

1. 作品功能与性能说明

1. 用户认证：通过密钥认证用户是否合法。
2. 文件操作：
 - 合法用户：可以添加文件、删除文件、浏览文件列表、查看真实的文件内容。
 - 非法用户：只能浏览文件列表，查看文件内容时会看到欺骗性的内容。
3. 用户管理：
 - 管理员：可以添加用户、设置用户密钥、查看用户列表。
 - 用户：只能进行文件操作，不能管理用户密钥。

2. 设计与实施方案

2.1 实现原理

(硬件框图、软件流程、相关描述等)

- 1、 用户输入角色和密钥进行认证。
- 2、 根据用户角色判断用户是管理员、合法用户还是非法用户。
- 3、 管理员可以进行用户管理操作，包括添加用户和设置用户密钥。
- 4、 合法用户可以进行文件操作，包括添加文件、删除文件、浏览文件列表、查看真实的文件内容。
- 5、 非法用户只能浏览文件列表，查看文件内容时会看到欺骗性的内容。

2.2 参考文献

National Institute of Standards and Technology. "FIPS PUB 197: Advanced Encryption Standard (AES)."

2.3 运行结果

通过 GUI 界面，管理员可以添加用户、设置用户密钥、查看用户列表。合法用户可以添加、删除、浏览和查看文件内容。非法用户只能浏览文件列表，查看文件内容时会看到欺骗性的内容。

