**信息安全技术实验报告**

**姓名:**

**学号:**

**专业：**

日期:

**Lab2: 基于GPG4Win的加解密实验**

**一、实验目的（简要写，不必全部照抄实验要求文档中的内容）**

了解公钥算法的应用。通过在GPG4Win软件下做文件加解密、签名和邮件加解密的实验，来掌握公钥算法在加解密和数字签名方面的应用。

**二、实验环境（如实给出实验平台）**

Win10系统

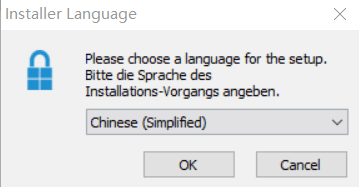
**三、实验内容（主要是实验结果，不必全部照抄实验要求文档中的内容。实验结果截图需按照顺序标号并给出标题，且给出简单文字说明。**

1、GPG4Win的下载、安装并简述GPG4Wi的基本功能

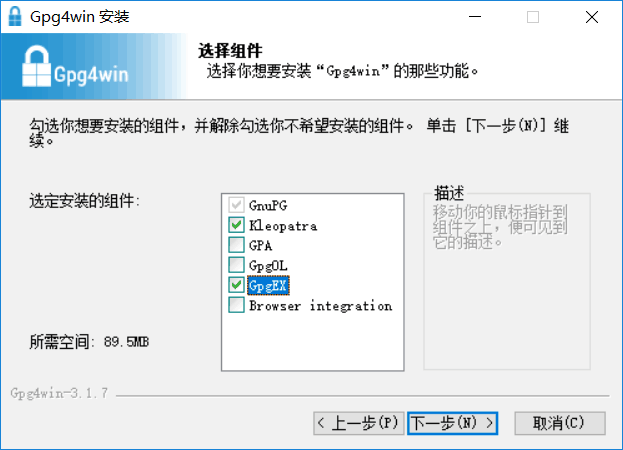
1. 下载

GPG4Win版本：3.1.7  

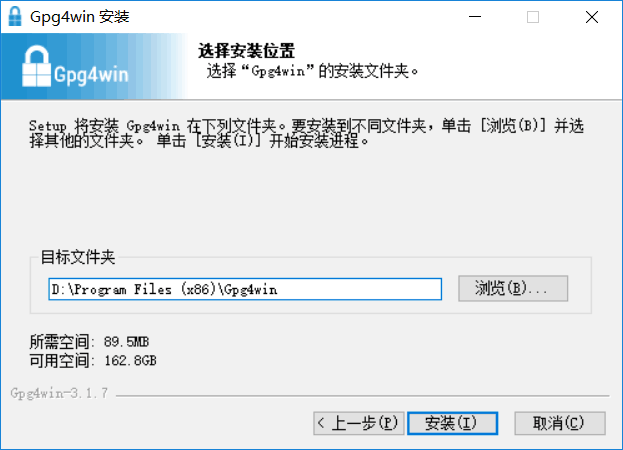

1. 安装
2. 选择语言：中文版本



1. 选择安装组件：Kleopatra、GpgEX



1. 选择安装路径：



1. 其他选择默认安装即可。
2. 简述GPG4Win的基本功能：

Gpg4win是一款基于GPG的非对称加密软件。非对称加密方式，简单理解就是用公钥加密文件，用私钥解密文件。如果你需要发送加密信息，首先获取接收者的公钥，然后利用该公钥加密后传递，对方利用对应的私钥就可解密。也就是说，公钥是锁，私钥是钥匙。非对称加密方式很好地解决了传递机密信息的问题。

