Indian Institute of Technology Jodhpur
Computer Science and Engineering Department

Lab 3

CSL6010 - Cyber Security

Date: 23-02-2023 **Marks: 10**

Part1 [4 marks]:
Use DES and AES with modes like ECB, CBC, CFB, and OFB provided in Symmetric block ciphers to Encrypt and Decrypt a Message. The Key used for encryption and decryption will be your roll number + first name (if the length is insufficient, pad the key with 0's).
Key Example: B22CS007CHIRAG00

Part2 [4 marks]:
Perform Diffie-Hellman key exchange between a client and server to share a secret key. Using this secret key, encrypt the message at the server side and send it to the client. Decrypt the message at client side using the same key.

Part3 [2 marks] - Image Encryption Decryption:
Perform Encryption and Decryption of the provided Image using any two modes of AES. Also compare the encrypted image in both the cases (anytype of comparison will suffice).

Library Allowed: You can use the **pycryptodome** library for all encryption algorithms and the **skimage** library for any image processing task. You can also use any other library as per your choice.

Submission Guidelines: Submit a report containing the codes and outputs in the same file in pdf format. For part 3 mention the finding of the comparison.