File Shredder Using Shamir's Secret Sharing

Saahil Mishra (22BCS105)
Rohit (22BCS100)
Shriya Udupa (22BCS121)
Laxmi (22BCS059)

Contents

1 Introduction

The "File Shredder Using Shamir's Secret Sharing" project is a secure file encryption and shredding tool. It combines AES encryption with Shamir's Secret Sharing (SSS) algorithm to split encryption keys into multiple shares, ensuring that the file can only be decrypted with a specific number of shares. Additionally, it securely deletes the original file to prevent recovery.

2 Features

1. **File Encryption:** Files are encrypted using AES for secure storage.
2. **Shamir's Secret Sharing:** AES keys are split into multiple shares, making the system highly secure.
3. **File Shredding:** Original files are securely deleted beyond recovery.
4. **Decryption:** Encrypted files can be decrypted by providing the required number of shares and the correct AES key.
5. **User-Friendly Interface:** Optional GUI for ease of use.

3 Project Structure

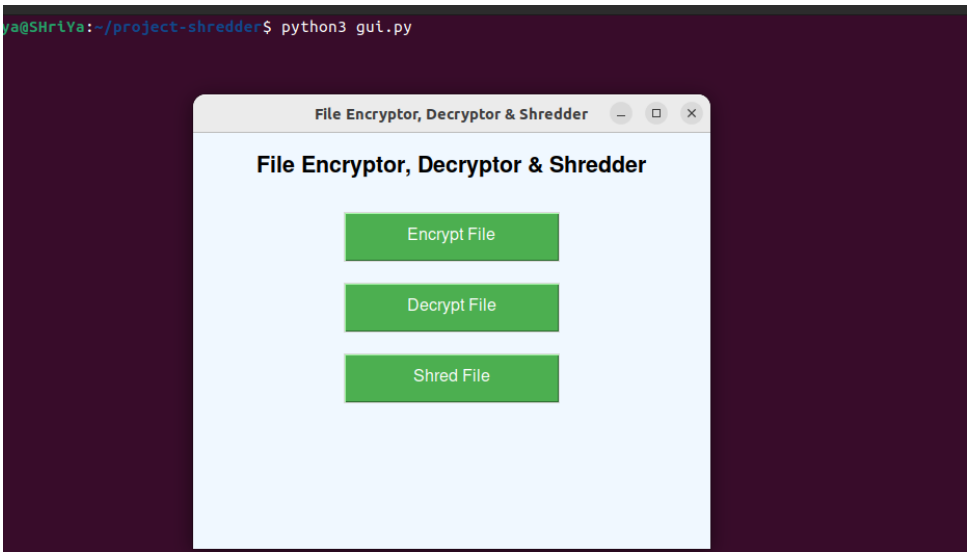
The project is organized into the following modules:

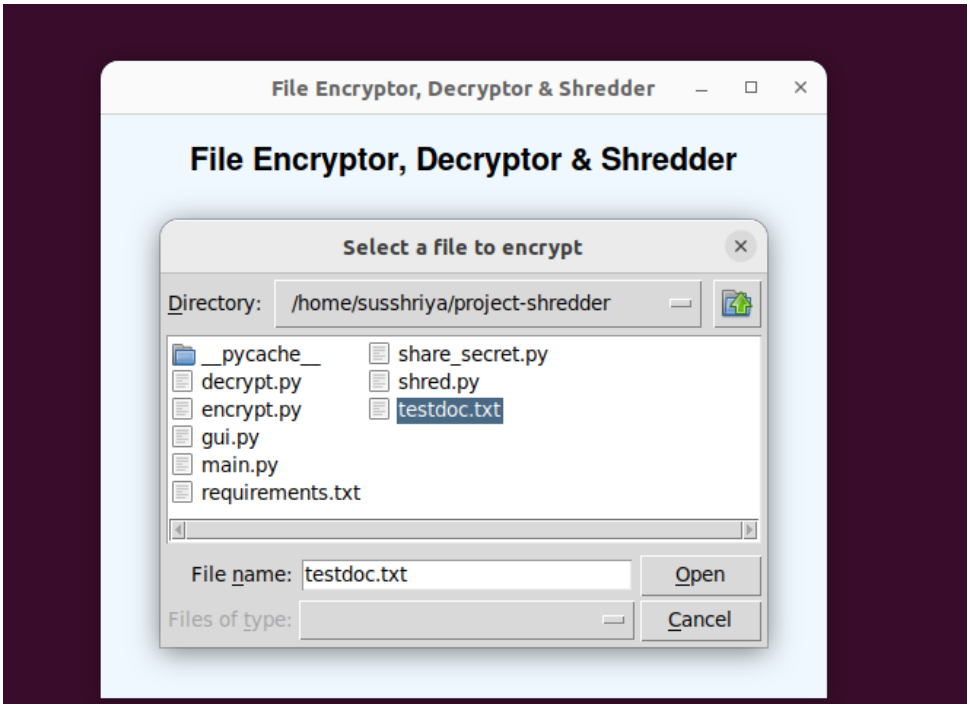
- **encrypt.py:** Handles file encryption and decryption using AES.
- **share_secret.py:** Implements Shamir's Secret Sharing algorithm for splitting and reconstructing the AES key.
- **shredder.py:** Provides functionality for secure file shredding.
- **main.py:** Executes the encryption, sharing, and shredding processes.
- **gui.py:** Implements the optional GUI.
- **requirements.txt:** Lists the Python libraries required for the project.