2.4 技术指标

- 加密算法：AES
- 填充方式：PKCS7
- 用户认证：基于密钥

- 界面库：Tkinter

3. 系统测试与结果

3.1 测试方案

通过 GUI 界面进行以下测试：

1. 输入合法密钥，进行文件操作测试。
2. 输入非法密钥，进行文件操作限制测试。
3. 查看文件内容的真实性。
4. 管理员添加用户和设置密钥。

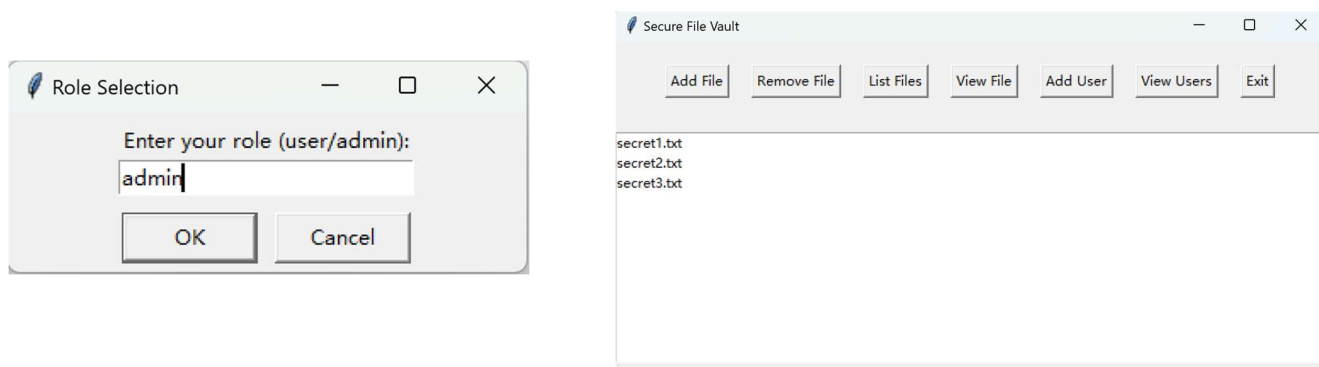
3.2 功能测试

测试以下功能：

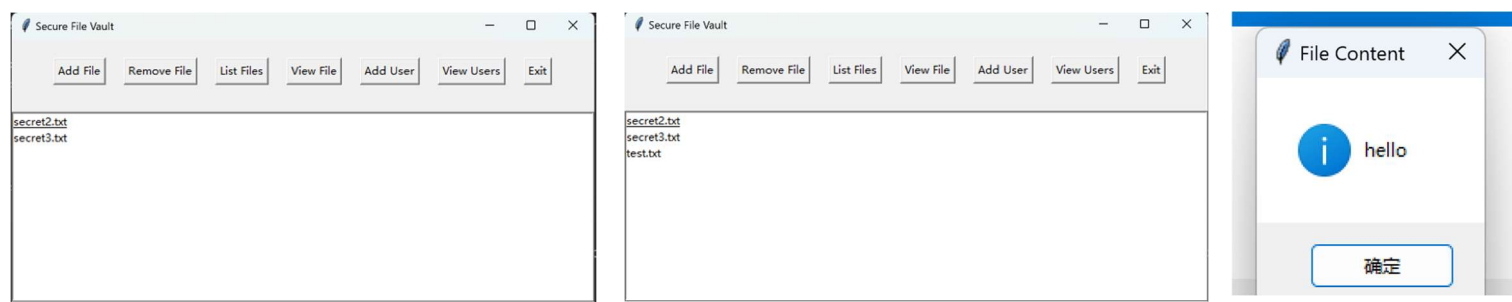
功能	合法用户	非法用户	管理员
添加文件			
删除文件			
浏览文件列表			
查看文件内容			
添加用户			
设置密钥			
查看用户列表			

