tcg crest
Inventing Harmonious Future

Institute for Advancing Intelligence, TCG CREST
(TCG Centres for Research and Education in Science and Technology)

Introduction to Computer Programming and Data Structures
Project

Maximum Marks: **100** Submission Deadline: **2022-Dec-15**
Topic: End-to-end encrypted conversation

Project problem # PP0001
Currently, we use WhatsApp, signal, etc. app for conversation. They claim they use end-to-end encryption that can be decrypted only when the user agrees to do so. However, frequently we see that the messages sent through these communication apps are revealed publicly by some hackers. Sometimes, the apps company itself sells the communication data in raw form. Since the source codes of these apps are not available publicly, we can not trust them.

However, using the app like wire, may solve the problem as this is with an open source with its code available on GitHub. However, wire like apps are not popular.

So, *we are interested in designing a system so that we can use most popular apps still keeping the messages secret*. The system should have the following properties.

- We will use any one of the popular apps like, WhatsApp, messenger, google chat, signal, etc., for communication. Best suitable should be found by proper investigation.
- Before sending the message the messages must be encrypted. We can use AES, or any other stream cipher, for the same.
- In the beginning, when two users agree to communicate, they must agree on some common key. This common key can be established using any key-agreement protocol.
- The receiver should be able to decrypt the message.
- For now, we only consider the text messages.

Why popular app, instead of designing our own?

- Sending a message from a sender to a receiver, some kind of network. If there is no cloud server, the sender and receiver must be online all the time for communication. A cloud server can temporarily hold the message until it can deliver the message to the receiver. So, we must require a cloud server.
- If we use some free cloud server, we may have to build communication codes by our own which is a time-consuming process.
- Using any popular app can save our time.

[100]