DIGISIM PS-1

Team Name: The Hawks

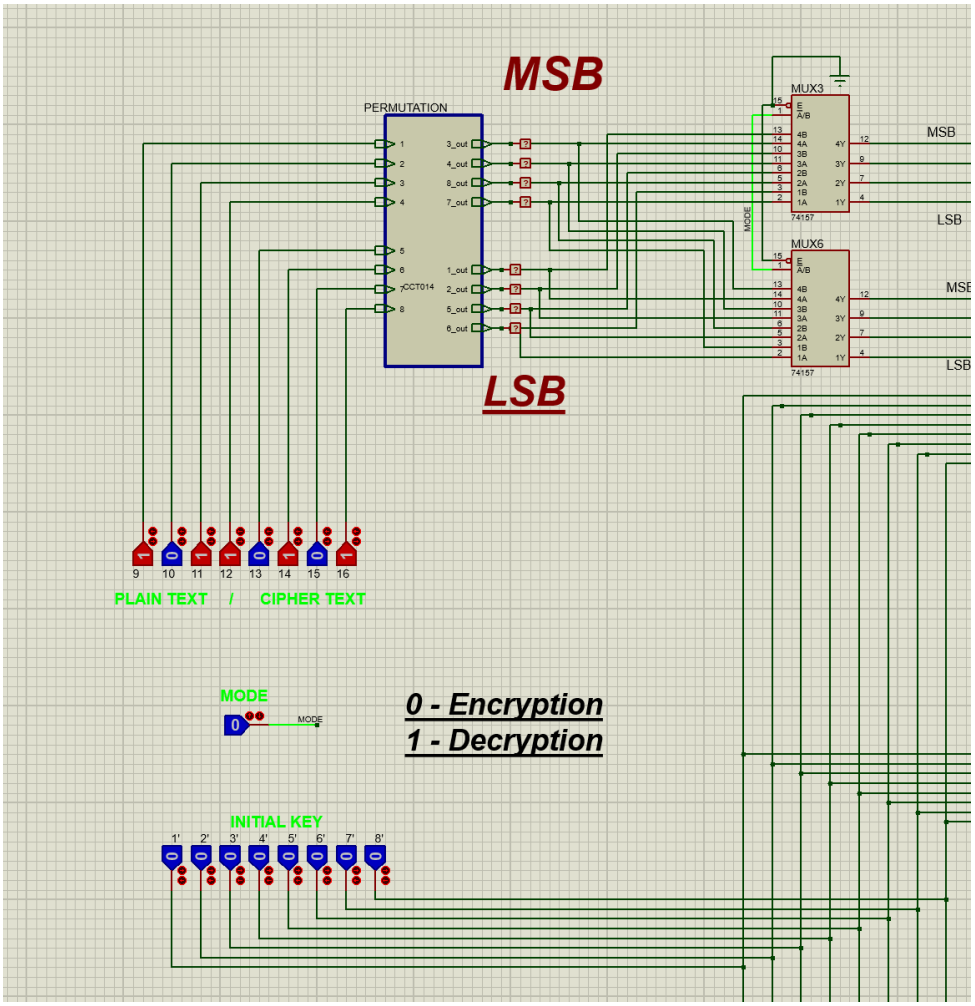
Combinational Circuit:

Part 2 (Encryption/Decryption): **Total Cost = 8.4 + 64 (for the 8 8x4 MUX being used).**

Circuit is same as part 1 except:

