**Group Members:**

**Faria Ahmed(232486)**

**Ayesha Mudassar(232471)**

**AES-Based File Protection and Security System**

**Introduction:**

This project, **"File Protection System Using AES Encryption"**, is a secure file management tool. It provides robust features such as **file encryption and decryption** using AES-256, **file integrity verification** via SHA-256 hashing, and **secure file deletion** (shredding). User authentication ensures that only authorized users can access these functions. This system is ideal for protecting sensitive files and maintaining data confidentiality.

**Objective:**

* To implement a system that ensures secure file encryption, decryption, integrity verification, and secure deletion.

**Features:**

* User Authentication
* File Encryption and Decryption
* Integrity Verification (SHA-256)
* Secure File Deletion (Shredding)

**Working:**

1. **Authentication:**
   * Verifies the user with a hashed password (PBKDF2 + SHA256).
   * Logs success or failure.
2. **Encryption & Decryption:**
   * **Encrypt:** Uses AES (CBC mode) with a 256-bit key to secure the file.
   * **Decrypt:** Restores the original file using the same key and IV.
3. **Integrity Check:**
   * Generates a SHA256 hash to verify file integrity.
4. **Secure Deletion:**
   * Overwrites the file with random data (3 passes) and deletes it permanently.
5. **Logging:**
   * Logs all actions (encrypt, decrypt, delete) for tracking.
6. **Menu:**
   * Provides options: Encrypt, Decrypt, Check Integrity, Secure Delete, and Exit.

**Tools and Technologies Used**:

* Programming Language: Python
* Libraries:
  + cryptography (for AES encryption and hashing)
  + os (for file handling and random key generation)
  + logging (for action tracking)

**Advantages:**

1. **File Security**: Protects files using AES encryption.
2. **User Authentication**: Prevents unauthorized access.
3. **File Integrity**: Ensures files remain untampered with SHA-256 hashing.
4. **Secure Deletion**: Safely deletes files beyond recovery.
5. **Logging**: Tracks user actions for accountability.
6. **User-Friendly**: Simple menu-driven interface.
7. **Comprehensive Protection**: Combines encryption, integrity checks, and secure deletion.

**Testing and Results**:

* Test cases for authentication, encryption, decryption, and secure deletion.
* File integrity verification before and after encryption.

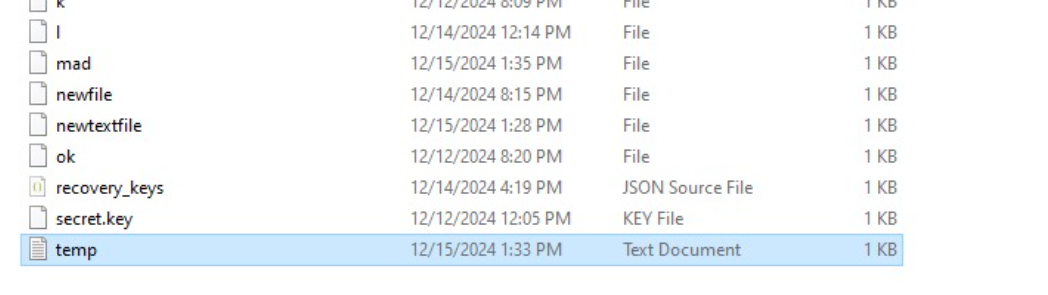
### ****Conclusion:****

The File Protection and Security System successfully ensures secure file management by integrating encryption, decryption, integrity verification, and secure deletion features. User authentication enhances access control, while AES encryption guarantees data confidentiality. File integrity is maintained using SHA-256 hashing, and secure deletion prevents unauthorized file recovery. The project effectively addresses critical aspects of data security, providing a reliable and robust solution for protecting sensitive files.