2、配置雷鸟邮件客户端

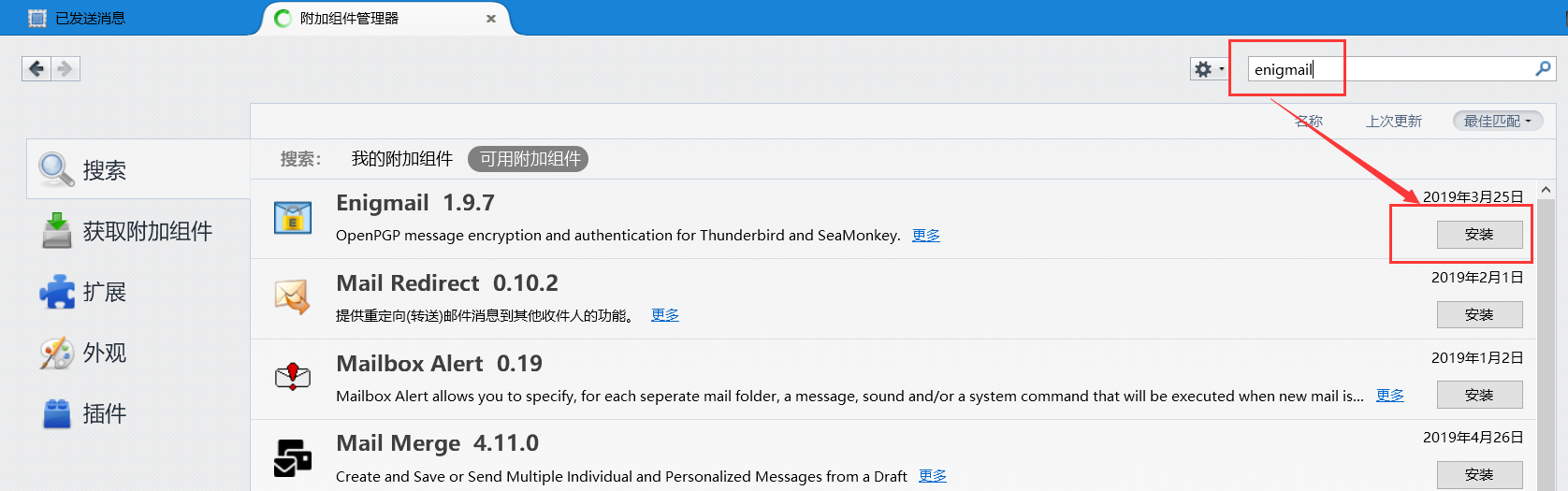
1. 在QQ邮箱中开启IMAP/SMTP服务：



1. 雷鸟邮件客户端关联QQ邮箱：

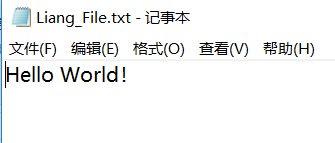


1. 安装enigmail插件：

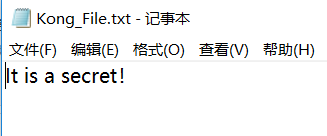


3、作者及结对伙伴各自的待加密文件介绍

1. 梁莉莉：Liang\_File.txt

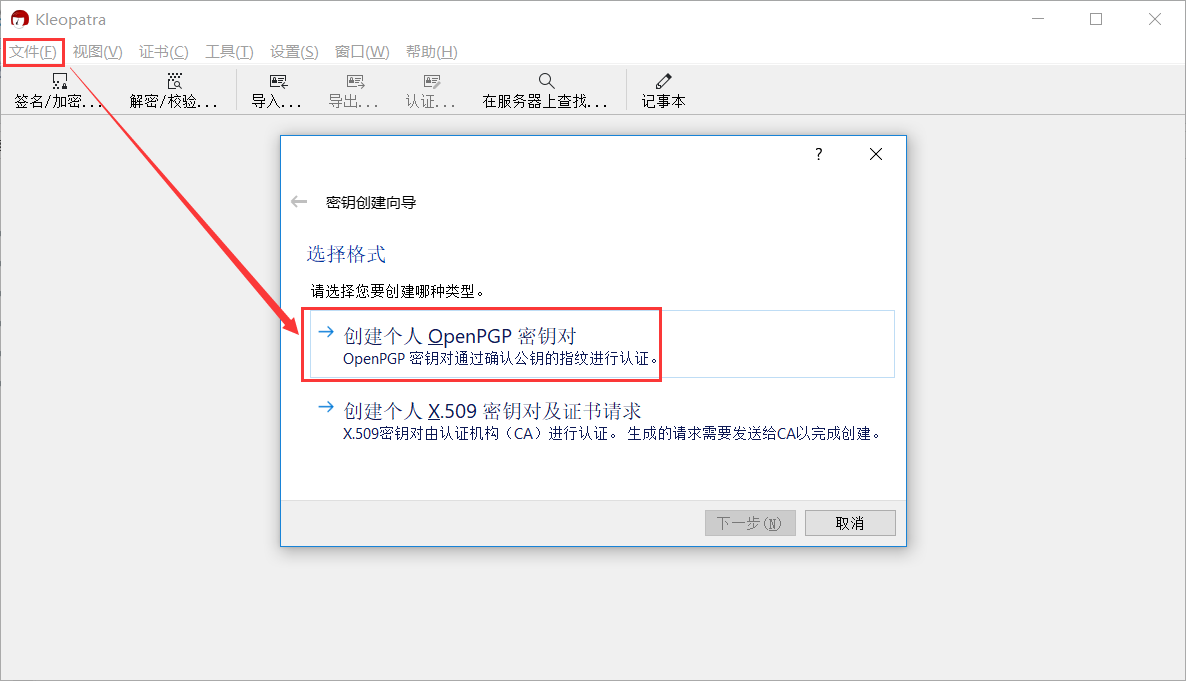


1. 孔一言：Kong\_File.txt

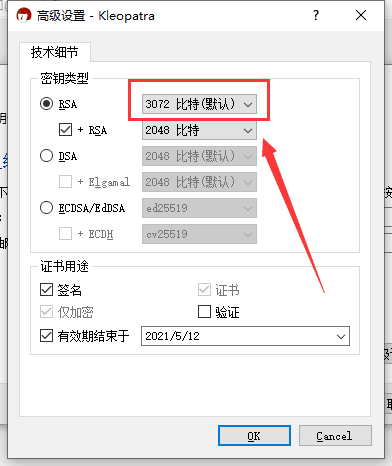


3、文件加解密及签名生成和验证

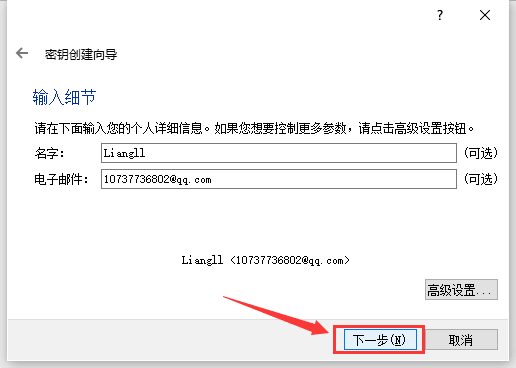
1. 使用Kleopatra生成公私钥对，导出公钥，与结对伙伴互换公钥：
2. 文件 → 新建密钥对 → 创建个人OpenPGP密钥对