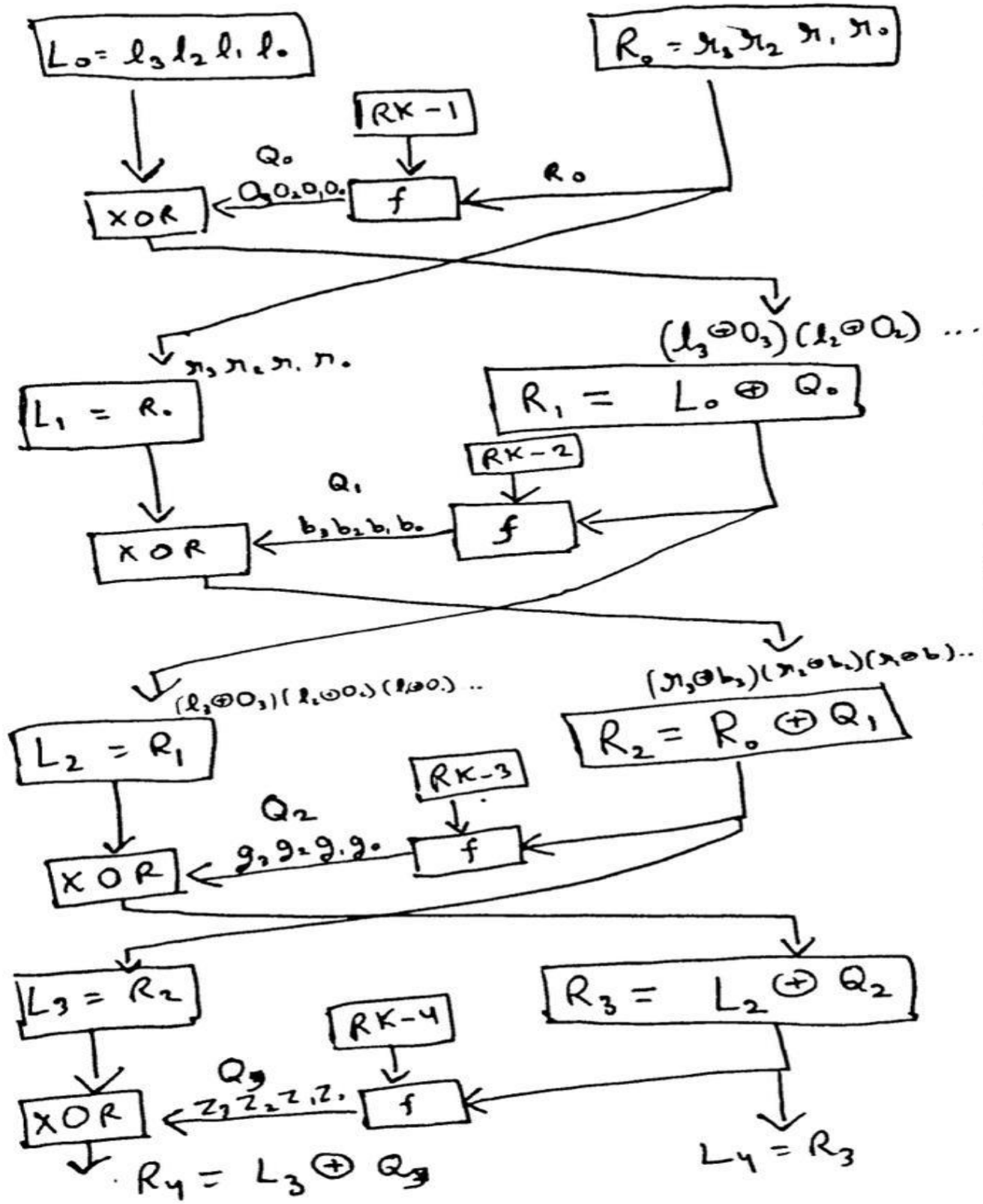
1. Mux is used after permutation to take inputs for the 2 modes (Swaps L0 with R0 in case of Decryption and remains unchanged in case of Encryption).
2. Similarly, a MUX is also used before inverse permutation.
3. A MUX is also being used to generate the round keys (i.e. swaps R4 with R1 and R2 with R3 in case of decryption).

The reason for the swapping of round keys is given as follows:



How Decryption works.

