实验六 PGP软件应用

**一、实验背景**

PGP（Pretty Good Privacy）是主要由美国的Philip Zimmermann创造的用于保护网络上电子邮件和文件传输安全的技术，在学术界和技术界都得到了广泛的应用。PGP的主要特点是使用单向散列算法对邮件/文件内容进行签名以保证邮件/文件内容完整性，使用公钥和私钥技术保证邮件/文件内容的机密性和不可否认性。PGP不仅提供程序试用，而且提供程序源码，是一款非常好的密码技术学习和应用软件。PGP的30天试用版本可以从http://www.pgp.com 下载。（注：由于本实验中只用到PGP加/解密和签名/验证功能，而此功能是PGP最基本的功能，因此任何一个PGP版本都支持此类功能。本实验仅以PGP.Desktop 9.9为例进行介绍。）

**二、实验目的**

通过使用PGP软件加强对公钥密码技术应用的理解和掌握。

**三、实验条件**

(1) PGP Desktop 9.9   
(2) 基于Windows的PC机2台，分别为发送者userA和接收者userB使用。

**四、实验任务**

(1) 掌握PGP基本原理

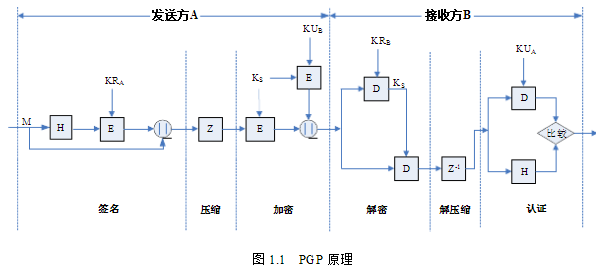
(2) 利用PGP软件对文件进行加密/解密

(3) 利用PGP软件对文件进行签名/验证

**五、实验内容**

1. PGP基本原理

如图1.1所示显示了PGP提供数字签名和机密性的操作过程。如果在实际操作中只需要数字签名服务，则把加密和解密模块取消即可；同样，若只需要机密性服务，则把签名和认证模块取消即可。



1) 签名 发送方A产生报文M，用单向散列算法（SHA或MD5）生成报文摘要，然后用自己的私钥KRA，采用RSA或DSS数字签名算法对报文摘要进行加密，把计算结果串接在M的前面。

2) 压缩 默认情况下，PGP在签名之后加密之前对报文进行压缩，用Z表示。此方法有利于在电子邮件传输和文件存储时节约空间，而且由于压缩过的报文比原始明文冗余更少，密码分析更加困难，因此也加强了加密的强度。一般在PGP软件中使用Pkzip算法进行压缩。 3) 加密 发送方生成128比特的用于作为该报文会话密钥的随机数 ，使用此会话密钥采用 CAST-128或IDEA或3DES算法对报文进行加密。然后，由于会话密钥只被使用一次，因此要把会话密钥和报文绑定在一起传输。为了保护此会话密钥，

需要使用接收者的公开密钥 采用RSA算法对会话密钥进行加密，并附加到报文的前面。

4) 解密

接收方收到发送方发来的报文，用自己的私钥采用RSA

算法解密出会话密钥 ，

然后用会话密钥 来解密报文。

5) 解压缩

将解密后的报文进行解压缩操作，得到压缩前的报文。

6) 认证 对解压缩后的报文进行处理，提取出发送方用自己的私钥加密的报文摘要和明文，对前者用发送方的公钥 来解密得到报文摘要，对后者用相同的散列算法生成新的报文摘要。 两个报文摘要相比较，如果两者相匹配，则报文作为已经认证的报文被接受。

2. PGP软件安装（略）

3. 交换公钥

在数据被处理之前，通信双方必须相互交换自己的公钥。为了存储密钥，PGP在每个结点提供一对数据结构，一个用来存储该结点拥有的公开/私有密钥对，被称为私有密钥环；另一个用来存储该结点所知道的其他用户的公开密钥，被称为公开密钥环。