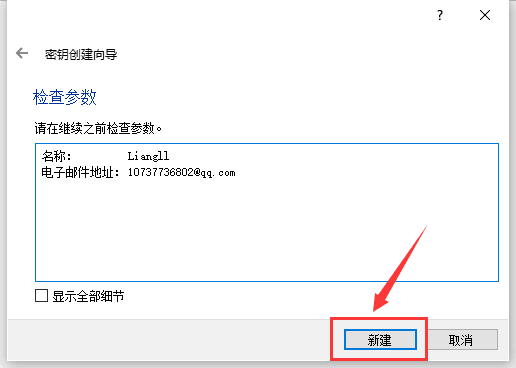


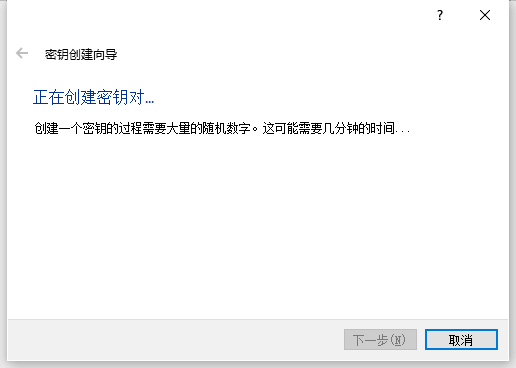
1. 在“高级设置”中选择RSA密钥类型为3072比特

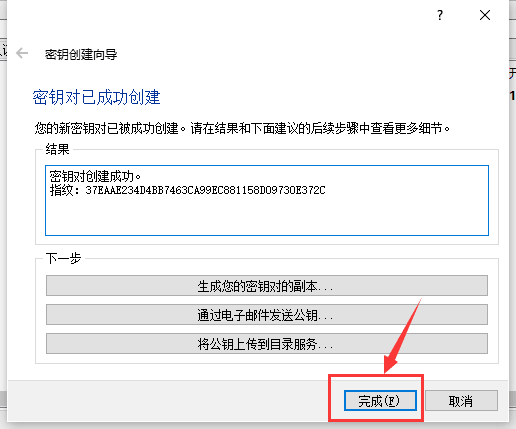


1. 填写个人姓名与邮件信息 → 新建 → 完成 即可：

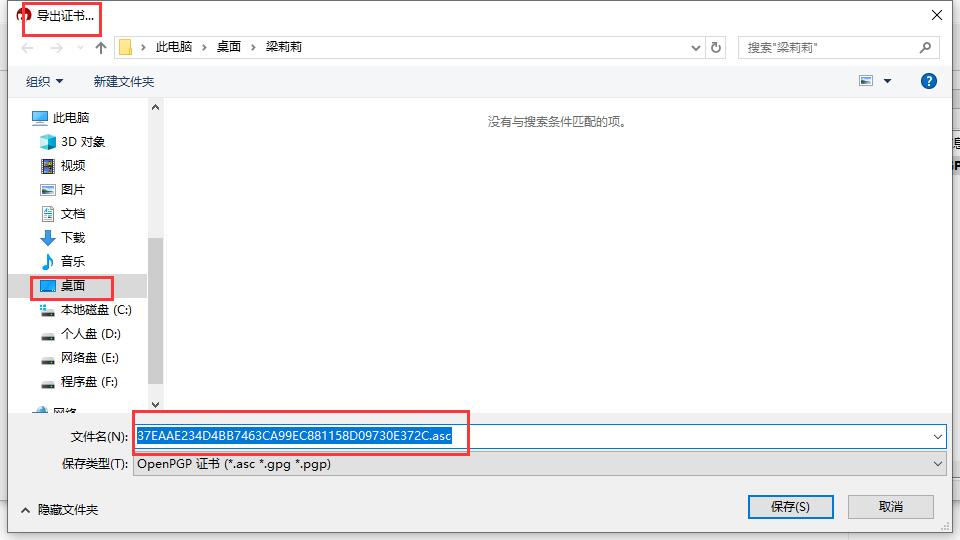






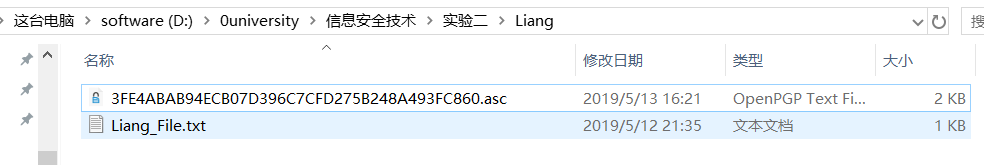