4 Implementation Details

4.1 File Encryption

Files are encrypted using the AES algorithm from the `pycryptodome` library. The encrypted file is stored separately while the AES key is split into shares.





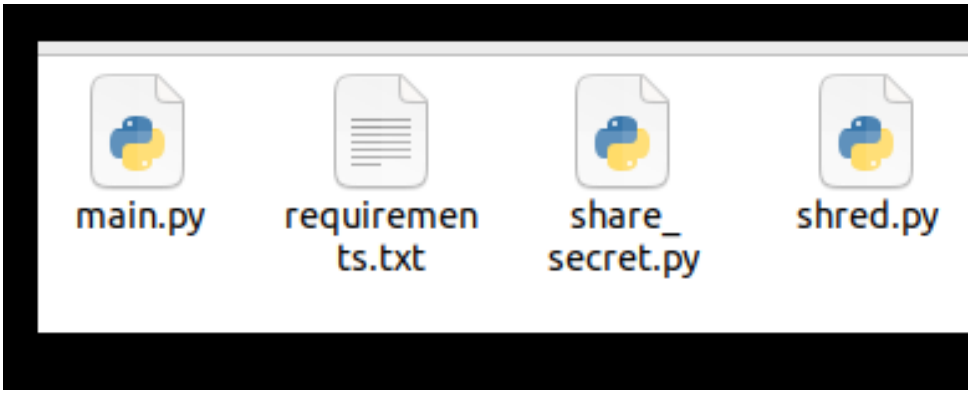
4.2 Key Sharing with Shamir's Secret Sharing

The AES key is split into n shares using Shamir's algorithm. A threshold k is specified, where k shares are required to reconstruct the key.

```
susshriya@SHriYa:~/project-shredder$ python3 gui.py
File shredded successfully: /home/susshriya/project-shredder/testdoc.txt
File encrypted successfully. Saved as: /home/susshriya/project-shredder/testdoc.txt.enc
AES Key (hex): 8a6bf950d2a16a595c30effa1f39436f
```

