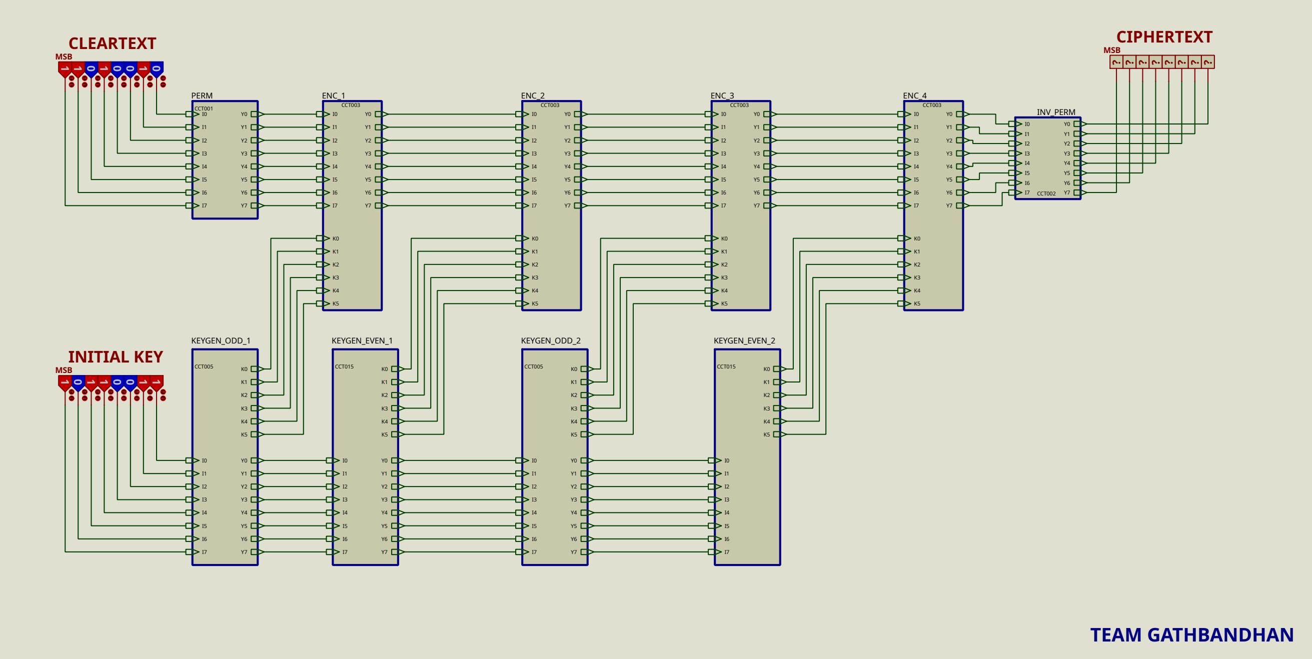
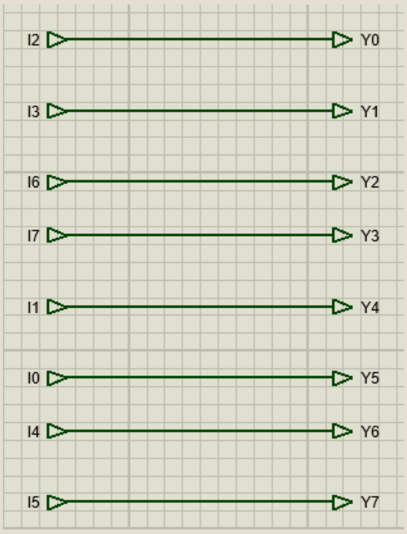
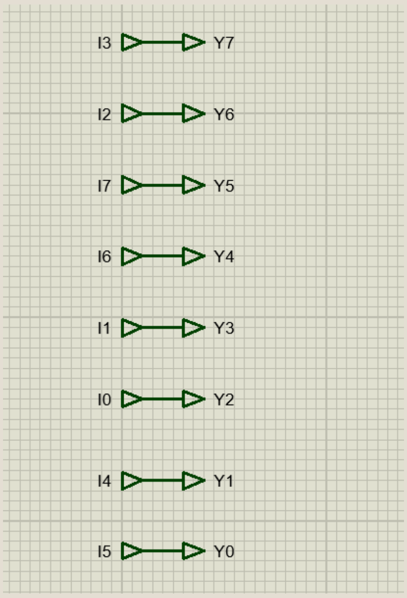
DIGISIM PS1 - COMBINATIONAL ENCRYPTION-ONLY CIRCUIT [PART 1]



