第一章　PGP 软件应用实验

1.1　实验介绍

PGP 软件是一款优秀的个人安全防护软件。请安装并使用该软件的主要功能，进行相关实验，验证 PGP 软件的可用性和有效性。

1.2　实验内容

密钥对的产生、公钥的导出导入、文件的加密、Email 的加密和签名、文件的粉碎、虚拟磁盘加密、磁盘空间的粉碎等功能。

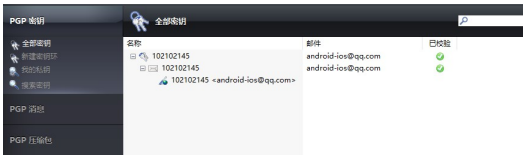
1.3　报告内容

按功能模块进行实验，并组织书写实验步骤与实验结果，分别以不同小节给出。实验中请使用与学号、姓名等特征信息相关的实验数据，体现相关实验是自己所完成的。

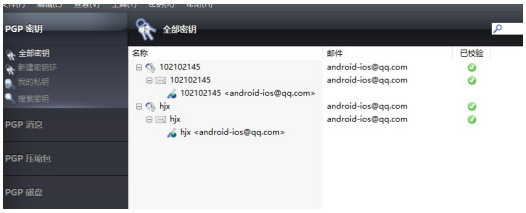
1.4　PGP 密钥对的产生与管理

相关技术原理:
密钥是加密运算和解密运算的关键，也是密码系统的关键。密码系统的安全取决于密钥的安全，而不是密钥算法或保密装置本身的安全。密码体制可以公开，密码设备可以丢失，同一型号的加密设备可以继续使用，但若密钥一旦丢失或出错，就会使非法用户窃取信息。因此密钥管理在计算机的安全保密系统中尤为重要。

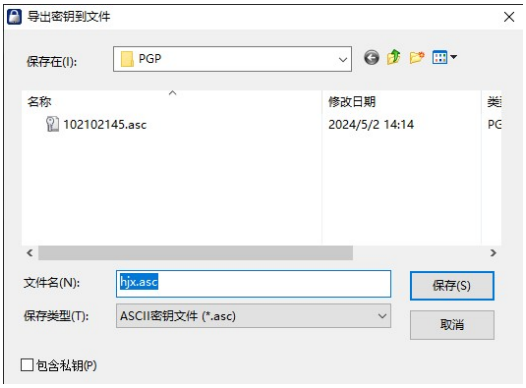
生成名为 “102102145” 的个人密钥对.



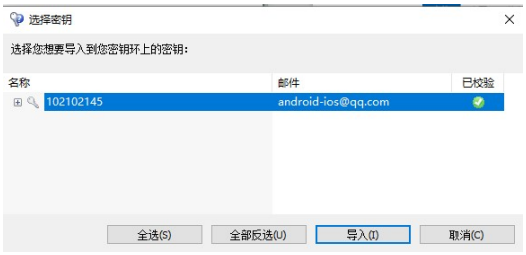
同理，再生成名为 “hjx” 的个人密钥对.



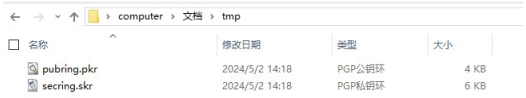
导出的两个公钥文件.



公钥的导入.



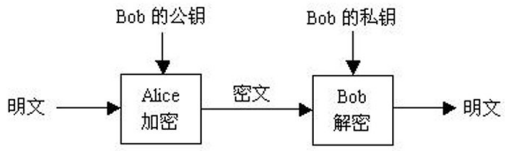
备份 PGPkeys 中已有密钥信息.



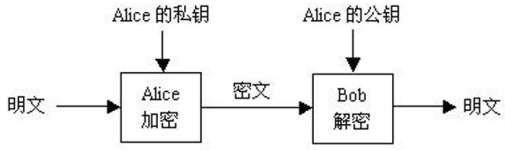
1.5 文件的加密与签名

相关技术原理:

简单来说，在加密的应用场景下，发送方是用接收方的公钥加密，接收方用私钥解密。而签名则是发送方用私钥加密，接收方用发送方公钥解密认证。



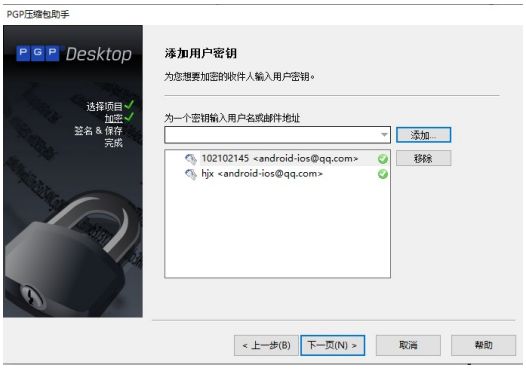
a）加密模型



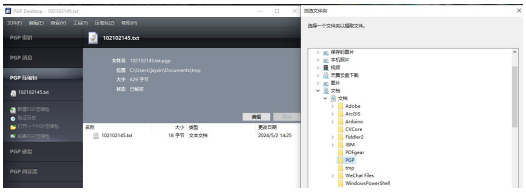
b）认证模型

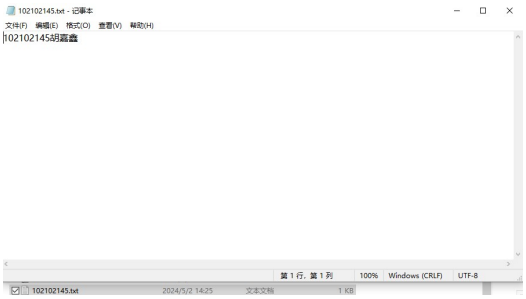
创建待加密文件.

设置对其进行密钥保护.

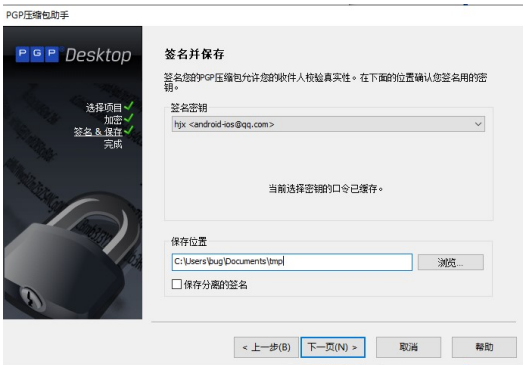


解密被加密文件.



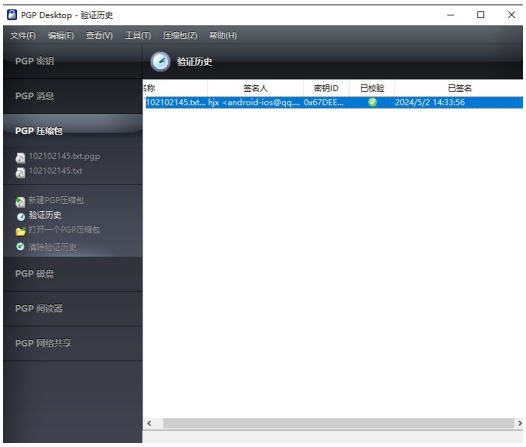


文件加密 & 签名.

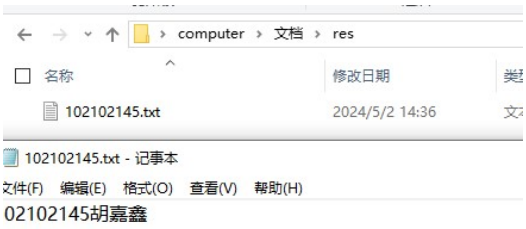


文件解密及其校验.

校验结果如下:

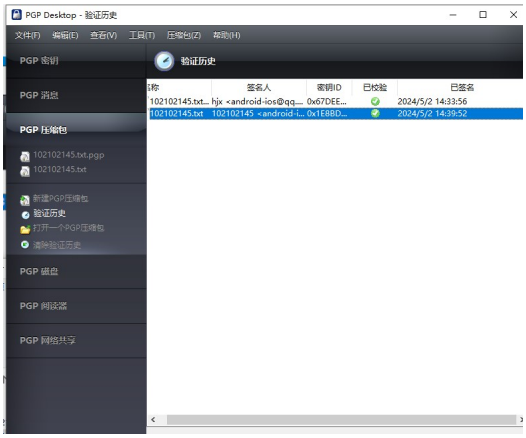


解密结果.