双击右下角工具栏 图标打开【PGP Desktop】界面，点击“文件”—“新建PGP秘钥”，按照向导生成新的用户秘钥。

选择界面左侧“PGP 秘钥”，可以看到生成的用户密钥信息，以用户userA为例生成密钥，以用户名和邮箱地址为标识。双击“userA”打开【userA-秘鈅属性】界面，可以查看密钥的ID、类型、创建时间（即时间戳）、加密算法等信息，如图1.2所示。

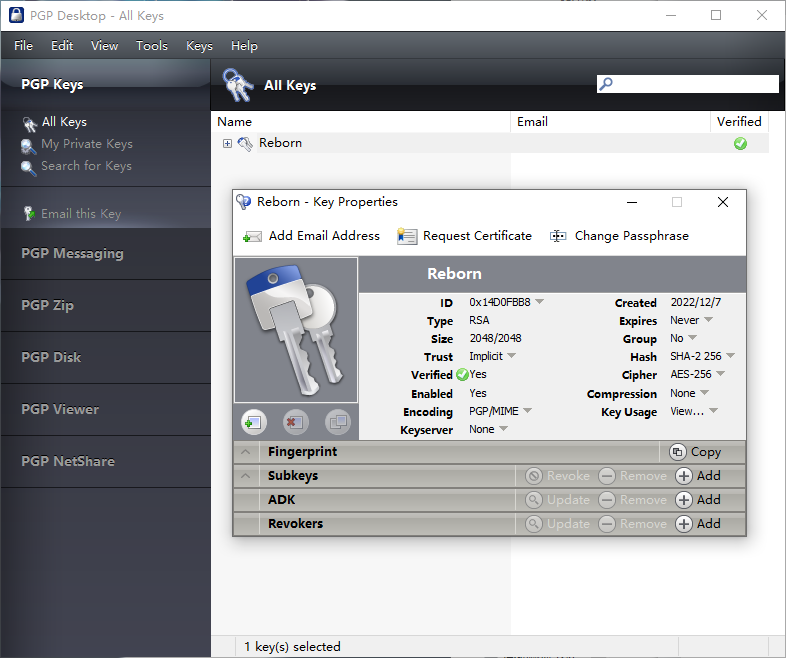


图 1.2 用户密钥信息

按照前面PGP安装步骤在另一台机器上安装PGP并生成userB密钥，然后在【PGP Desktop】窗口中用鼠标右击要交换的密钥userB→“导出”，导出密钥，存成userB.asc的文件，然后把这个文件自由地传送给給userA，如利用邮件或文件共享方式进行交换。 userA取得发送方公钥文件以后，双击userB.asc附件，出现【选择秘鈅】界面，选择密钥userB，然后单击“导入”导入发送方公钥。如图1. 3所示。