This is the Encryption-only Combinational Circuit for DES Algorithm.
We have divided the circuit into several sub-circuits. These are :

PERM and INV_PERM

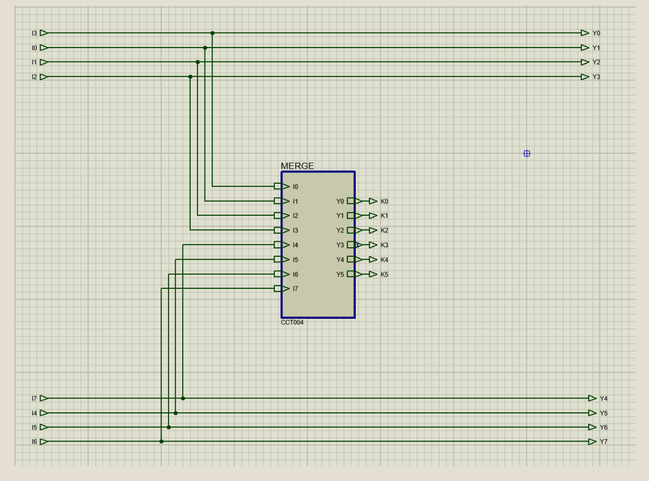
These are the sub circuits for permutations that are carried at the beginning and end of the encryption chain.

 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

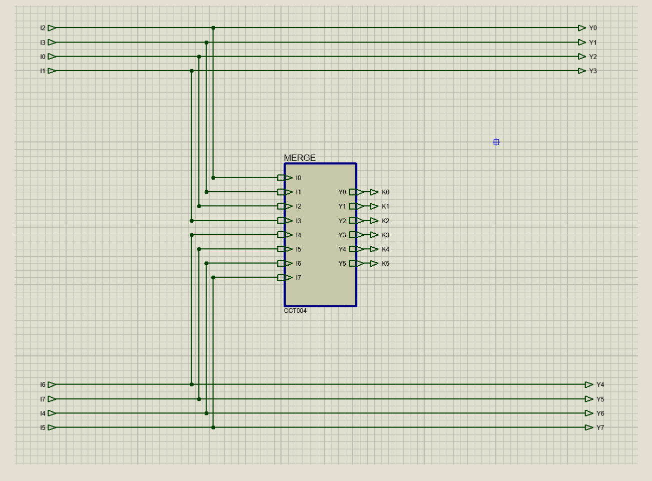
We have implemented these permutations by simply connecting the inputs and outputs in the required order.

KEYGEN

These are sub-circuits for key generation. We have created two different type of sub-circuits for even and odd rounds. The difference is only in the initial shift, which is done by simply taking the inputs in the shifted order.
Every round passes out the shifted bits to the next round and also outputs a key from the MERGE sub-circuit.