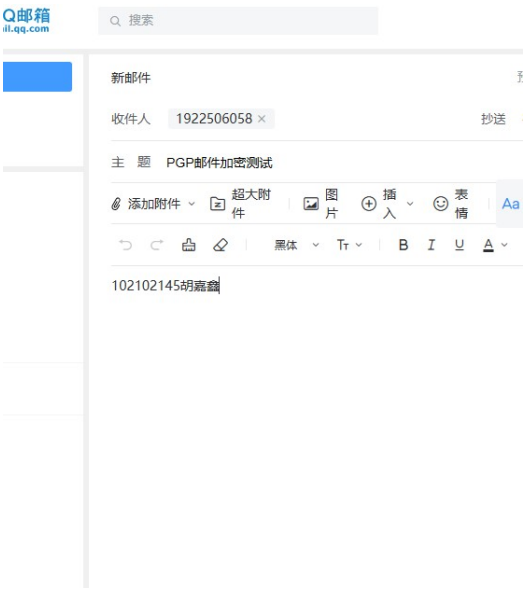
文件签名.

校验结果查看.



1.6 Email 的加密与签名

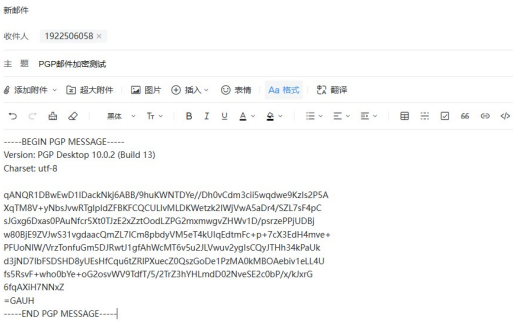
用邮箱 `android-ios@qq.com` 发送邮件给 `1922506058@qq.com`，下图是原始信息.



将原始信息复制，用 PGP 剪贴板进行加密.

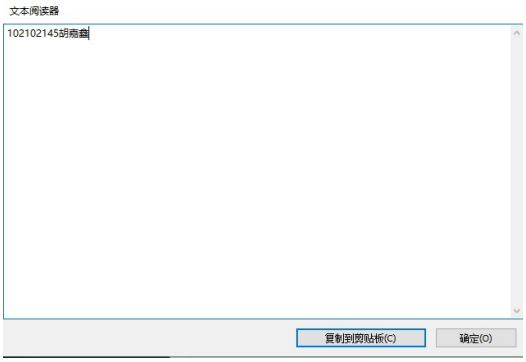
选择用收件人的公钥进行加密.

将加密后内容粘贴到发件框中，覆盖原来的未加密内容.



登录接收端账号 1922506058@qq.com，复制接收信息到剪贴板.

使用接收端私钥进行解密, 解密后还原出原始内容如下:



1.7 文件的粉碎

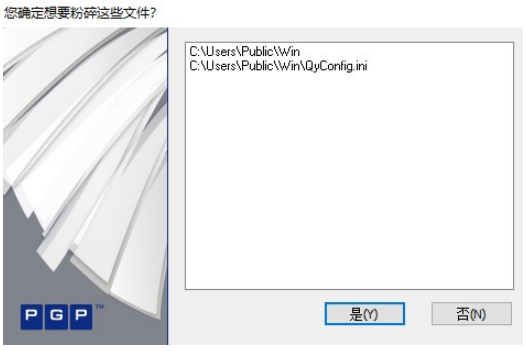
相关技术原理:

存储在硬盘中的每个文件都可分为两部分：文件头和存储数据的数据区。

文件头用来记录文件名、文件属性、占用簇号等信息，文件头保存在一个簇并映射在 FAT 表（文件分配表）中。而真实的数据则是保存在数据区当中的。平常所做的删除，其实是修改文件头的前 2 个代码，这种修改映射在 FAT 表中，就为文件作了删除标记，并将文件所占簇号在 FAT 表中的登记项清零，表示释放空间，这也就是平常删除文件后，硬盘空间增大的原因。

而真正的文件内容仍保存在数据区中，并未得以删除。要等到以后的数据写入，把此数据区覆盖掉，这样才算是彻底把原来的数据删除。如果不被后来保存的数据覆盖，它就不会从磁盘上抹掉。用 Fdisk 分区和 Format 格式化和文件的删除类似，前者只是改变了分区表，后者只是修改了 FAT 表，都没有将数据从数据区直接删除。

由文件删除的原理可知，要彻底删除数据，只有把删除文件所在的数据区完全覆盖掉。绝大部分彻底删除工具所使用的就是这个道理：把无用的数据反复写入删除文件的数据区，并进行多次地覆盖，从而达到完全删除文件的目的。



1.8 虚拟磁盘的加密

相关技术原理:

把文件，网络文件，内存等通过技术手段“伪装”成磁盘，让用户感觉像一个真实磁盘的“磁盘”

就称为虚拟磁盘。

1.9 磁盘空间的粉碎

原理类似文件的粉碎.