**西安电子科技大学**

**《PGP邮件加密实验》 课程实验报告**

网络与信息安全 学院 2118021 班

成 绩

姓名 盖乐 学号 21009200991

同作者

实验日期 2024 年 5 月 31 日

|  |
| --- |
| 指导教师评语：  指导教师：  年 月 日 |
| **实验报告内容**  一、实验目的  二、实验所用仪器（或实验环境）  三、实验基本原理及步骤（或方案设计及理论计算）  四、实验数据记录（或仿真及软件设计）  五、实验结果分析及回答问题（或测试环境及测试结果） |

一、实验目的

1.熟悉非对称加密算法

2.掌握私钥和公钥再签名和加密中的应用

3.了解PGP工具的操作

二、实验所用仪器（或实验环境）

PGP658

windows7虚拟机

windows10主机

三、实验基本原理及步骤（或方案设计及理论计算）

PGP加密系统是采用公开密钥加密与传统密钥加密相结合的一种加密技术。它使用一对数学上相关的钥匙，其中一个(公钥)用来加密信息，另一个(私钥)用来解密信息。PGP采用的传统加密技术部分所使用的密钥称为“会话密钥”(sek)。每次使用时，PGP都随机产生一个128位的IDEA会话密钥，用来加密报文。公开密钥加密技术中的公钥和私钥则用来加密会话密钥，并通过它间接地保护报文内容。

PGP中的每个公钥和私钥都伴随着一个密钥证书。它一般包含以下内容:

1)密钥内容(用长达百位的大数字表示的密钥)

2)密钥类型(表示该密钥为公钥还是私钥)

3)密钥长度(密钥的长度，以二进制位表示)

4)密钥编号(用以唯一标识该密钥)

5)创建时间

6)用户标识（密钥创建人的信息，如姓名、电子邮件等)

7)密钥指纹(为128位的数字，是密钥内容的提要表示密钥唯一的特征)

8)中介人签名(中介人的数字签名，声明该密钥及其所有者的真实性，包括中介人的密钥编号和标识信息)

PGP把公钥和私钥存放在密钥环(KEYR)文件中。PGP提供有效的算法查找用户需要的密钥。PGP在多处需要用到口令，它主要起到保护私钥的作用。由于私钥太长且无规律，所以难以记忆。PGP把它用口令加密后存入密钥环，这样用户可以用易记的口令间接使用私钥.PGP的每个私钥都由一个相应的口令加密。

PGP主要在3处需要用户输入口令:

需要解开收到的加密信息时，PGP需要用户输入口令，取出私钥解密信息当用户需要为文件或信息签字时，用户输入口令，取出私钥加密

对磁盘上的文件进行传统加密时，需要用户输入口令

公钥、私钥加密特性

在PGP系统里经常遇到公钥、私钥，大家如果不理解就无法使用了。公钥、私钥只是个代号而已，我们这里称它们为a钥、b钥。a、b 钥就像一对密码本，但是它很特殊:

1)用a加密的东西只能用b来解，b加密的东西只能用a解。

2) a不能解密a自己加密的东西。b不能解密b自己加密的东西。

3) a有且仅有一个b与自己配对。b有且仅有一个a与自己配对。不存在第

三者。

如果我们把a留给自己用，把b发给大家（别人)，那a就称为“私钥”()，b就称为“公钥”。当然，反过来那b就称为“私钥”，a就称为“公钥”。系统只是自动给了个名称，防止你以后乱不清到底是把 a当公钥发给别人了，还是把 b当公钥发给别人了。