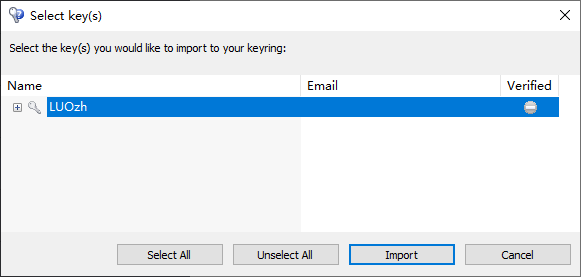


图 1.3 导入对方公钥

userB密钥导入后userA的【PGP Desktop-全部秘鈅】界面如图1. 4所示。

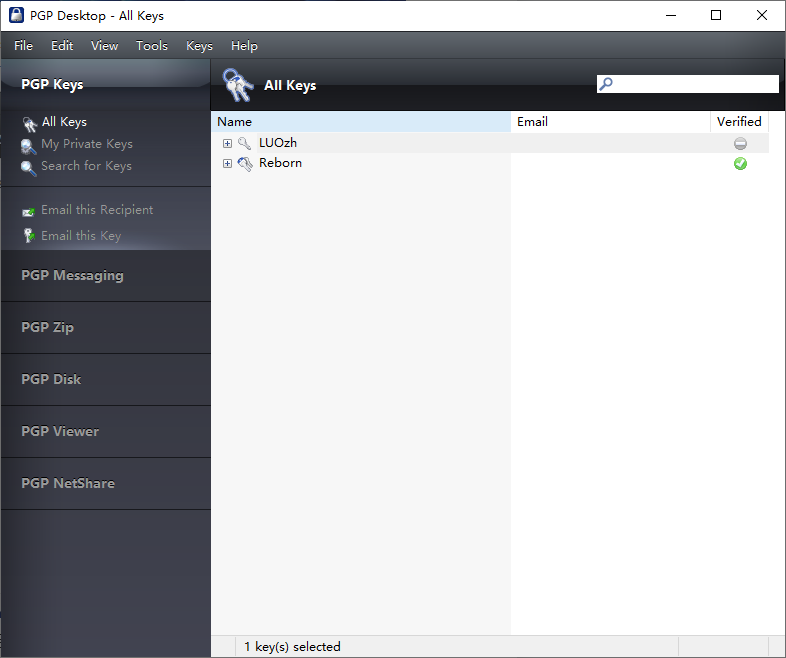
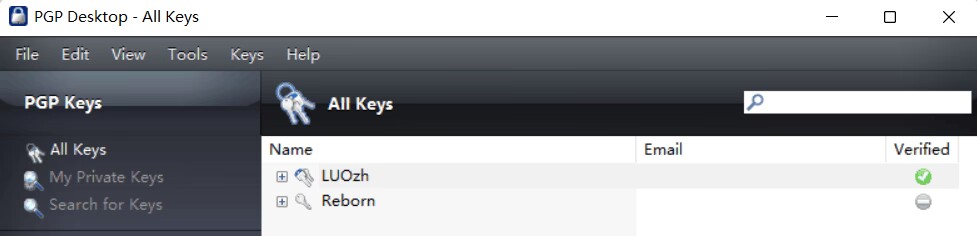


图 1.4 密钥查看

同样将userA的密钥导入到userB 的密钥环中。



4. 加密/解密文件

在userA机器上新建一个文本文件，输入内容并选中。如图1.5所示

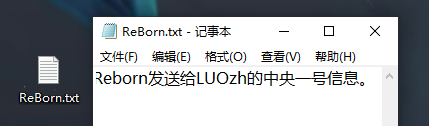


图1.5 明文信息

单击右下角工具栏PGP图标→“当前窗口”（Current Window） →“加密”(Encrypt)，出现【密钥选择对话框】界面， 双击userB密钥使其出现在“收件人”对话框，如图1. 6所示。