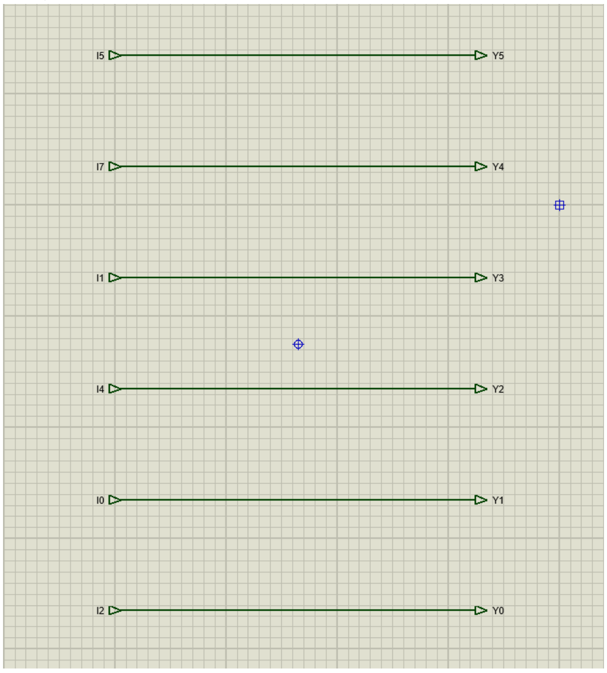
FOR ODD ROUNDS



FOR EVEN ROUNDS

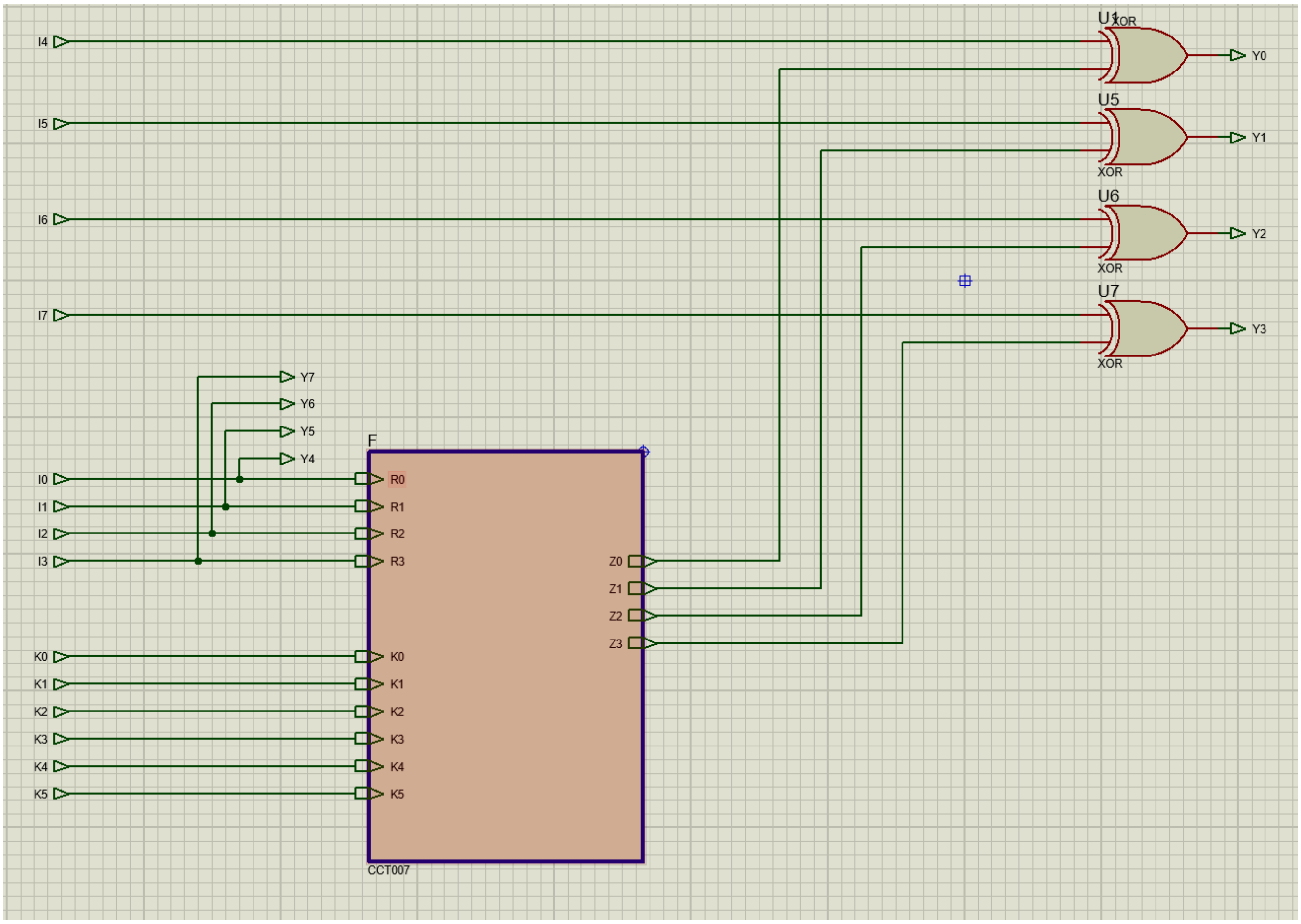
MERGE

