ANDROID JABBER APPLICATION

By: Praneeth Manubolu

Objective – To create an android based chatting(jabber) application which encrypts and authenticates data using AES and SHA-256, Where initially AES key is encrypted using RSA.

Description - This project aims to create an android chat application where users can communicate with others users through the app using text. The app connects to a java server which handles connections between multiple users. The java server is built using open source Apache MINA project which handles socket connects.

Android APP - The application lets users to add others through an ID. Once added the new user is shown in the friend's tab. The friends tab holds all the available users online or offline. On selecting any one of the friends shown in this tab opens a new screen which has options to send new text messages and see previous messages.

The app scope is only for that instance, closing the application will erase text message data but the friends list will still stay intact if the server is available.

RSA public and private keys and AES keys are generated on starting the application. Public key and AES keys are stored in the Java server. When a text message is sent to other users, senders public RSA key and AES keys are sent to the receiver for the first time. The message hashed and encrypted using AES. This is used to verify the integrity of the message there by validation the message.

Java Server – MINA project helps in maintaining socket session with the android application. Code is written to store and communicate data between different android applications. Stored data includes Keys and friends list.