1. 导出公钥：

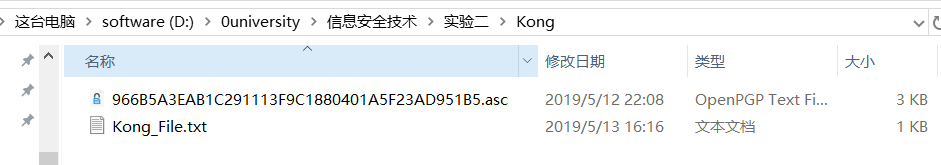


1. 作者与结对伙伴待加密文件及密钥介绍

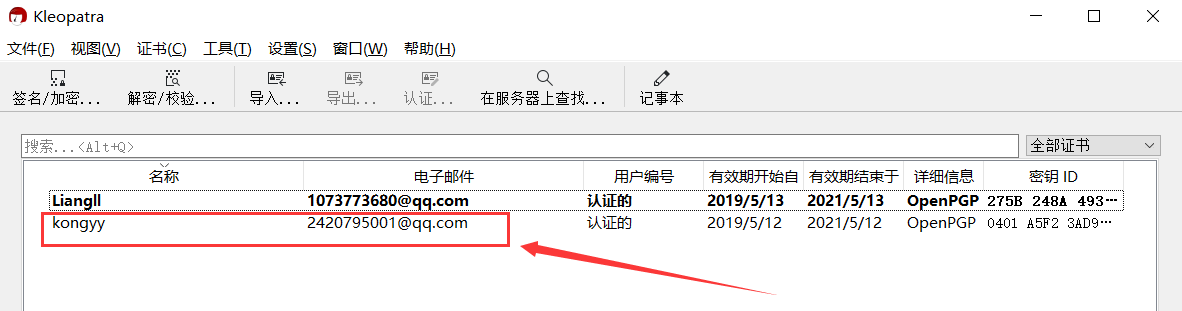
梁莉莉：



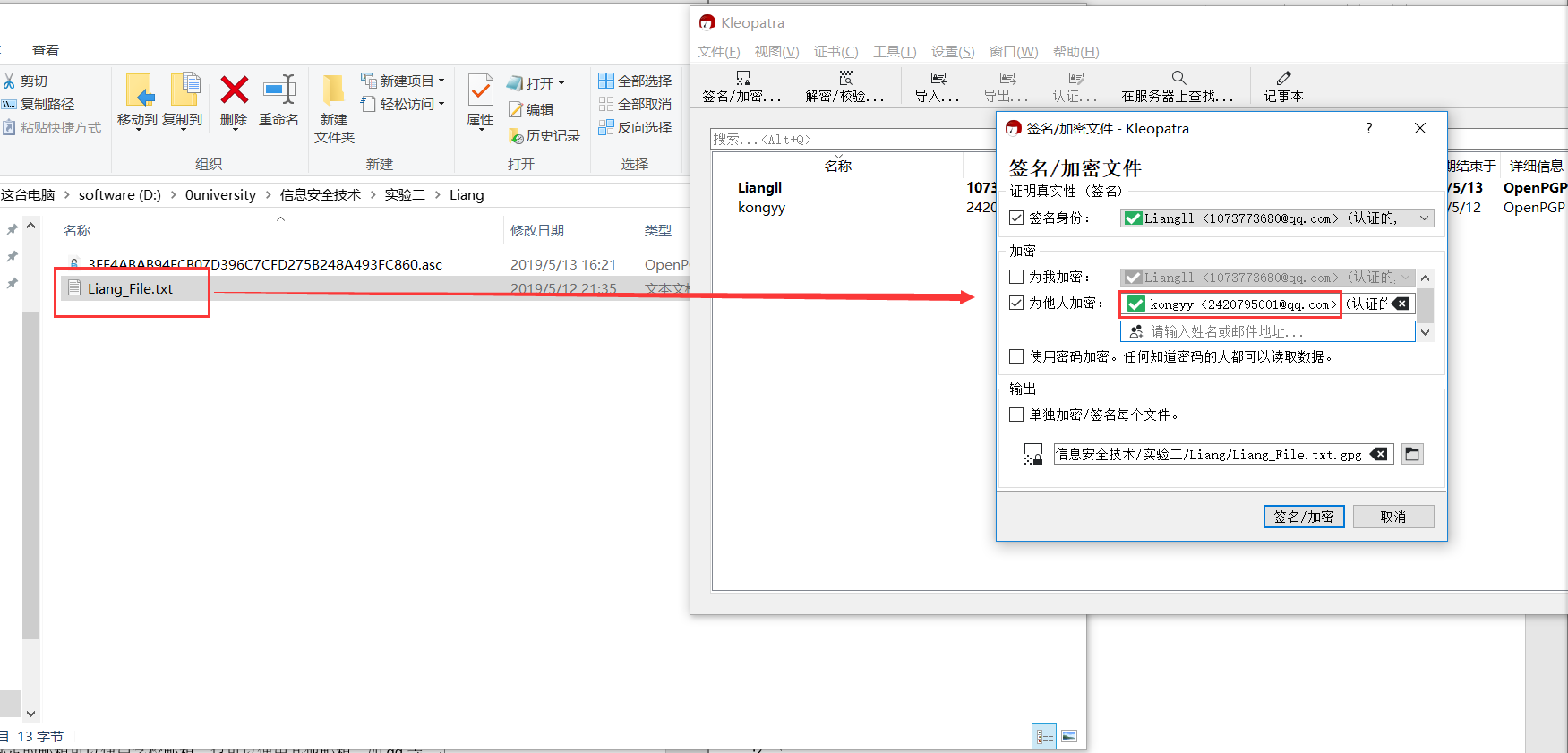
孔一言：



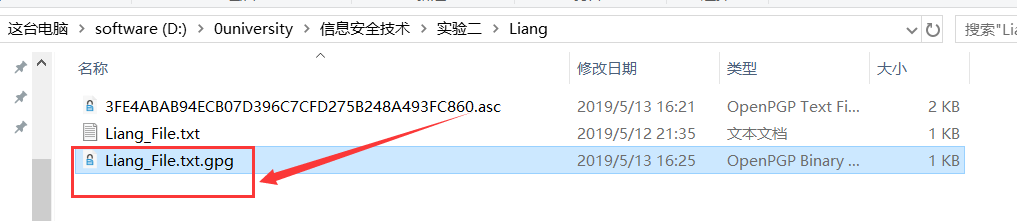
1. 利用结伴伙伴的公钥实现文件加密，并将加密的文件用邮件发送给伙伴，伙伴接收保存文件并利用自己的私钥解密文件
2. 在本机中导入对方公钥：