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



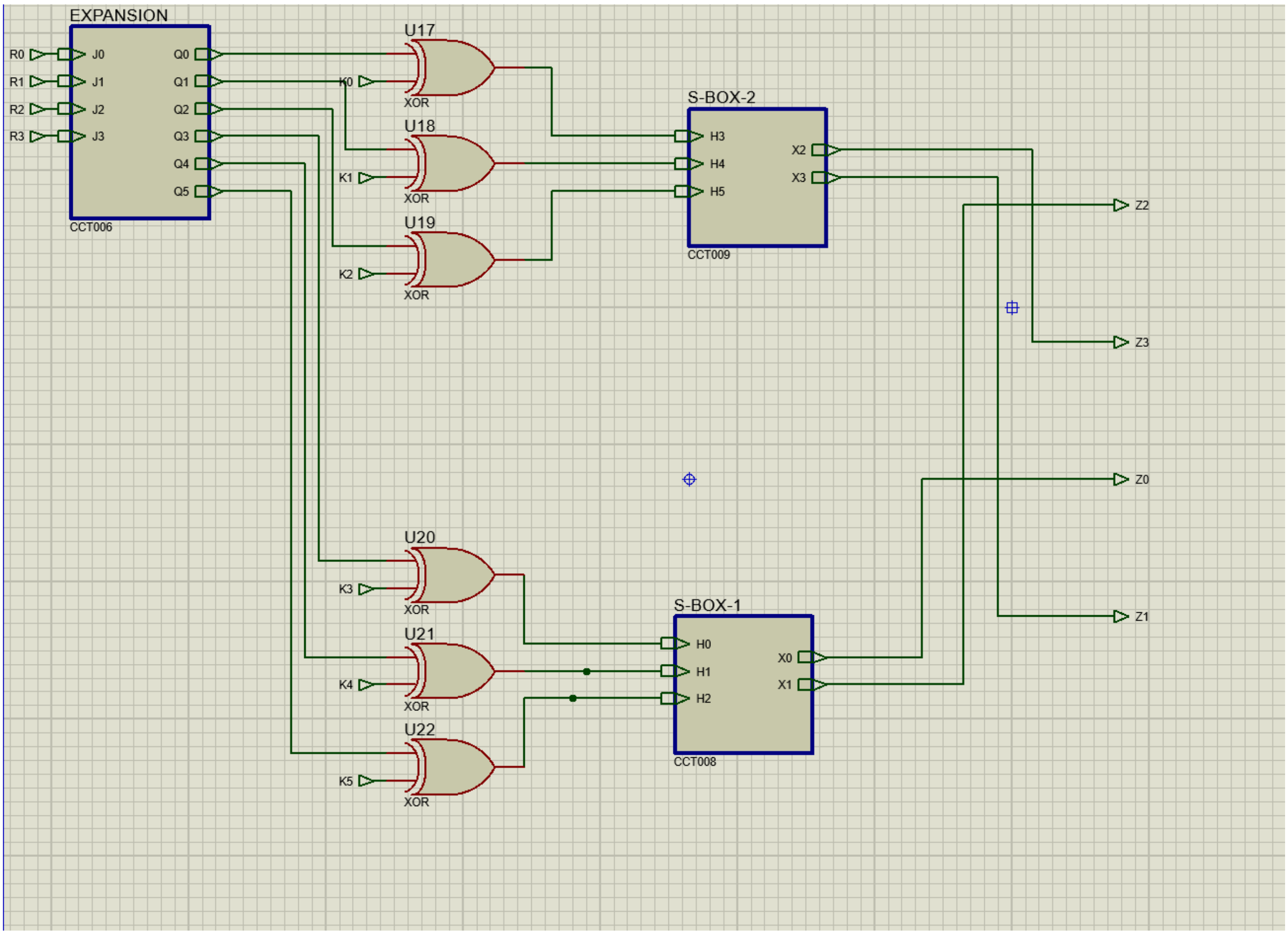
ENC

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.

