**Security Analysis**

**Findings**

Our project provided several critical insights through the mechanism we have implemented. The end-to-end encryption ensures that messages are protected, significantly enhancing data confidentiality. The use of public-private key pairs, with additional layer of security being added by encrypting the private key using the user’s password. Diffie-Hellman Key Exchange facilitates a secure method of deriving symmetric keys, and AES encryption ensures strong protection for message data. The password reset functionality was successfully implemented, allowing users to securely change their passwords while maintaining access to their private keys and previously encrypted messages.

Nevertheless, a constraint was found in the execution of the "forgot password" feature. If the user forgets their password, the system will be unable to decrypt the private key since it is encrypted with the password. If you can't access the original password, the private key is also out of reach, making it impossible to decrypt messages encrypted before. This limitation results in a fundamental trade-off between robust security and ease of account recovery. As a result, this functionality could not be implemented without compromising the integrity of private key encryption or introducing a complex recovery mechanism. This finding underscores the importance of informing users about potential data loss in the event of password loss.

**Results**

Firebase Authentication provided robust user validation, ensuring secure access to accounts. Database interactions demonstrated that encrypted messages remain secure during both storage and retrieval. However, the lack of a "forgot password" mechanism means that users who lose their passwords risk losing access to their encrypted messages permanently.

**Lessons Learned**

The implementation of private key encryption with user passwords provides strong protection against unauthorized access but introduces challenges in account recovery i.e. forgot password functionality. A critical lesson learned is the trade-off between security and usability. In order to implement recovery mechanisms, we could use secure recovery key or multi-layer encryption, to allow password recovery without compromising private key integrity. Another lesson is the importance of user education, ensuring that users understand the risks associated with losing their passwords.