Names: Ali Jalil, Joshua Egwaikhide, Nick Chalardsoontornvatee

The sequence diagram for the Encrypted Messaging App shows how two users (User1 and User2) and a server interact securely, covering stuff like authentication, message encryption, and keeping everything in sync. It starts with both users sending "Verify Credentials" requests to the server. The server checks these credentials and sends back either a success or failure message - only letting authenticated users move forward with messaging.

After getting authenticated, User1 writes and encrypts a message right on their device to keep it private. They send this encrypted message to the server, which just acts like a middle-man, passing the encrypted message to User2 without ever decrypting it. When User2 gets the message, they decrypt it on their own device to read it, keeping that end-to-end encryption going throughout the whole exchange.

User2 can then hit back with a reply by encrypting their message on their device and sending it back to User1 through the server, which again just passes it along without seeing what's inside. User1 decrypts the reply when they get it, keeping the whole conversation private.

The last part of the diagram shows what happens when someone logs in on a new device. After logging in, they ask the server to sync up their recent messages so they can jump right back into conversations. The server delivers these messages while keeping everything secure since all the decryption happens right on the user's device - showing how serious the app is about privacy.