4.3 File Shredding

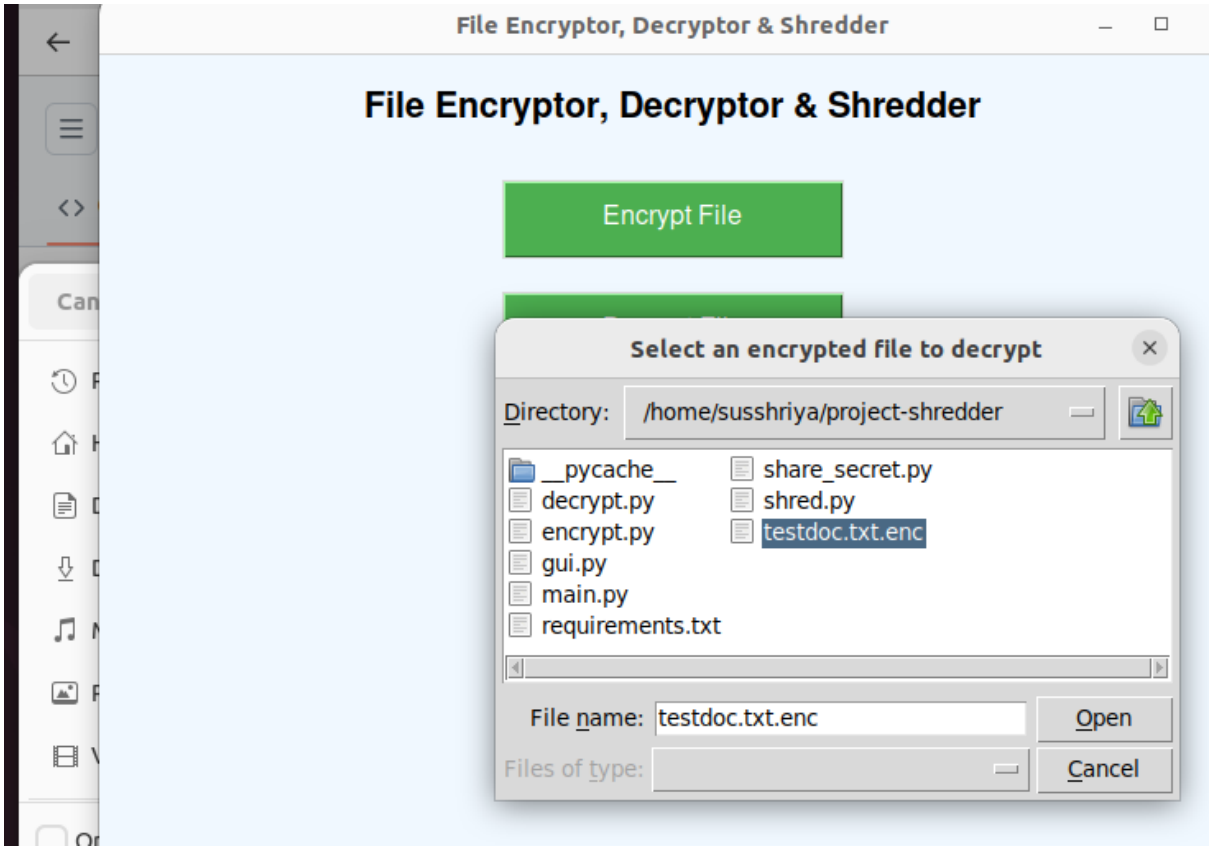
The original file is securely deleted using multiple overwrites to ensure that it cannot be recovered.

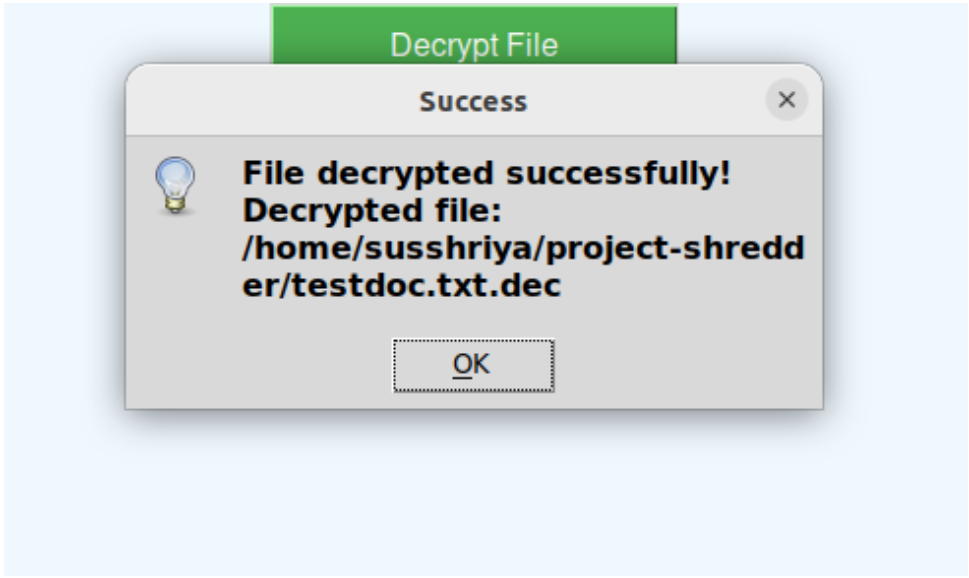


4.4 File Decryption

To decrypt the file, the user must provide:

- The encrypted file.
- A minimum of k shares to reconstruct the AES key.
- The AES key.





5 Conclusion

The File Shredder project demonstrates a secure approach to file management by integrating AES encryption, Shamir's Secret Sharing, and secure deletion techniques. This tool ensures that sensitive files are both encrypted and irrecoverable, making it highly reliable for data security applications.

6 Future Enhancements

- Adding advanced GUI features for better user interaction.
- Integrating cloud storage for distributing shares securely.
- Providing an option for different shredding standards (e.g., DoD 5220.22-M).