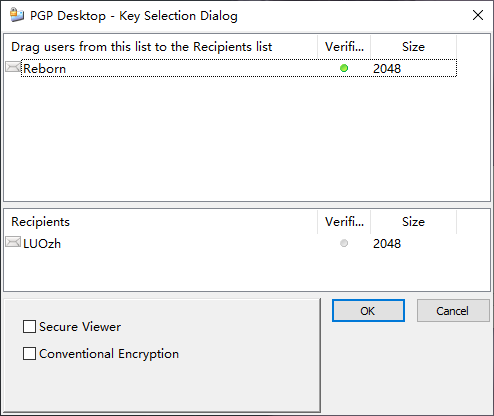


图1.6 选择接收方公钥

单击“确定”，发现文本内容已被加密，如图1.7所示。

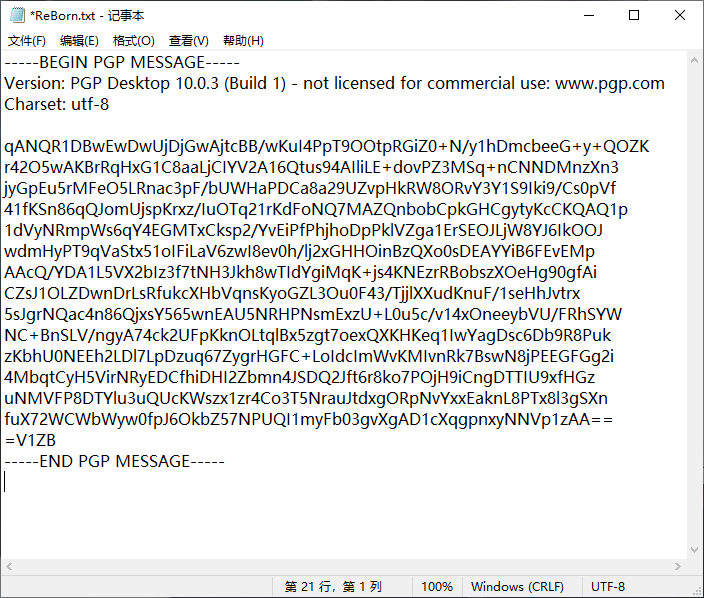
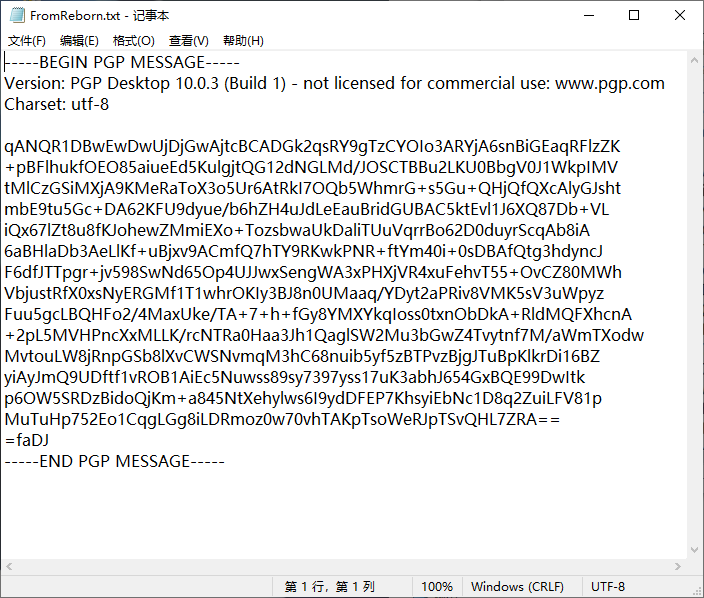


图1.7 密文信息

将文件保存成fromA.txt，用邮件或文件共享方式发给userB。userB收到userA发来的加密文件fromA.txt后双击打开，右击右下角工具栏PGP图标→“当前窗口” →“解密& 验证”(Decypt&Verify)， 出现如图1. 8所示界面。



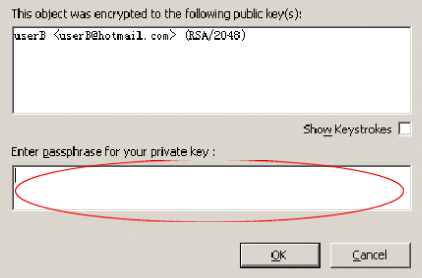
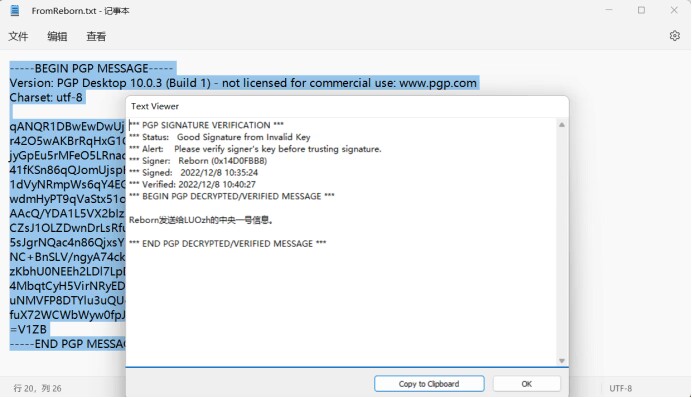


