SENG 360 Assignment 3 - Cryptography

To be carried out in groups of 2-3 students.

Objective

Implement secure Instant Messaging (IM) between a client and a server program.

Details

IM software offers real-time text transmission over the network. Short messages are typically transmitted bi-directionally between two parties. To simplify this assignment, we only consider messaging between two parties: a *server* and a *client*. The server is supposed to be always up and running. At any time, the client can initiate an IM session by sending an “open session” message. After establishing the session, the client and server will be communicating by exchanging text messages.

Before a session is established, the communicating parties (client and server) select (through a GUI or a text interface) the security properties they require for their communication. The list of selectable security properties should include:

1. **Confidentiality**: Encrypting messages sent from the client to the server and vice versa
2. **Integrity**: Checking integrity of the messages coming from client to the server and vice versa, such that no one in the middle can change or add some blocks to the exchanged messages
3. **Authentication**: Authenticating the origin of the messages coming from client or server in a way to make sure that messages have actually been sent by that party.

If the client attempts to open a new session while the security properties selected in client and server are not the same, the session should be rejected with an appropriate error message.

Please use Java and the Java Cryptographic Architecture for implementing your program. You can fine documentation here:
http://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html

Deliverable

Submit one single zip file (no other archiver allowed) to Coursespaces by Nov. 9, 2017, containing the following:

1. A directory containing all source files
2. Your compiled program
3. A documentation file (PDF) describing technical details of your program, how to compile it, and how to use it (provide screen shots of a sample use of your program).