Design 1: Basic Structure

- **Introduction**
  - 1.1 Purpose: This document outlines the requirements for a secure messaging application.
  - 1.2 Scope: This SRS covers the core functionality: user authentication, message encryption/decryption, and secure storage.
  - 1.3 Intended Audience: This document is for Olivia Sabb (developer) and potential testers/users.
  - 1.4 Definitions and Acronyms:
    - AES: Advanced Encryption Standard
    - RSA: Rivest-Shamir-Adleman
    - SRS: Software Requirements Specification
- **Overall Description**
  - 2.1 Product Perspective: This is a standalone application designed to provide secure messaging. It does not directly integrate with other systems.
  - 2.2 User Needs: Users need a way to send and receive messages with strong privacy and security guarantees. Existing solutions are inadequate due to potential surveillance and data breaches.
  - 2.3 Assumptions and Dependencies:
    - The user has a basic understanding of security concepts.
    - Cryptography libraries are readily available and reliable.
- **Specific Requirements**
  - 3.1 Functional Requirements:
    - FR1: The system shall allow users to register with a unique username, email, and password.
    - FR2: The system shall authenticate users using hashed and salted passwords (bcrypt/argon2).
    - FR3: The system shall allow users to send encrypted messages using AES or RSA.
    - FR4: The system shall allow users to receive and decrypt messages.
    - FR5: The system shall provide an inbox and outbox for each user.
  - 3.2 Non-Functional Requirements:
    - NFR1: The system shall deliver messages with a latency of less than 0.5 seconds.
    - NFR2: The system shall protect against common web vulnerabilities.
    - NFR3: The system shall have a clean and intuitive user interface.
- **Appendices**
  - Use Cases:
    - Registering a new user
    - Logging in
    - Sending a message
    - Receiving a message