International Institute of Information Technology Hyderabad

System and Network Security (CS5470)

Lab Assignment 1:
Design of an end to end messaging system like WhatsApp

Deadline: January 25, 2021 (Monday), 23:59 PM
Total Marks: 100

Note:- *It is strongly recommended that no student is allowed to copy programs from others. No assignment will be taken after deadline. Name your program as rollnos_assign_1.ext. Upload your only rollnos_assign_1.ext file along with a README file in a zip file (groupno_rollnos_assign_1.zip) to course portal (moodle).* ***You are allowed to use any programming language implementation (for example, C, C++, Java, Python).***

Problem Description

Your task will be to design an end to end messaging system like WhatsApp with the below functionalities:

- Multiclient chat application that has a server component and 4 clients [atleast].
- The system should support the signup and sign in feature. [error message with wrong credentials].
- User can send message to other user [p2p message] [SEND command] [<SEND> <USERNAME> <MESSAGE>]
- Each user can join multiple chat rooms (groups) at a time.
- Each user can list all the groups. [LIST Command] [show all group and number of participants in each group]
- Each user can join a group [JOIN command]. If the group does not exist then the first create it then joins it.
- Each user can create a group [CREATE command].
- If one user sends a message to a group it should be sent to all members of that group.

- The message is encrypted using Tripple DES (3DES) and the key will be Diffie–Hellman key type exchanged between clients.
- For each group make one key (random nonce).
- Message can be any type, for example, text, images, video, and audio.

Note: The one time Diffie–Hellman type key must be include a prive key (for instance roll nos.).

All the best!!!