详细设计

一、引言

1、编写目的

本概要为文件保险箱的说明概要，为用户指出本软件的具体信息和使用方法

2、背景

A、软件名称：文件保险箱

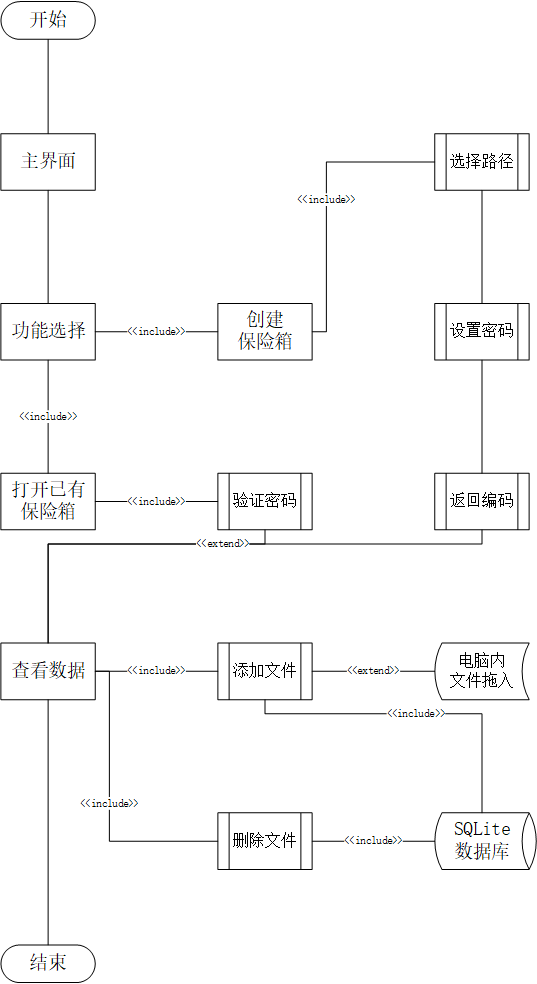
B、开发人员：任浩龙、周添、宋杰、任俊霖

3、定义

本软件是为用于Windows系统用户对于计算机储存的文件进行加密保存、并通过账户和密匙进行管理的软件

二、程序系统的结构

结构图表见下页



三、程序设计说明

1、程序描述

文件保险箱软件是一款具有一般的文件管理功能，包括增加、更改、查找、删除的功能，以及文件保险箱特殊的功能：文件加密功能 的软件，我们使用更为安全的非对称式加密进行文件加密。

2、功能

使用保险箱对文件进行加密，管理保险箱中的文件等功能

3、输入项

输入：账号和密匙

拖动输入：从外部拖动文件到保险箱进行加密

4、输出项

返回编码

输出保险箱数据

5、加密算法

RSA非对称式加密算法

6、流程逻辑

具体流程已经在（二）中图表体现

7、接口

接口：  
       RSAE:  
               ENCY:加密文件  
               DECY:解密文件  
               LKEY:读取密钥  
               GKEY:生成密钥  
               PKEY:获取密钥  
               SKEY:写入密钥  
       MD5E:  
               MD5C:获取摘要  
               MD5P:判断密码  
               MD5Q:更改密码  
      FIFT:读取文件  
      FIFR:写入文件  
      CHEC:判断1A  
   READ\_SZIE:获取长度

8、注释设计

#ifndef RSAE\_HPP

#define RSAE\_HPP

#include"HEAD.CPP"

#define KEY\_LENGTH 1024 // 密钥长度

#define PUB\_KEY\_FILE "PUBK.PEM" // 公钥路径

#define PRI\_KEY\_FILE "PRIK.PEM" // 私钥路径

#define RSA\_S RSA\_FLAGS\_SECURIT // 加密标识

#define RSA\_P RSA\_PKCS1\_PADDING // 填充方式

class RSAE

{

public:

void LKEY(); //载入密钥，从文件读取公私钥

void GKEY(string[2]); //创建密钥，本地文件会被覆盖

void PKEY(string[2]); //读取密钥，存放在字符串数组

void SKEY(string[2]); //写入密钥，从传入字符串写入

string ENCY(const string&);//加密

string DECY(const string&);//解密

private:

string RSAK[2]; //主密密钥

};

#endif

#ifndef MD5E\_HPP  
#define MD5E\_HPP  
#include "HEAD.CPP"  
class MD5E  
{  
public:  
        MD5E(){}                  //构造函数  
       ~MD5E(){}                  //析构函数  
        string MD5E\_TEXT;         //原始文本  
        string MD5E\_ENCY;         //摘要字符  
        string MD5E\_EN16;         //摘要文本  
 unsigned char MD5E\_ESTR[33]= {0};//中间数据  
          char MD5E\_BUFF[65]= {0};//缓冲文件  
          char MD5E\_TEMP[ 3]= {0};//临时转存  
    bool MD5P(string);            //验证密码  
    void MD5Q(string);            //写入密码  
  string MD5C();                  //获取摘要  
  string MD5C(string);            //获取摘要  
};  
#endif

9、限制条件

文件名不能超过4096字节，文件内容不能超过2^32字节，文件名称不能包含空格，加密字符串不能有26号ASCII字符

10、测试计划

将文件放入保险箱，检验加密功能，并应用解密，检查解密文件是否与原文件相同

11、尚未解决的问题

文件安全擦除，私钥AES高强度加密，带salt的MD5摘要，PKI前向安全性