Names: Ali Jalil, Joshua Egwaikhide, Nick Chalardsoontornvatee

The sequence diagram for the Encrypted Messaging App illustrates secure interactions between two users (User1 and User2) and a server, covering key elements like authentication, message encryption. The process begins with both users entering "Verify Server Address" requests to the server, which validates these credentials and sends back either a success or failure response, allowing only authenticated users to proceed with messaging.

Once authenticated, User1 composes a message that is encrypted on their device before being sent, ensuring protection against unauthorized access during transmission. This encrypted message is then sent to the server, which acts as a relay, forwarding the encrypted message to User2 without decrypting it, thus preserving confidentiality until it reaches the intended recipient. When User2 receives the message, it is decrypted to be able to read it, maintaining end-to-end encryption throughout the communication process.

User2 can respond by sending their reply on their device and sending it back to User1 via the server, which again simply relays the encrypted message without exposing its contents. User1 decrypts the response upon receipt, keeping the entire conversation private and secure.

The final section of the diagram addresses scenarios where a user logs in on a new device or a message is sent to an offline user. After logging in, the user requests the server to synchronize recent messages, allowing them to seamlessly resume conversations. The server delivers these messages securely, with decryption happening solely on the user’s device, highlighting the app’s commitment to privacy.