CS Lab Assignment-4

Session: July-Dec, 2025
Duration: ~ 3 weeks

Web Applications

1. Web-App: Secure File Vault

Description: A web-based system to store files in a confidential and integrity protected way.

- Client (user) selects a file.
- Generates a random AES-256 key.
- Calculates the SHA-256 digest of the file
- Encrypts the file content along with its hash-digest with AES-256-GCM.
- Encrypts the AES key using the user's RSA public key.
- Store the following on server:
  - Encrypted file and hash
  - Encrypted AES key
- To decrypt retrieve the content stored on server and then:
  - Decrypt AES key with private RSA key.
  - Use AES key to decrypt the file.
  - Verify the hash
- **All encryptions and decryptions and hashing are executed at the client-side (browser)**
- No key is sent to the server side
- You can generate the RSA key pair manually - convert the generated keys in HEX format
- The GUI prompts for the keys during encryption / decryption (copy-paste in HEX format)
- You may store the public-key in localstorage of the browser, but never store the private-key

Tech Stack Suggestion:-

- Frontend : React + WebCrypto API
- Backend : Node.js / NextJs
- Crypto Libraries : crypto (Node.js), OpenSSL, Crypto++ or, any other

2. Web-App: PGP-Based Encrypted Messaging App