**Class Activity # 04**

**Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **Roll Number: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Question # 01:**

Find Cipher text for the first 2 rounds of DES in Output Feedback Mode (Stream Size=1 byte). After receiving L2R2 reverse their order and apply inverse permutation.

Note: Make the necessary assumptions and state them clearly. Also specify any vectors used.

Key: 00111010 01010101 11100001 00111100 10100000 00011110 10111111 00001011

Plain Text: 11010000 11110000 10101010 11001010 11100001 10111101 10101111 11110010