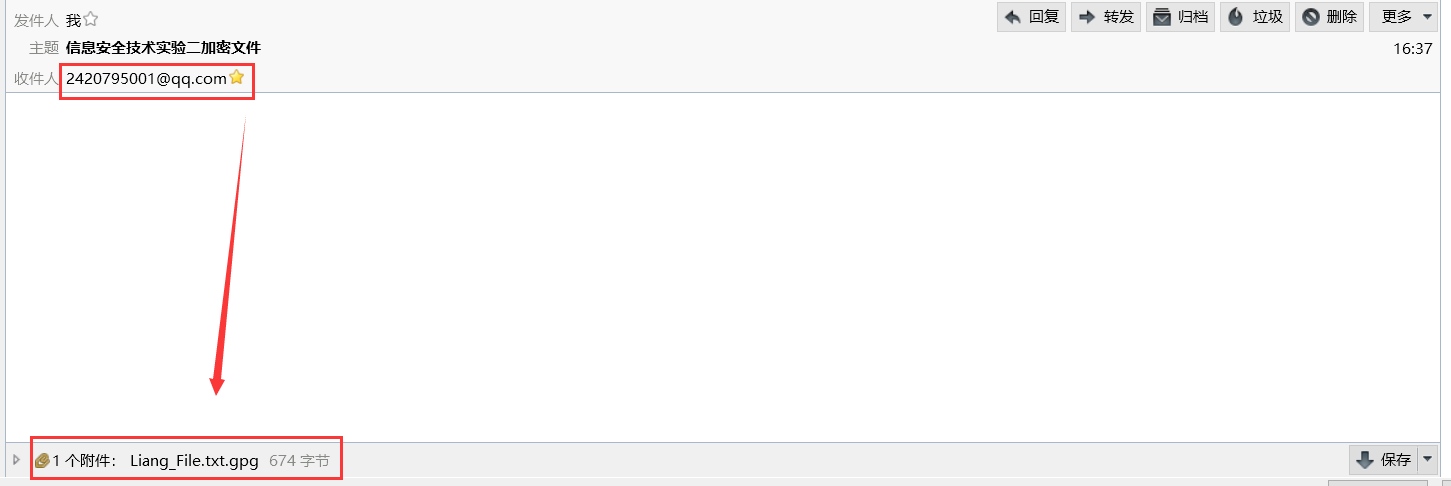


1. 使用对方的公钥实现文件加密：

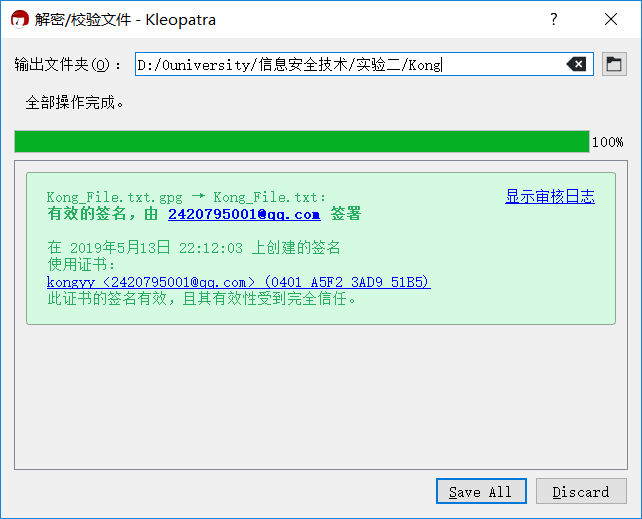


1. 生成加密文件并用邮件发送给对方：

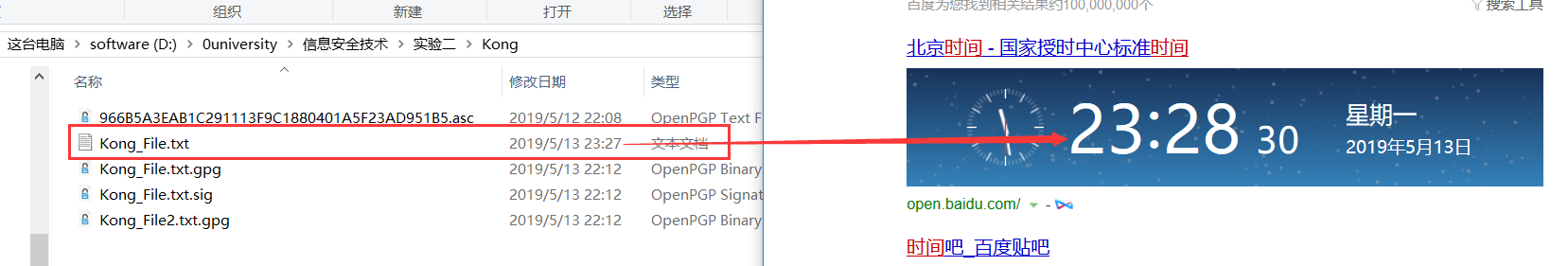


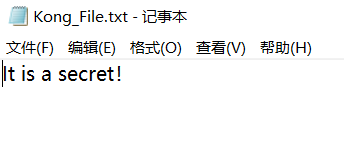


1. 接收对方的加密文件，并用自己的私钥解密文件：

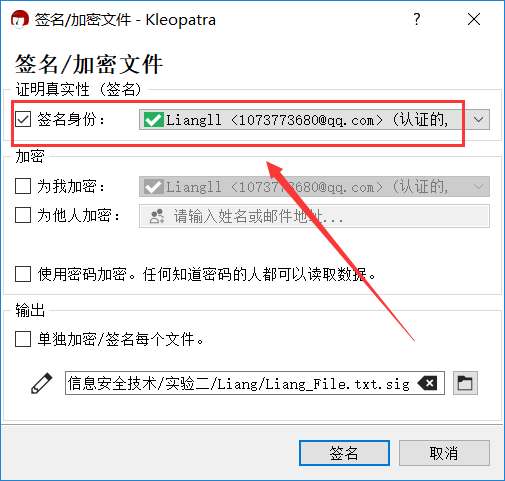


解密后的文件：

