified	18 March 2024
Total Parts In Design	179

178 Integrated Circuits

Quantity	References	Value	Unit Cost
92	U1-U2,U5-U6,U8-U9,U11-U12,U17-U18,U20-U21,U23,U30,U32,U34,U42,U45,U63,U69-U73,U75-U86,U100-U115,U128-U135,U137-U144,U148-U153,U188-U195,U201-U209,U215	AND	₹0.10
47	U3,U7,U10,U13,U19,U22,U31,U41,U46,U48-U49,U51,U53,U55,U64-U65,U67-U68,U74,U87-U92,U94-U99,U118-U121,U124-U127,U196-U199,U210-U213	OR	₹0.10
12	U4,U14-U16,U35-U40,U52,U60	XOR	₹0.10
17	U24-U29,U33,U43,U50,U61-U62,U116,U136,U154-U155,U200,U214	NOT	₹0.10
1	U57	74125	₹0.10
1	U58	74161	₹2.00
1	U59	NOR	₹0.10
1	U66	4025	₹0.20
1	U93	4013	₹1.00
1	U117	74111	₹1.00
4	U122-U123,U146-U147	74179	₹2.00
Sub-totals:			₹29.20

1 Miscellaneous

Quantity	References	Value	Unit Cost
1	CL2	CL	₹40.00
Sub-totals:			₹40.00

Totals: ₹69.20

TOTAL COST : RS 69.20