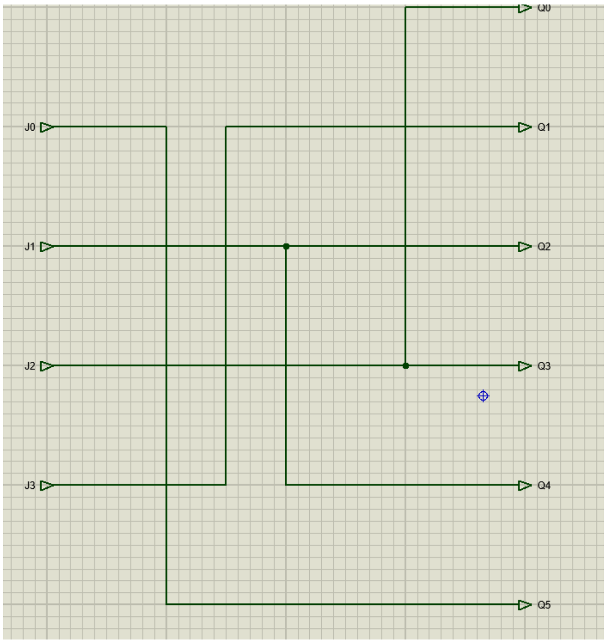


F

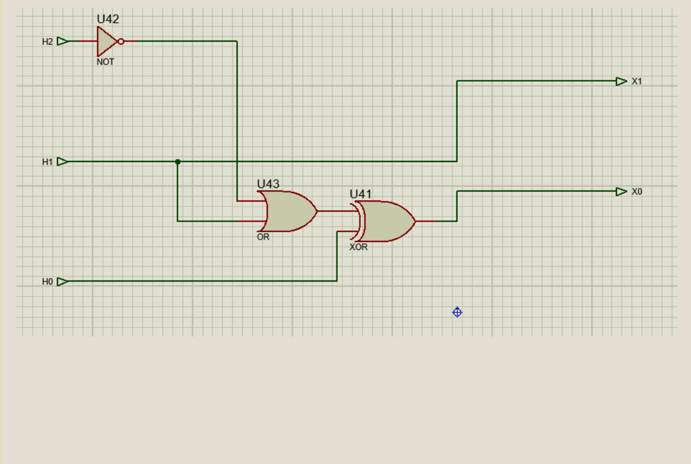
This sub-circuit implements function *"f"*. Here, the input[4-bits] is expanded to 6 bits, which is then bitwise XOR'ed with the round key. The output is then split into halves and then fed into the S-BOXES. The 2-bit outputs are then permuted and outputted.