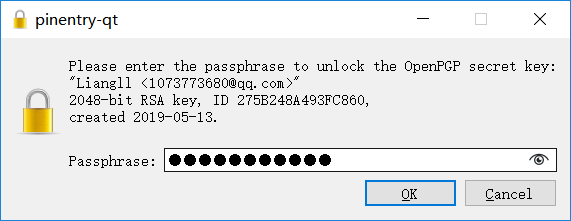




1. 使用自己的私钥生成文件的数字签名，并将签名文件发送给伙伴，伙伴利用发送方公钥可以验证签名
2. 生成文件的数字签名：



1. 输入密钥口令：

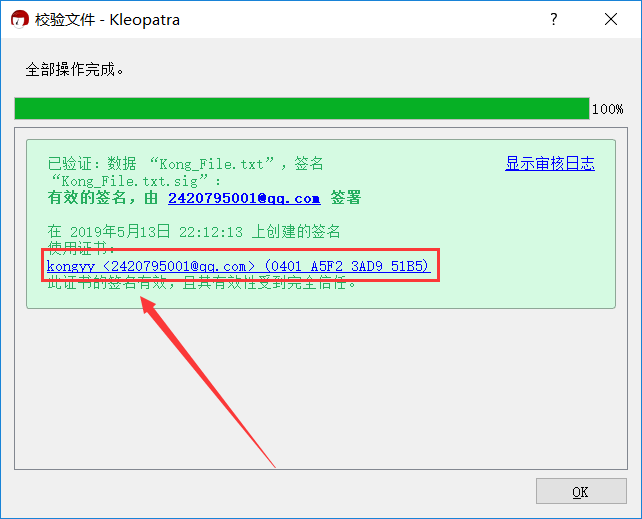


1. 将签名文件发送给对方：

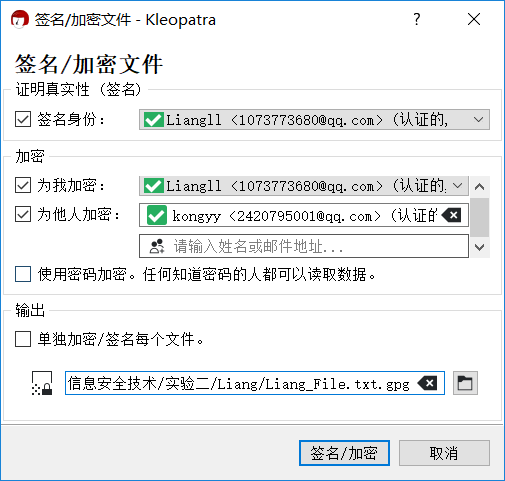


1. 利用发送方的公钥验证对方的文件签名：

操作文件：Kong\_File.txt.sig



1. 同时实现加密和签名：
2. 生成加密签名文件：