Let $L_0 = l_3 l_2 l_1 l_0$, $R_0 = r_3 r_2 r_1 r_0$



$L_4 = R_3 = L_2 \oplus Q_2 = L_0 \oplus Q_0 \oplus Q_2$

$R_4 = L_3 \oplus Q_3 = R_0 \oplus Q_1 \oplus Q_3$

$\therefore$ O/P of Encryption =

$\{L_4, R_4\}$

Note :- To ~~Decry~~ Decrypt

We use $A \oplus B = C$

then $A \oplus C = B$

Now If $L_4 = L_0 \oplus Q_0 \oplus Q_2$

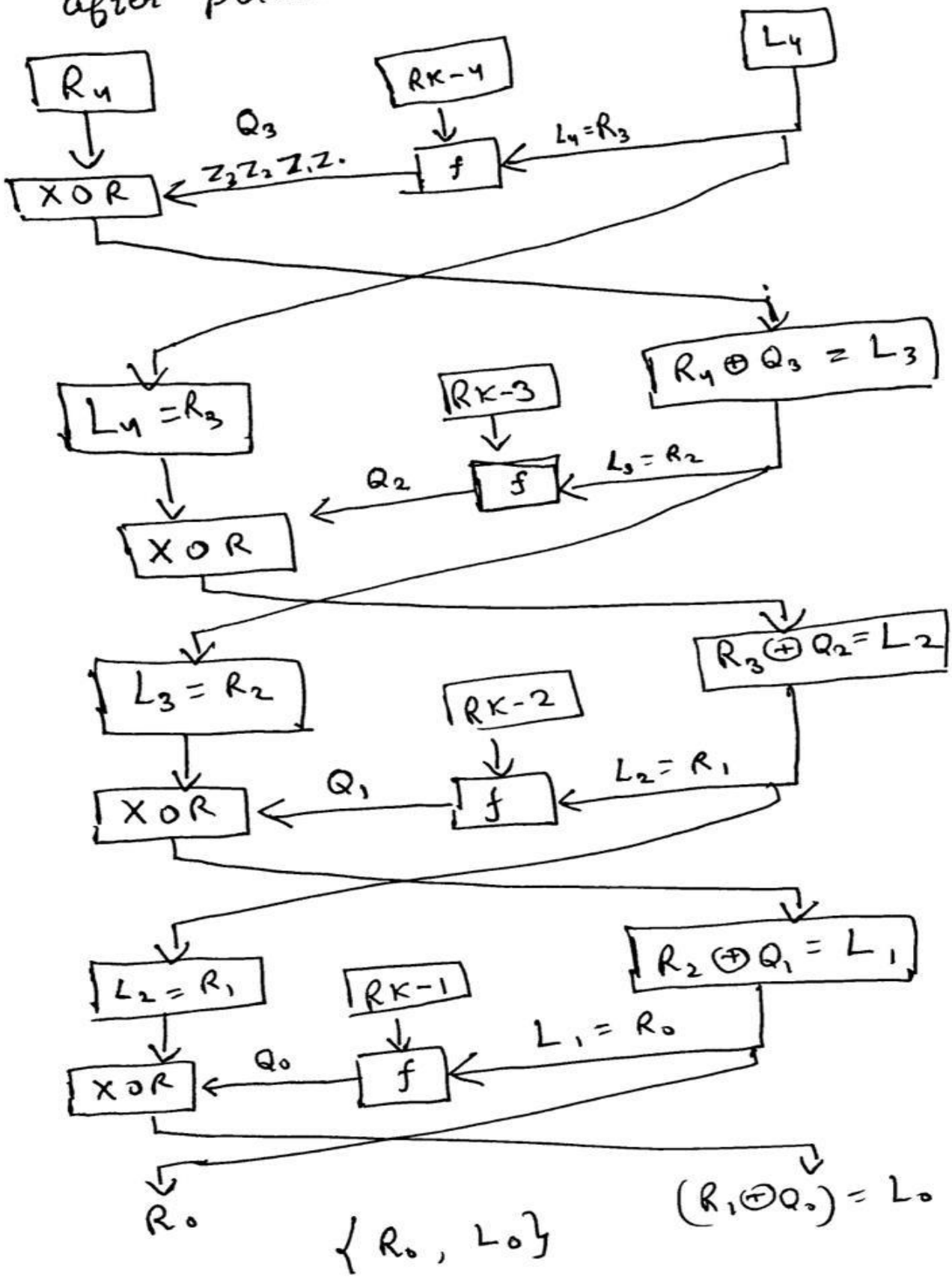
$L_0 = L_4 \oplus Q_0 \oplus Q_2$

and

$R_4 = R_0 \oplus Q_1 \oplus Q_3$

$R_0 = R_4 \oplus Q_1 \oplus Q_3$

If we give {R_4, L_4}
after permutation



$\{R_0, L_0\}$