图1.8 输入口令短语

输入userB的口令短语，单击“OK”，系统会提取userB的私钥对密文进行解密从而恢复出明文。



5. 签名/验证

右击右下角工具栏PGP图标→“当前窗口” →“签名”(Sign)生成签名文件如图1.9所示



图1.9 签名信息

将文件保存成signA.txt，用邮件或文件共享方式发给userB。userB收到userA发来的签

名文件后双击打开，右击右下角工具栏PGP图标→“当前窗口” →“解密& 验证”，出现验证界面，如图1.10所示。

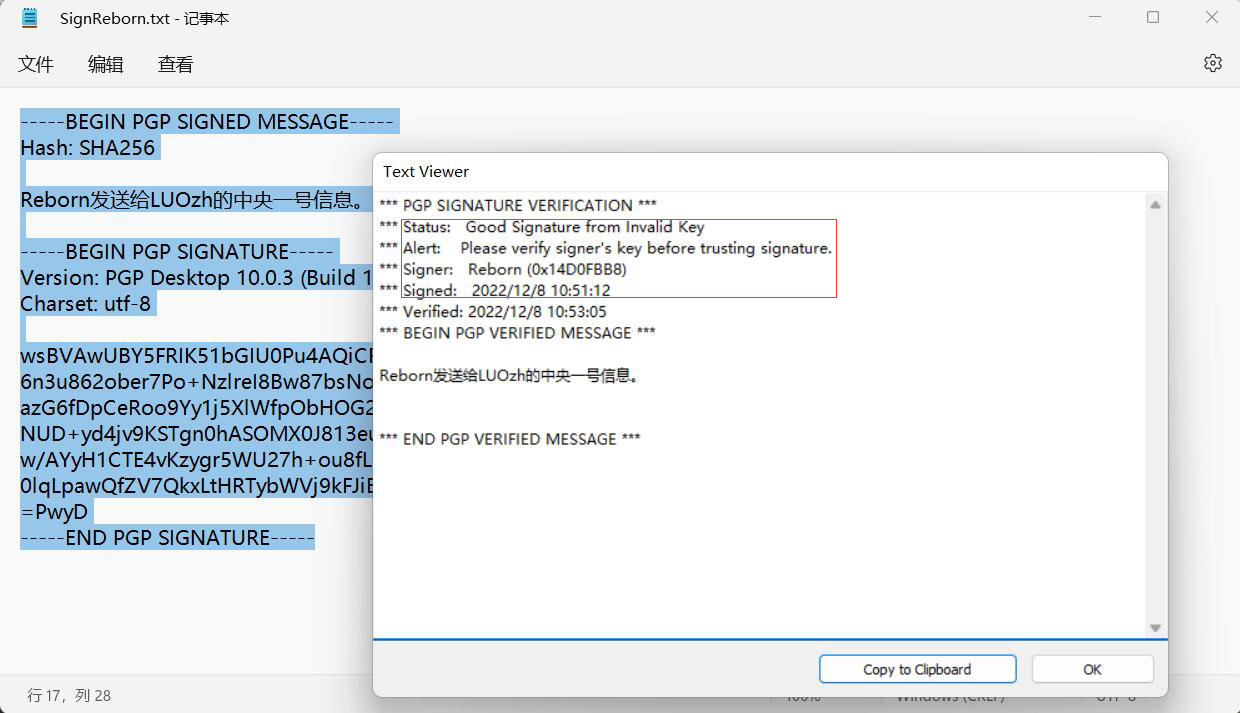
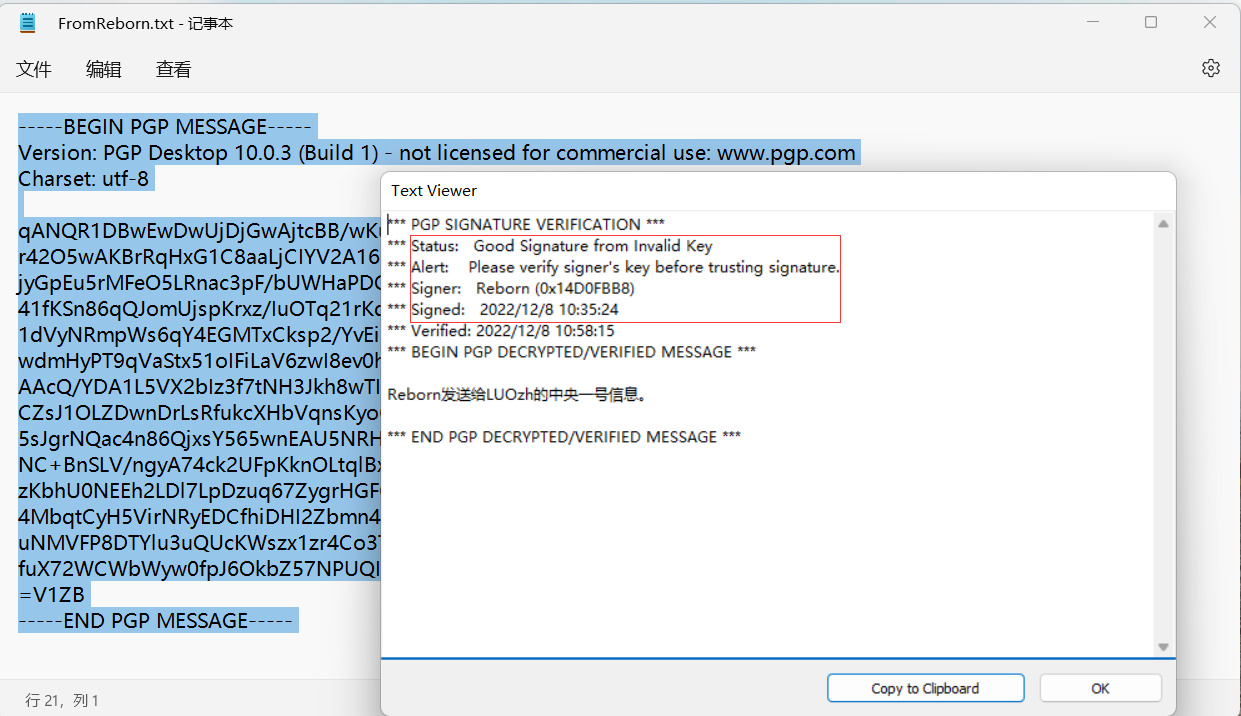