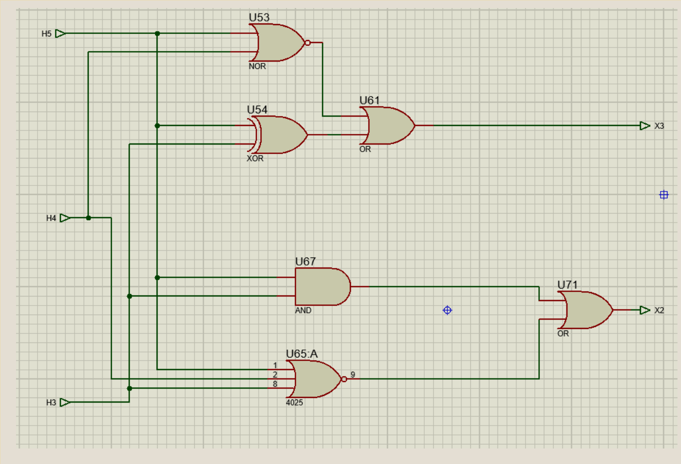
EXPANSION



S-BOXES

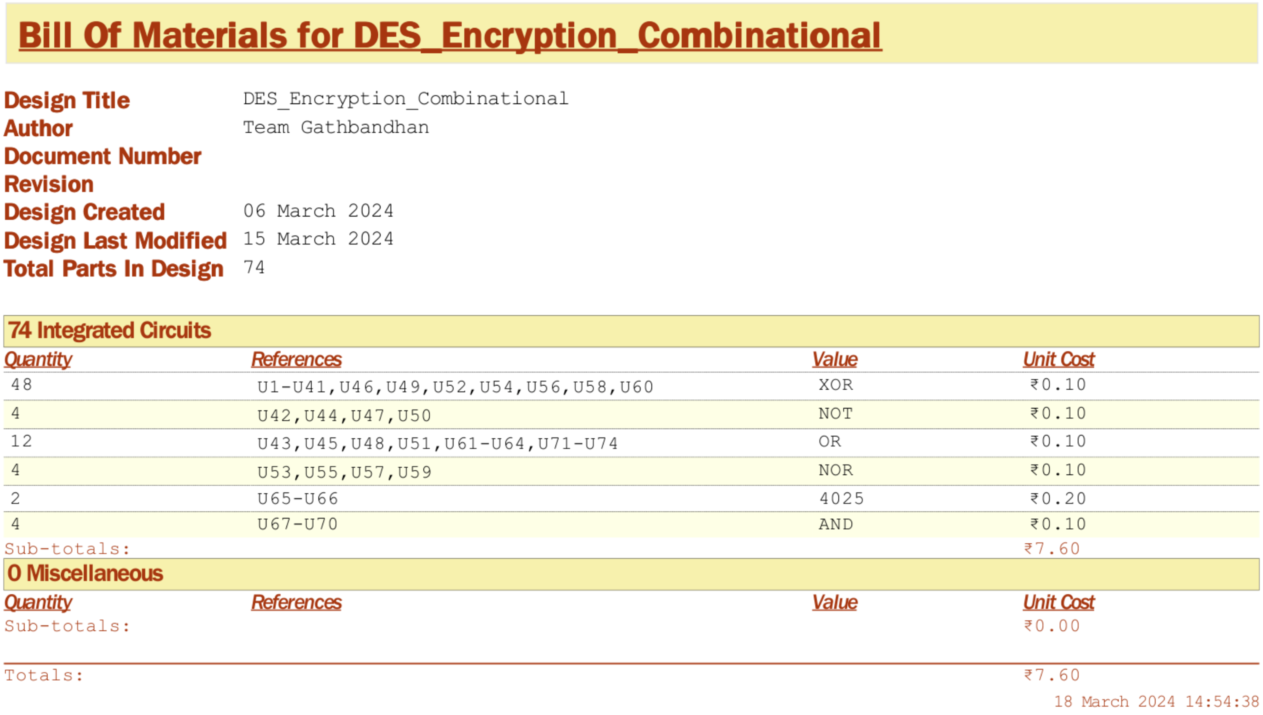


S-BOX-1



S-BOX-2

BILL OF MATERIALS FOR PART 1 [COMBINATIONAL]



Bill Of Materials for DES_Encryption_Combinational

Design Title	DES_Encryption_Combinational
Author	Team Gathbandhan
Document Number	
Revision	
Design Created	06 March 2024
Design Last Modified	15 March 2024
Total Parts In Design	74

74 Integrated Circuits

Quantity	References	Value	Unit Cost
48	U1-U41,U46,U49,U52,U54,U56,U58,U60	XOR	₹0.10
4	U42,U44,U47,U50	NOT	₹0.10
12	U43,U45,U48,U51,U61-U64,U71-U74	OR	₹0.10
4	U53,U55,U57,U59	NOR	₹0.10
2	U65-U66	4025	₹0.20
4	U67-U70	AND	₹0.10
Sub-totals:			₹7.60

0 Miscellaneous

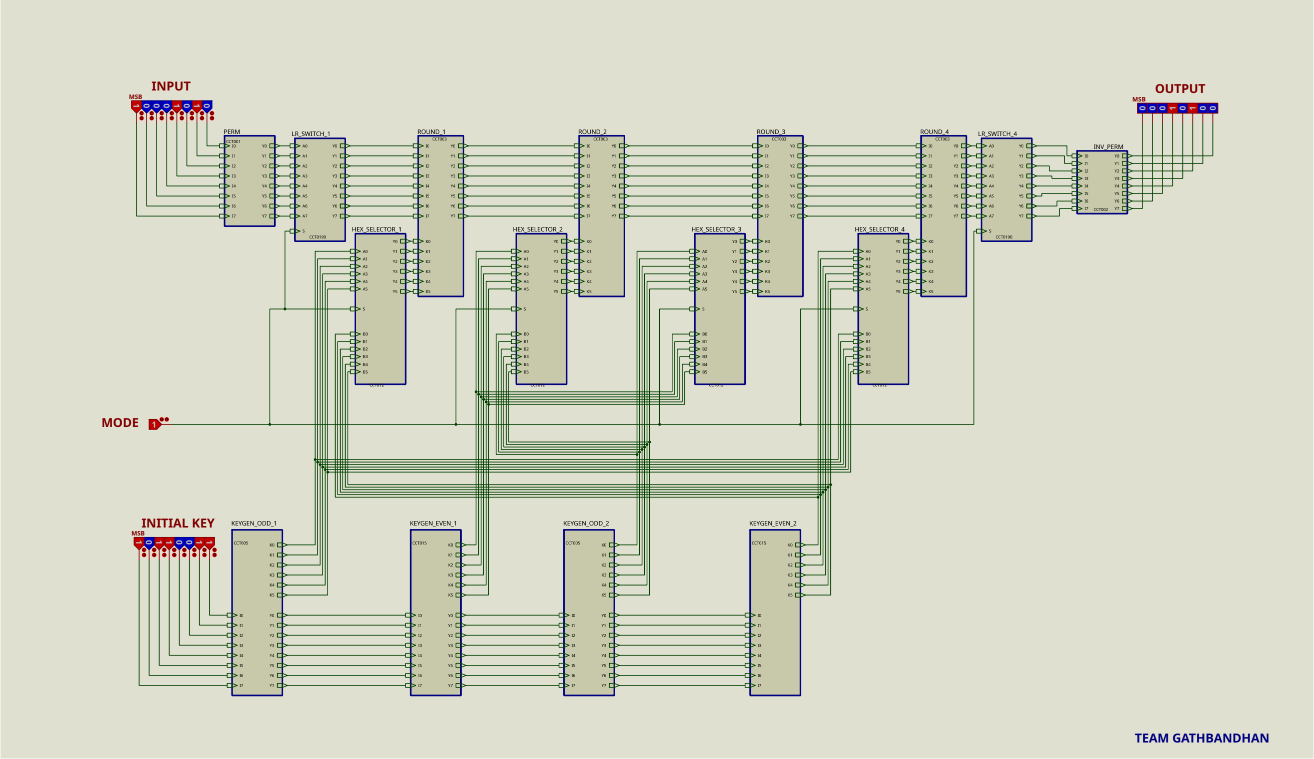
Quantity	References	Value	Unit Cost
Sub-totals:			₹0.00

