🔨 **Atividades a serem implementadas**

1️⃣ Cadastro e Autenticação de Usuários

- Criar um sistema de **cadastro** onde os usuários possam registrar login e senha.
- Armazenar a senha de forma **segura** usando **bcrypt** com **sal aleatório**.
- Criar um **método de login** que:
    - Receba login e senha do usuário.
    - Compare a senha inserida com o **hash armazenado**.
    - Se a senha for correta, gere um **Token JWT** de acesso ao sistema.

✅ **Critérios:**
✓ Senhas nunca podem ser armazenadas em **texto plano**.
✓ A senha deve ser armazenada usando **bcrypt com sal aleatório**.
✓ O sistema deve emitir um **Token JWT** válido por tempo limitado após o login bem-sucedido.
✓ Usuários autenticados devem apresentar um **Token JWT válido** para acessar funcionalidades protegidas.

2️⃣ Autorização com Tokens JWT

- Criar um **mecanismo de autenticação baseado em JWT**, garantindo que:
    - O usuário só tenha acesso a recursos protegidos se possuir um **Token JWT válido**.
    - O Token JWT contenha **informações seguras do usuário**, como **ID e tempo de expiração**.
    - Tokens expirados sejam rejeitados.

✅ **Critérios:**
✓ O Token JWT deve ser assinado digitalmente pelo servidor.
✓ O sistema deve rejeitar tokens inválidos ou expirados.
✓ Toda solicitação a funcionalidades protegidas deve ser validada via **Token JWT**.

3️⃣ Criptografia Simétrica (AES) para Mensagens

- Implementar um sistema de **criptografia de mensagens** usando **AES (modo CBC)**.
- Cada mensagem enviada deve ser criptografada antes de ser armazenada.
- O usuário só poderá descriptografar mensagens caso tenha a **chave correta**.

✅ **Critérios:**
✓ O **Vetor de Inicialização (IV)** deve ser gerado aleatoriamente para cada criptografia.
✓ A criptografia deve garantir **integridade e confidencialidade**.
✓ A mensagem deve ser criptografada antes de ser armazenada no banco de dados.

4️⃣ Proteção da Chave AES com Criptografia Assimétrica (RSA)

- Cada usuário terá um **par de chaves RSA** (pública e privada).
- A **chave AES** usada para criptografar as mensagens será protegida com **RSA**:
    - A **chave AES será criptografada com a chave pública** do destinatário antes de ser armazenada.
    - O destinatário usará sua **chave privada RSA** para recuperar a **chave AES** e então descriptografar a mensagem.

✅ **Critérios:**

✓ Cada usuário deve possuir um **par de chaves RSA**.

✓ A **chave AES nunca deve ser transmitida em texto plano**.

✓ Somente o destinatário correto poderá descriptografar sua chave AES e acessar a mensagem.