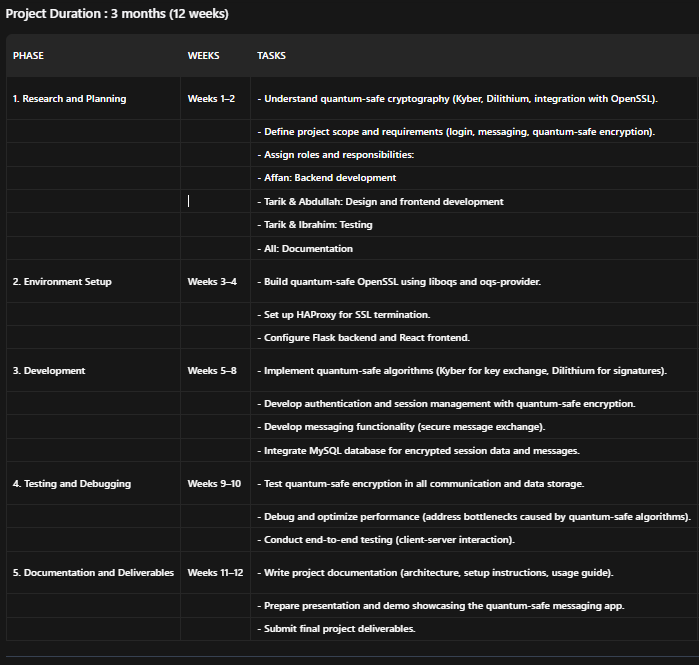
**Quantum-safe-messaging web app Graduation Project**

*Gantt Chart*

****

**Explanation of the Gantt Chart**

**1. Research and Planning (Weeks 1–2)**

* Understand Quantum-Safe Cryptography :
  + Study quantum-safe algorithms like Kyber (key encapsulation mechanism) and Dilithium (digital signature algorithm) and how they integrate with OpenSSL.
  + Explore the Open Quantum Safe (OQS) project’s tools and libraries (liboqs, oqs-provider).
* Define Project Scope and Requirements :
  + Clearly outline the features of the messaging app, such as user authentication, secure messaging, and quantum-safe encryption.
  + Identify the technologies to be used (Flask, React, MySQL, HAProxy, OpenSSL with quantum-safe algorithms).
* Assign Roles and Responsibilities :
  + Affan : Backend development (Flask API, session management, database integration).
  + Tarik & Abdullah : Design and frontend development (React UI, user experience).
  + Tarik & Ibrahim : Testing (unit tests, integration tests, performance optimization).
  + All : Collaborate on documentation.

**2. Environment Setup (Weeks 3–4)**

* Build Quantum-Safe OpenSSL :
  + Follow the tutorial to build OpenSSL with quantum-safe algorithms using **liboqs** and **oqs-provider**.
  + Ensure the environment is configured correctly for quantum-safe encryption.
* Set Up HAProxy :
  + Configure HAProxy for SSL termination to handle secure connections.
  + Remove Apache HTTPD from the setup since it will not be used.
* Configure Flask Backend and React Frontend :
  + Affan sets up the Flask backend to handle APIs for authentication, session management, and messaging.
  + Tarik and Abdullah set up the React frontend for the user interface.

**3. Development (Weeks 5–8)**

* Implement Quantum-Safe Algorithms :
  + Use Kyber for key exchange and Dilithium for digital signatures in session management and database encryption.
  + Ensure all cryptographic operations are quantum-safe.
* Authentication and Session Management :
  + Affan develops the authentication system with session-based login using quantum-safe encryption.
  + Encrypted session data is stored securely in the MySQL database.
* Messaging Functionality :
  + Develop secure messaging functionality where messages are encrypted using quantum-safe algorithms.
  + Affan handles the backend logic, while Tarik and Abdullah work on the frontend UI for sending and receiving messages.
* Integrate MySQL Database :
  + Store encrypted session data and messages in a MySQL database.
  + Affan ensures the database schema supports quantum-safe encryption.

**4. Testing and Debugging (Weeks 9–10)**

* Test Quantum-Safe Encryption :
  + Verify that all communication (e.g., login, messaging) and data storage use quantum-safe algorithms.
  + Tarik and Ibrahim ensure that the encryption and decryption processes work seamlessly.
* Debug and Optimize Performance :
  + Address any performance bottlenecks introduced by quantum-safe algorithms (e.g., increased computation time).
  + Optimize the application for better speed and efficiency.
* End-to-End Testing :
  + Conduct comprehensive testing to ensure the entire system works seamlessly from client to server.
  + Validate that the application meets all functional and security requirements.

**5. Documentation and Final Deliverables (Weeks 11–12)**

* Write Project Documentation :
  + Document the architecture, setup instructions, and usage guide for the quantum-safe messaging app.
  + Include details about the technologies used, implementation steps, and troubleshooting tips.
* Prepare Presentation and Demo :
  + Create slides and a live demo showcasing the quantum-safe messaging app.
  + Highlight the key features, challenges overcome, and future improvements.
* Submit Final Project :
  + Deliver the completed project by the deadline, ensuring all components (code, documentation, presentation) are polished and ready.