图1.10 验证签名

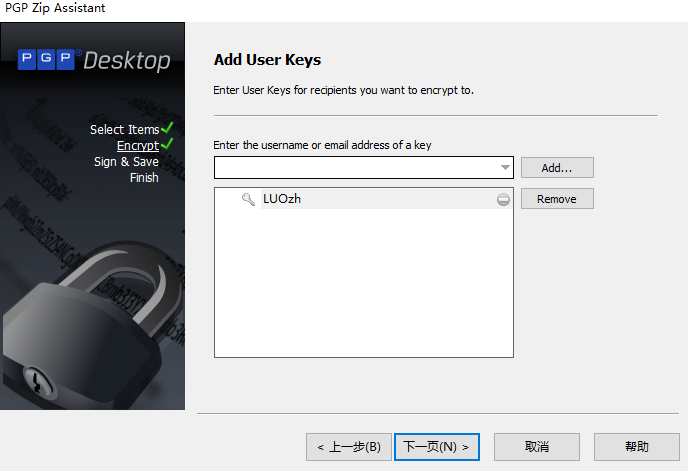
看到签名状态为“Good Signature”则证明签名有效。 如果userA想发给userB既签名又加密的信息，则需要右击右下角工具栏PGP图标→“当前窗口” →“加密 & 签名”，过程同前。