3.3 测试数据与结果

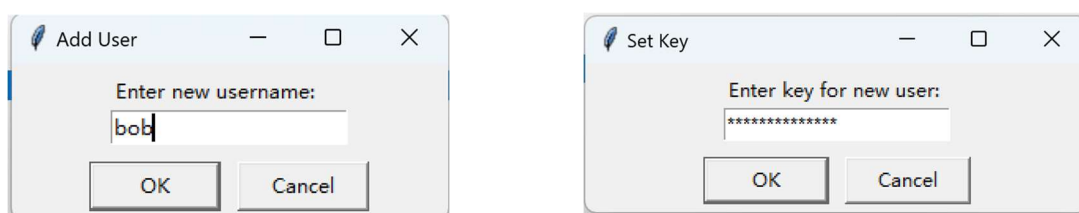
首先，选择管理员模式，输入管理员的登录密钥后，可以看到如下窗口：



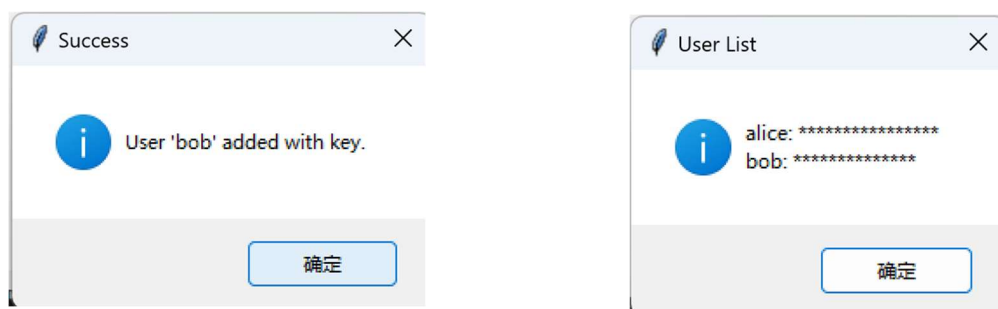
先测试删除文件、添加文件、查看文件：



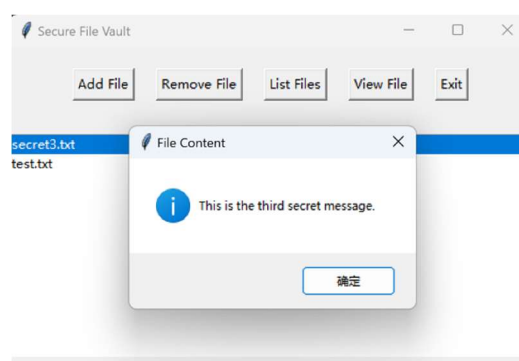
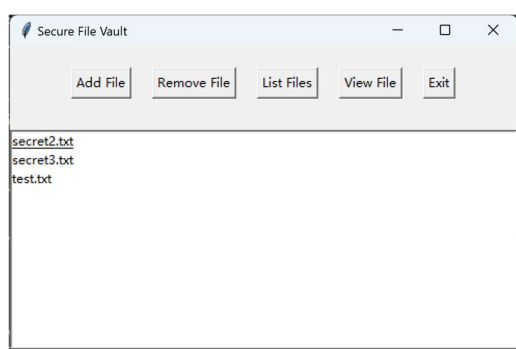
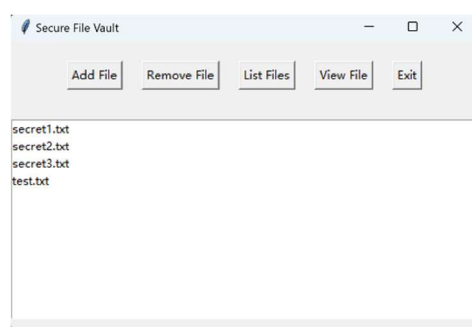
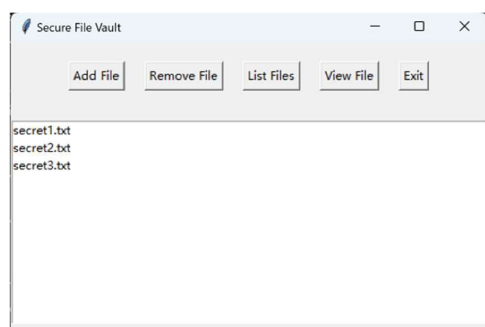
然后，测试管理员添加用户，首先输入用户名和用户密钥，



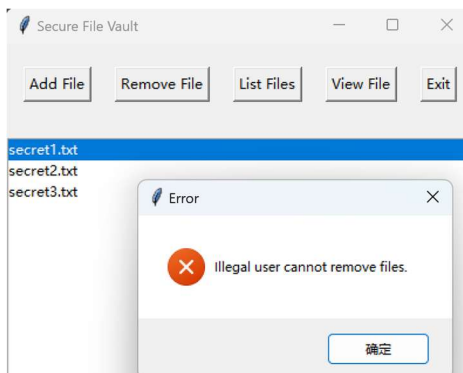
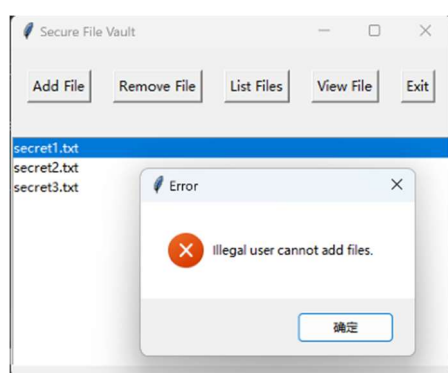
可以查看到用户信息：



管理员退出登陆后，使用用户 bob 登录，输入用户名和正确的密钥后，测试添加文件、删除文件和查看文件。



退出登陆后，再次输入 bob 的用户名，但是输入错误的密钥，测试上述功能。



测试结果如下：

功能	合法用户	非法用户	管理员
添加文件	成功	拒绝操作	成功
删除文件	成功	拒绝操作	成功
浏览文件列表	成功	成功	成功
查看文件内容	显示真实内容	显示欺骗性内容	显示真实内容
添加用户	不可用	不可用	成功

设置密钥	不可用	不可用	成功
查看用户列表	不可用	不可用	成功

4.应用前景

该工具适用于需要保护文件内容安全的场景，如企业文档管理、个人隐私文件管理等。

5.结论

通过设计和实现保密文件库工具，实现了对文件内容的安全保护。通过合法用户和非法用户的区别对待，确保了文件的保密性和安全性。图形用户界面的设计使得工具易于使用，具有较好的应用前景。