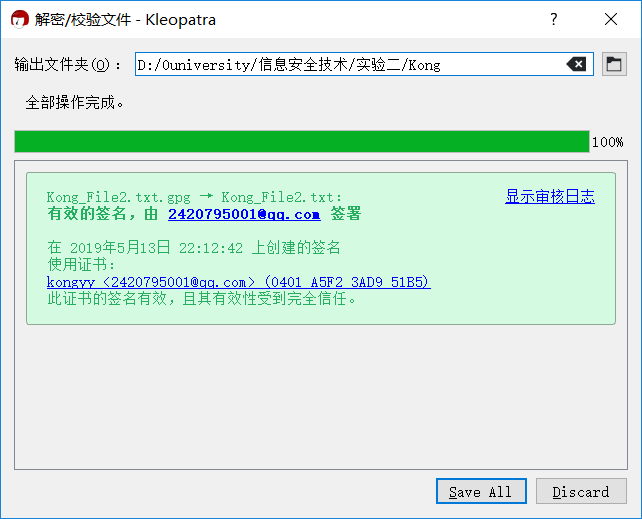


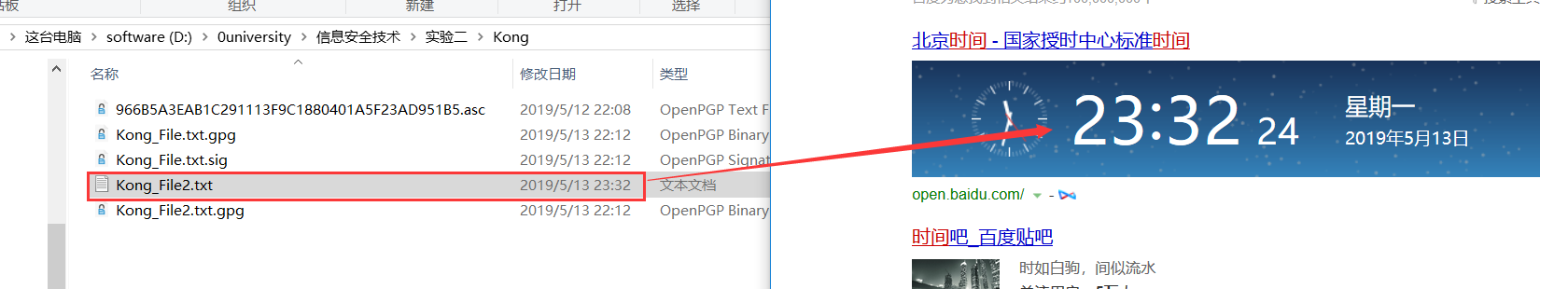
1. 将签名文件发送给对方：

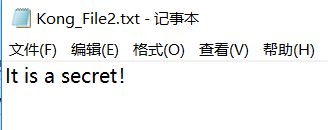


1. 解密对方发送的加密文件：

操作文件：Kong\_File2.txt.gpg

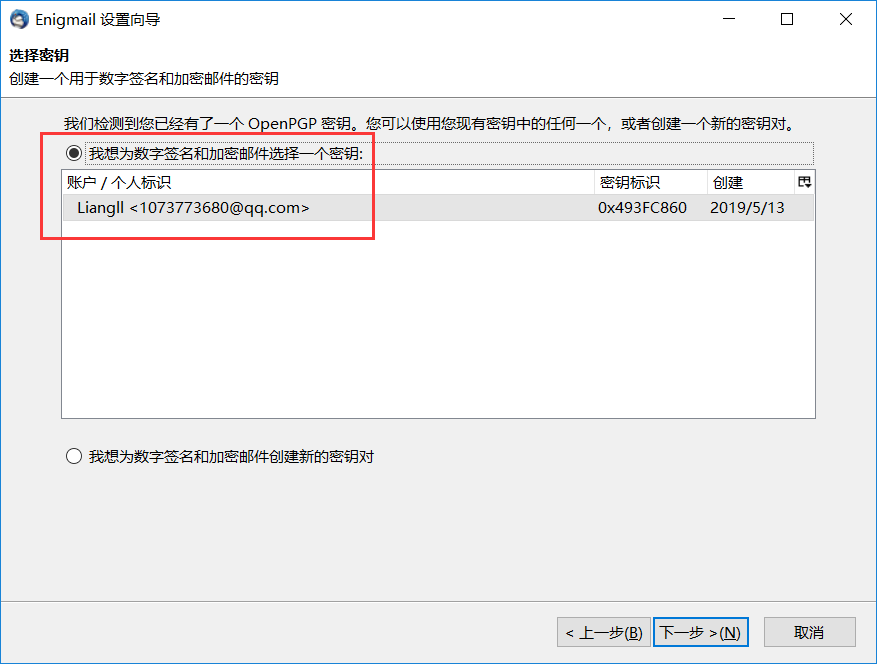




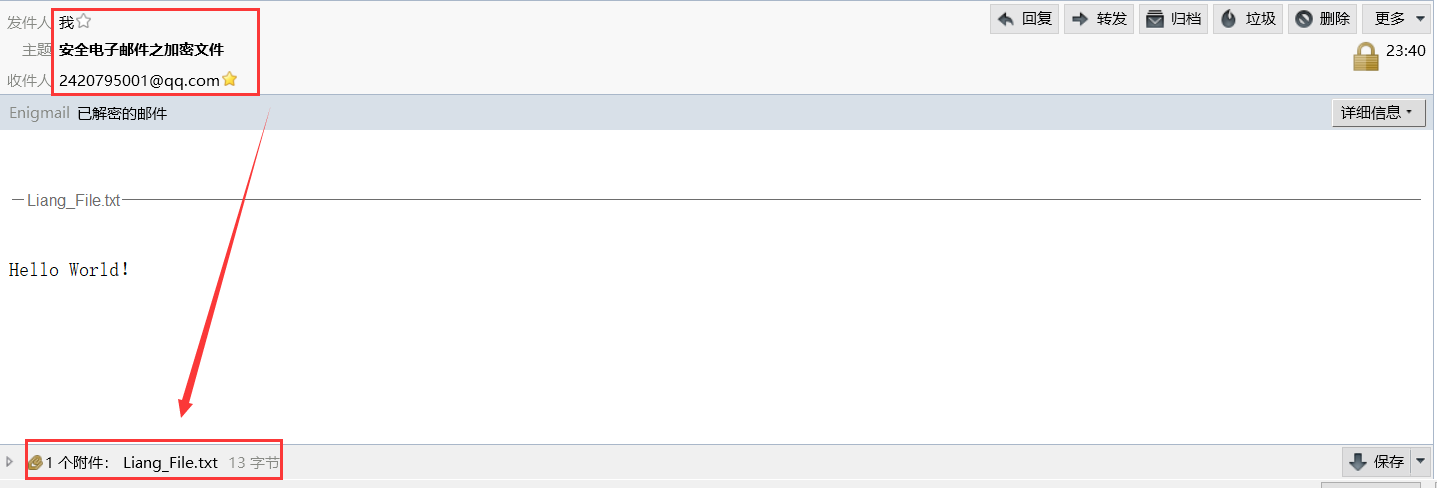


3、 安全电子邮件

