基于GPG4Win的加解密实验

**实验目的**：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。

实验内容：结对实验，实验内容包括以下三个部分：

1. GPG4Win的下载、安装并简述GPG4Wi的基本功能；

https://www.gpg4win.org/

2. 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）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。

（3）类似的方法可以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。

（4）也可以同时实现加密和签名（这部分因为步骤和（2）（3）两步骤非常类似，可以选作）

以上步骤中请注意公私钥对的使用。

以上实验可以参考百度文库：基于GPG4Win的文件加解密

<https://wenku.baidu.com/view/91b707f4f90f76c661371a6c.html>

3. 安全电子邮件

（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）带有数字签名的邮件发送以及签名的验证。

以上两个步骤和文件加解密和数字签名是类似的。

主要问题可能在于邮件客户端软件的使用。

（1）配置邮件客户端，可以使用outlook，或者雷鸟邮件客户端软件（bb平台已提供），并绑定邮箱。绑定的邮箱可以使用学校邮箱，也可以使用其他邮箱，如qq等。

a. qq邮箱的客户端配置，可以参见: <https://service.mail.qq.com/cgi-bin/help?subtype=1&&no=371&&id=28>。

b.可能遇到的问题包括qq邮箱或其他邮箱的授权码，可以参见：<https://service.mail.qq.com/cgi-bin/help?subtype=1&&no=1001256&&id=28>

提交实验报告：结对伙伴每人提交自己的实验报告文档。按照实验模板，给出具体实验内容，包括：结对伙伴姓名学号，上述实验步骤的操作及实现结果在截屏（仅包括自己部分即可）和实验总结（必须有）。