Totals:			₹7.60

18 March 2024 14:54:38

> **TOTAL COST : RS 7.60**

COMPLETE 4-ROUND DES [COMBINATIONAL]



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 **MODE** button from 0 to 1.

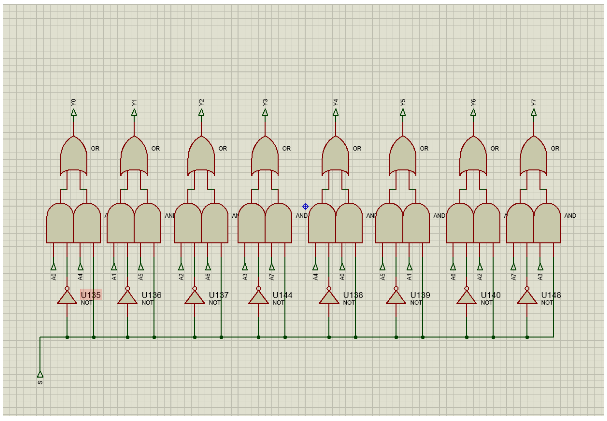
Logically, it differs from the encryption-only circuit in two ways:

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:

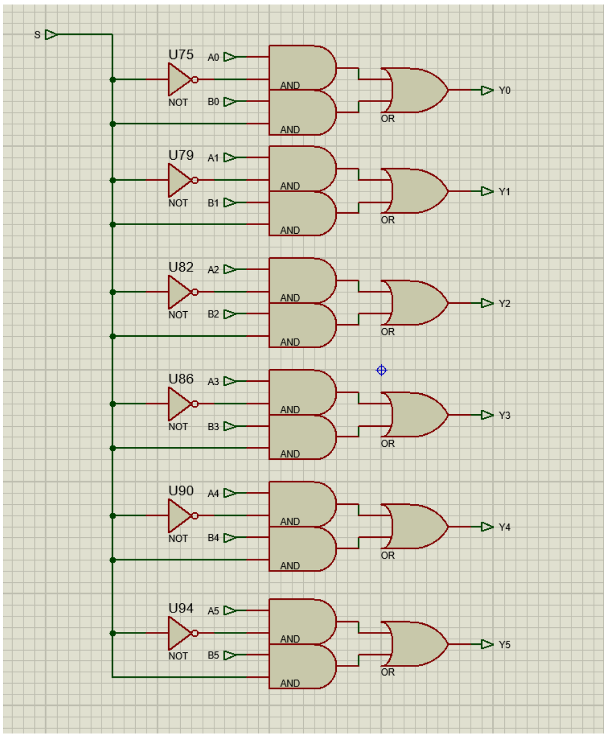
1. LR_SWITCH

This is a simple sub-circuit that switched the left and right halves when MODE is HIGH.