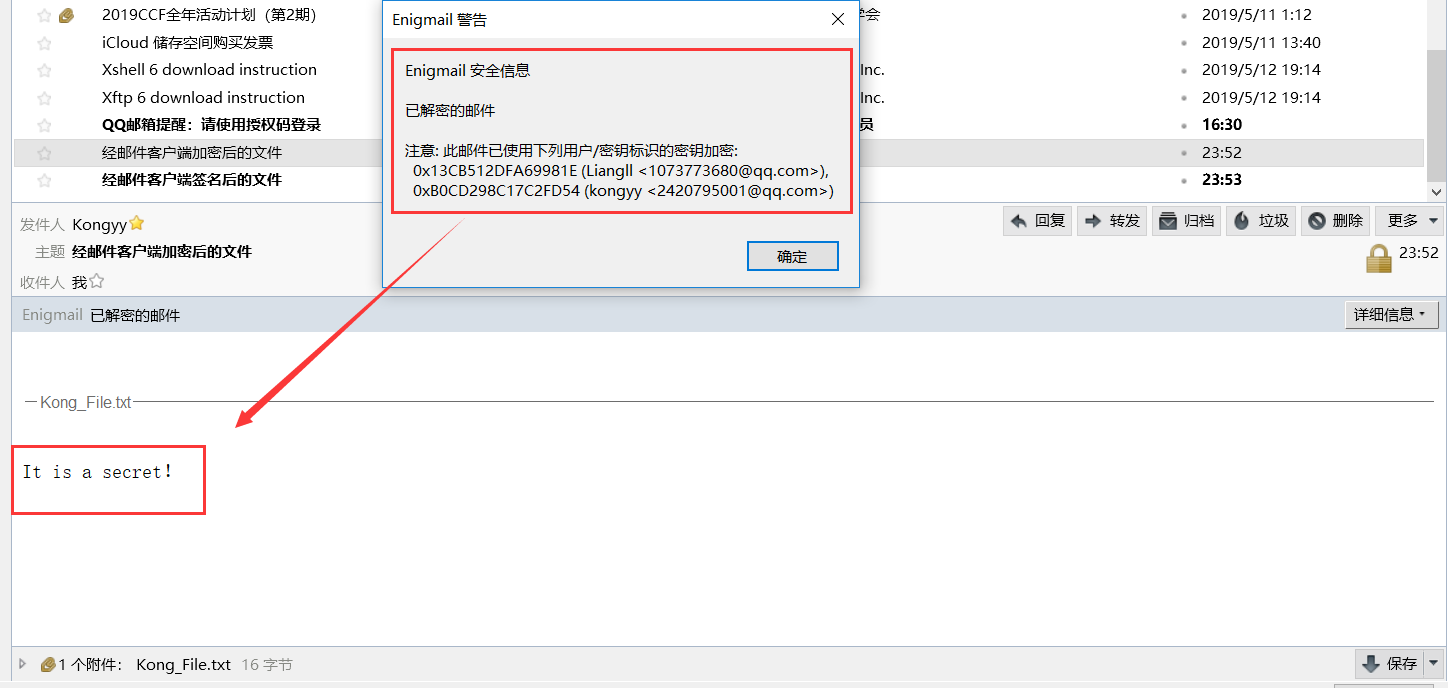
基本配置：



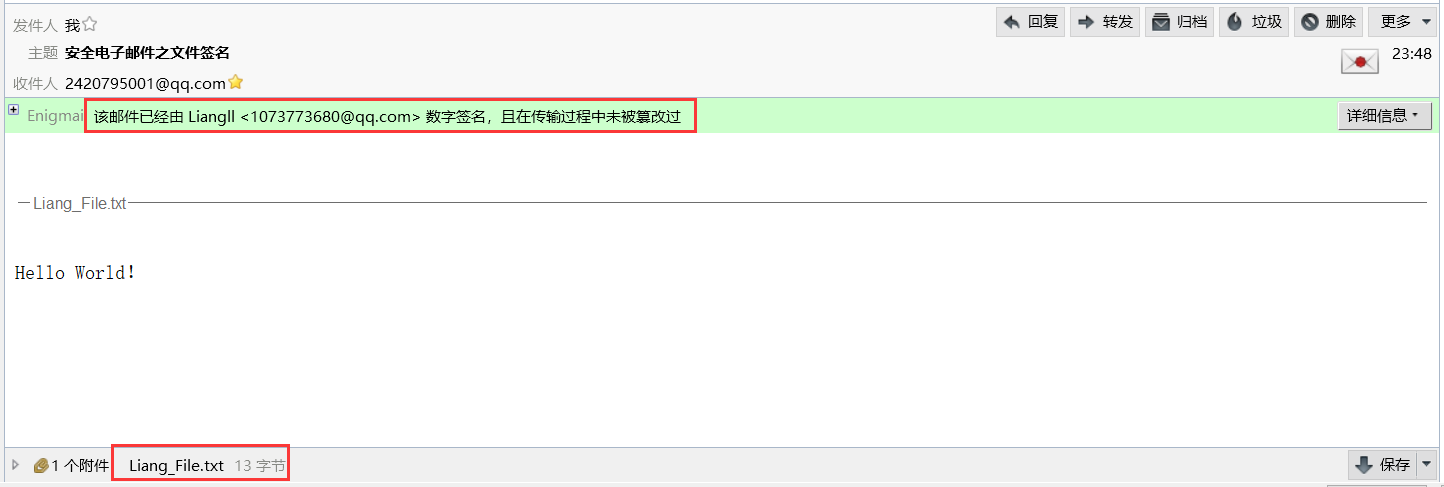
1. 使用类似的过程实现加密邮件（直接加密邮件内容，而不是用附件发送加密文件）的发送和接收
2. 发送：



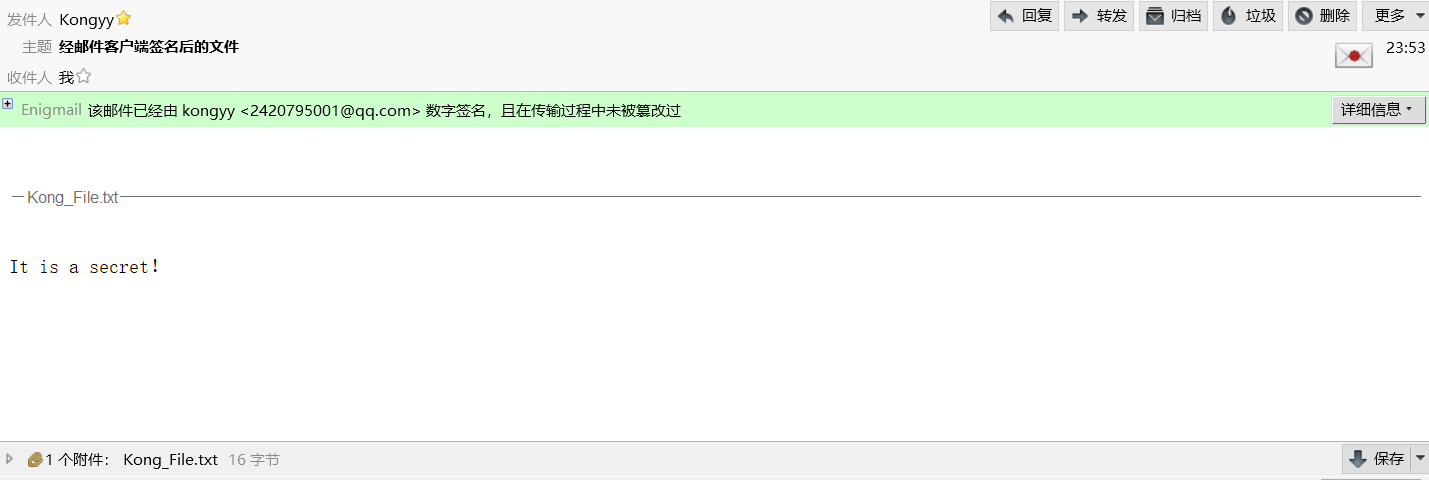
1. 接收对方的文件并解密：



1. 带有数字签名的邮件发送以及签名的验证
2. 发送：



1. 接收对方的签名文件：



**四、实验总结（此部分必须有）**

可以是实验中遇到的问题，问题的解决方法以及收获等。