6. 直接对文件进行加密/解密密，签名/验证：

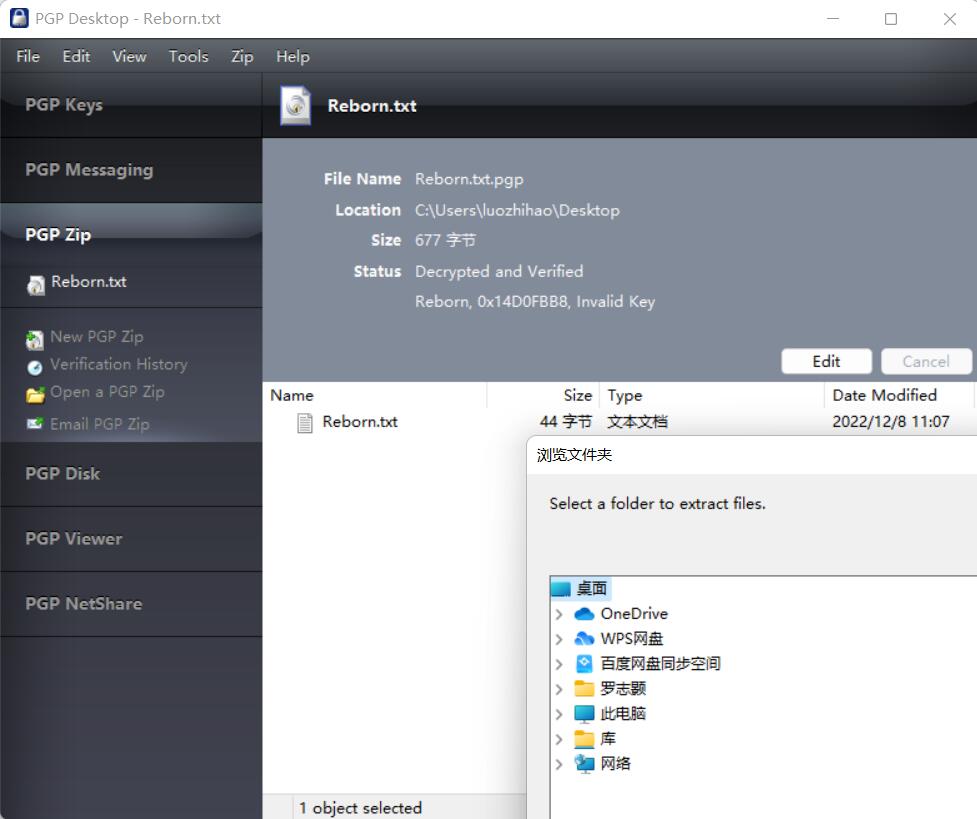
右击要加密的文件A.txt→“PGP Deskop”→“使用密钥保护 A.txt”。

在【PGP压缩包助手】界面的下拉菜单中选中要加密的公钥userB，单击“下一步”

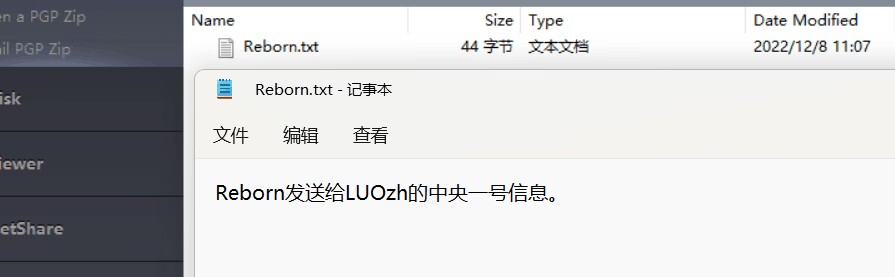
，生成文件A.txt.pgp，



将文件发送给userB，userB双击解密



选择导出到桌面



得到解密之后的文件。

对文件直接签名与加密类似，选择好签名密钥以后在保存目录下生成一个.sig文件，即是签名文件，然后将原文件与签名文件一起发送给接收方。接收方收到以后进行验证。

实验报告要求

1、使用PGPDesktop加密工具完成实验内容：导入密钥、加解密、签名与验证

2、实验报告内容应体现具体的操作流程，除相关的文字说明外，应有一定的截图说明。（密钥的导入、加解密结果、签名验证结果均需要截图）

要求：思路清晰，内容完整。