Cryptography and Network Security

<u>File Hash Calculator</u>

User Steps

1. **Accessing the Webpage:**
   - The user opens a web browser and navigates to the URL of your Flask application (e.g., http://127.0.0.1:5000/ if running locally).
2. **Encryption:**
   - **File Selection:** The user sees a "Choose File" button or similar file selection interface. They browse their local files and select a file to encrypt.
   - **Upload:** The user clicks an "Upload" or "Encrypt" button to submit the selected file to your web application.
   - **Results:** The webpage updates, displaying:
     - Confirmation of successful encryption.
     - Original file hash (SHA-256).
     - Encryption key (Make sure there's a way for them to securely store this).
     - Download link for the encrypted file.
3. **Decryption**
   - **File Upload:** The user selects the encrypted file using a file selection interface.
   - **Key and Hash:** The user is prompted to enter:
     - The encryption key used during encryption.
     - The original file hash (for validation).
   - **Submit:** The user clicks a "Decrypt" button.
   - **Results:** The webpage displays:

- Decryption status (success or failure).
- Hash of the decrypted file.
- Comparison of the original and decrypted file hashes.
- Download link for the decrypted file.