**OUTPUT:**

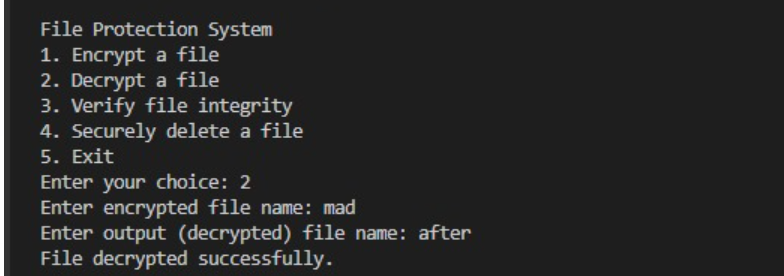
**Option 1 :**

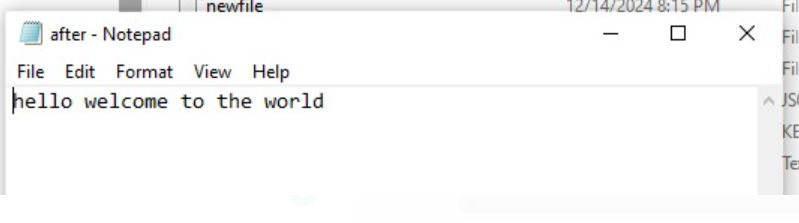
****

****

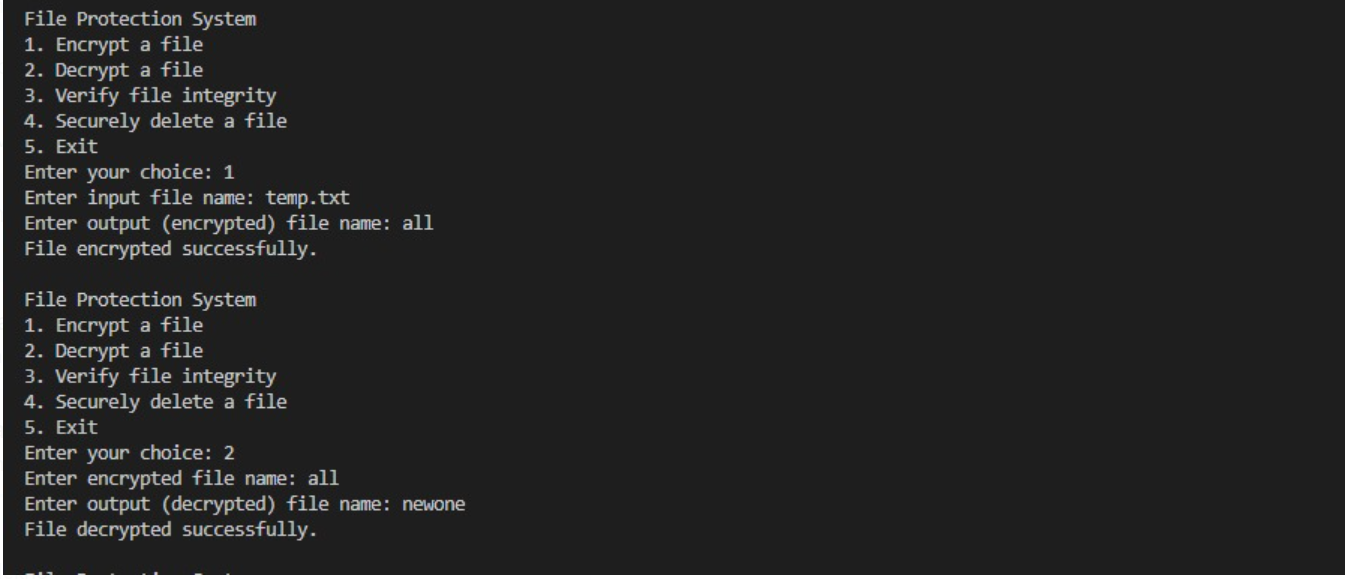
****

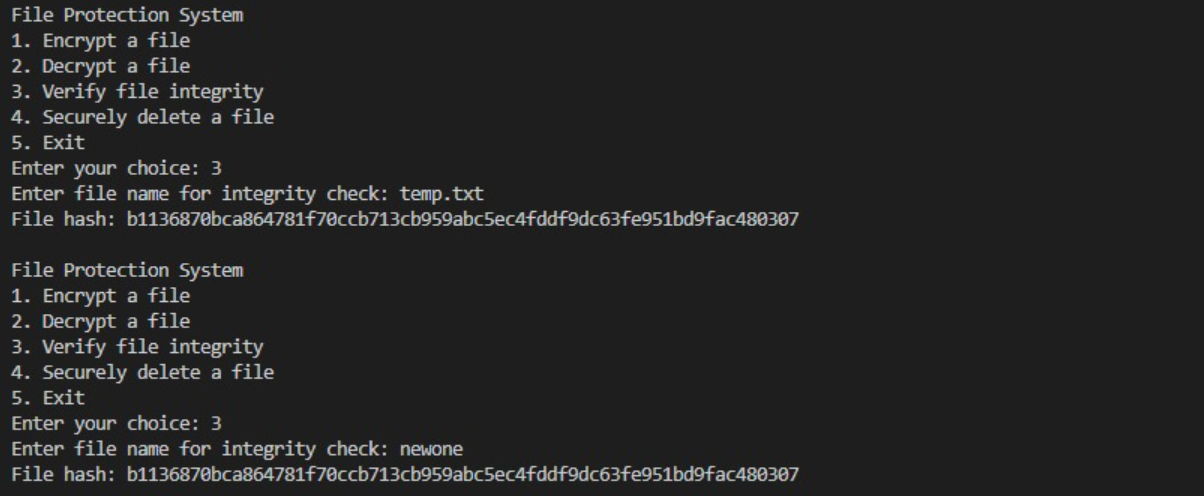
**Option 2:**

****

****

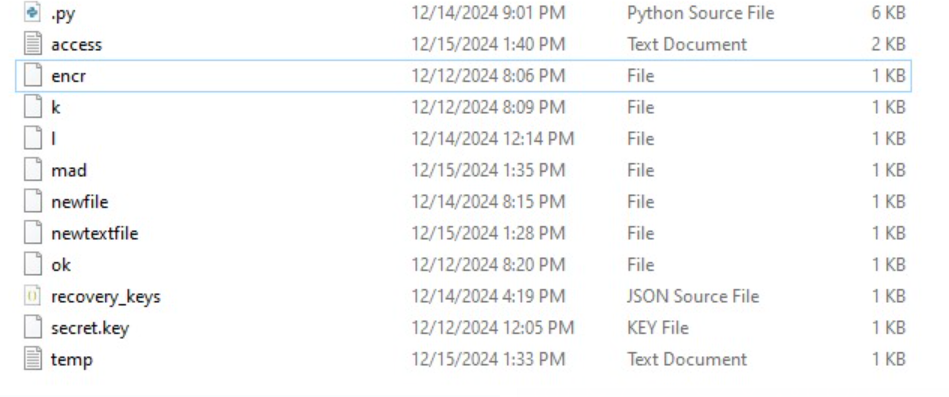
**Option 3:**

****

****

**Option 4:**

****

****

**Option 5:**

****