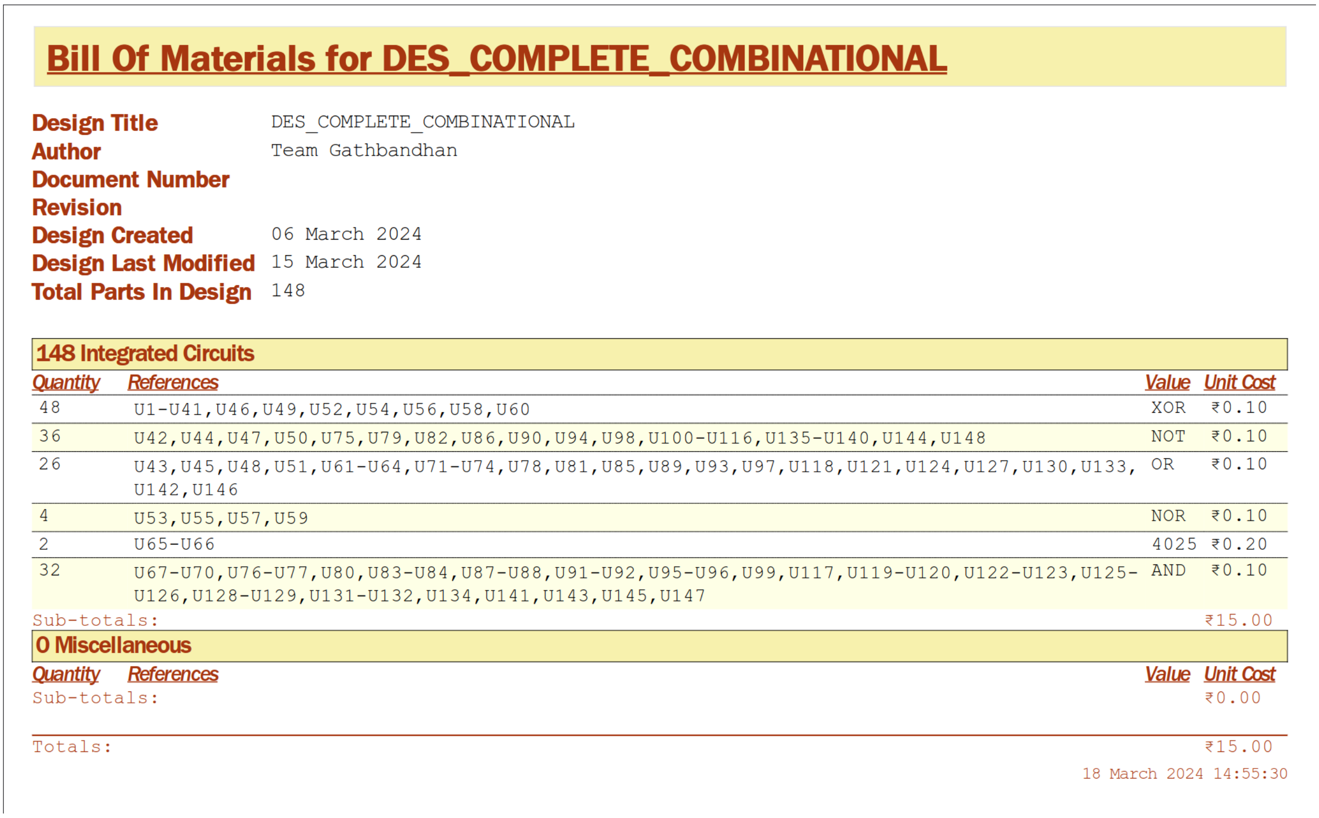


2. HEX_SELECTOR

This subcircuits switches between the normal round-key order and the reverse order if MODE is set to HIGH.



BILL OF MATERIALS FOR PART 2 [COMBINATIONAL]



Bill Of Materials for DES_COMPLETE_COMBINATIONAL

Design Title	DES_COMPLETE_COMBINATIONAL
Author	Team Gathbandhan
Document Number	
Revision	
Design Created	06 March 2024
Design Last Modified	15 March 2024
Total Parts In Design	148

148 Integrated Circuits

Quantity	References	Value	Unit Cost
48	U1-U41,U46,U49,U52,U54,U56,U58,U60	XOR	₹0.10
36	U42,U44,U47,U50,U75,U79,U82,U86,U90,U94,U98,U100-U116,U135-U140,U144,U148	NOT	₹0.10
26	U43,U45,U48,U51,U61-U64,U71-U74,U78,U81,U85,U89,U93,U97,U118,U121,U124,U127,U130,U133,U142,U146	OR	₹0.10
4	U53,U55,U57,U59	NOR	₹0.10
2	U65-U66	4025	₹0.20
32	U67-U70,U76-U77,U80,U83-U84,U87-U88,U91-U92,U95-U96,U99,U117,U119-U120,U122-U123,U125-U126,U128-U129,U131-U132,U134,U141,U143,U145,U147	AND	₹0.10
Sub-totals:			₹15.00

0 Miscellaneous

Quantity	References	Value	Unit Cost
Sub-totals:			₹0.00

Totals: ₹15.00

18 March 2024 14:55:30

TOTAL COST : RS 15.00