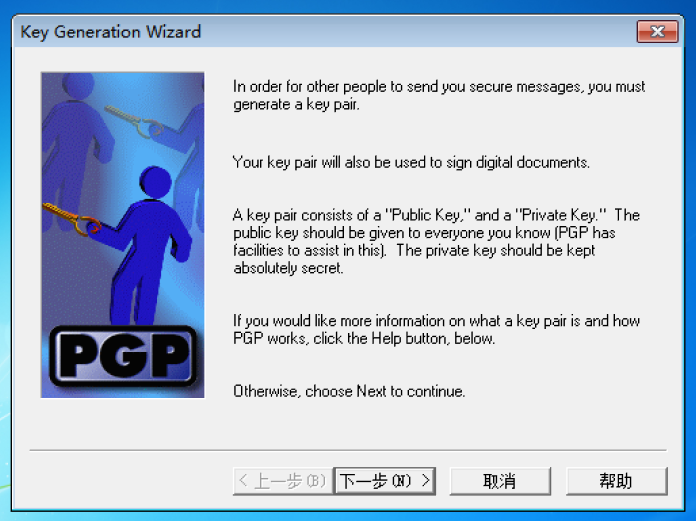
四、实验数据记录（或仿真及软件设计）

(一)PGP的使用

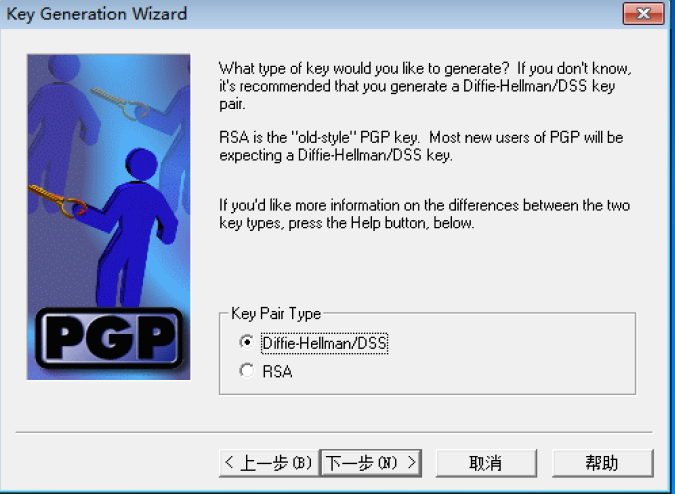
1，首先使用PGP生成创建密钥对及导出公钥和签名

打开开始菜单→程序→PGP，启动PGP。

打开File菜单下的NEWPGPKEY启动新密钥向导对话框，按如下图示生成公钥

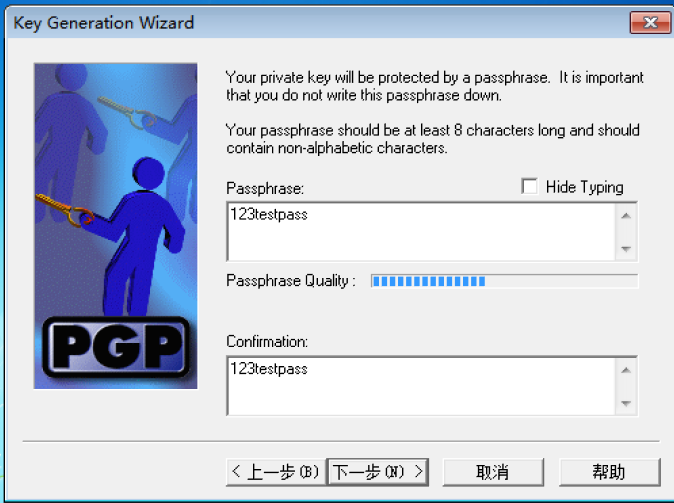


2.输入全名和和邮件地址实验，[单击下一步。](mailto:15145120182@163.com，单击下一步。)

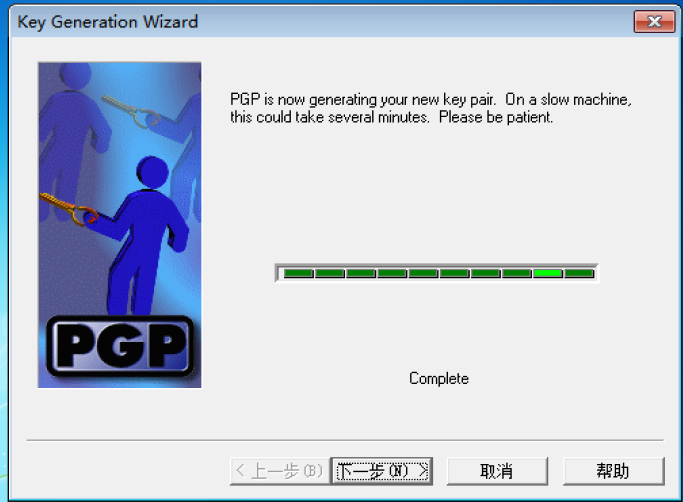




3.在要求输入 passphrase 的对话框中，我们以 123testpass 作为自己私钥的密码



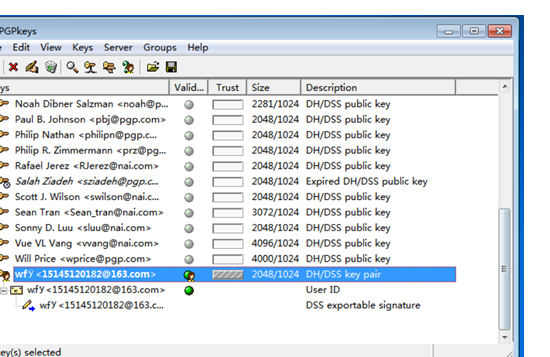
4.在 PGP 完成创建密钥对后，单击下一步,完成



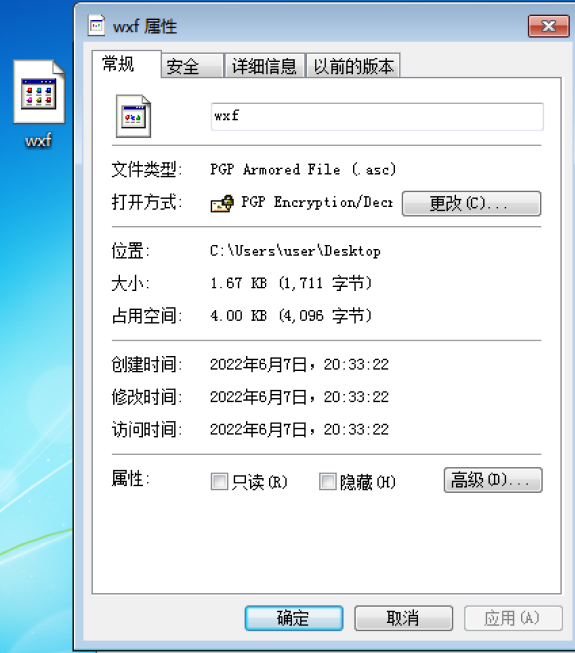




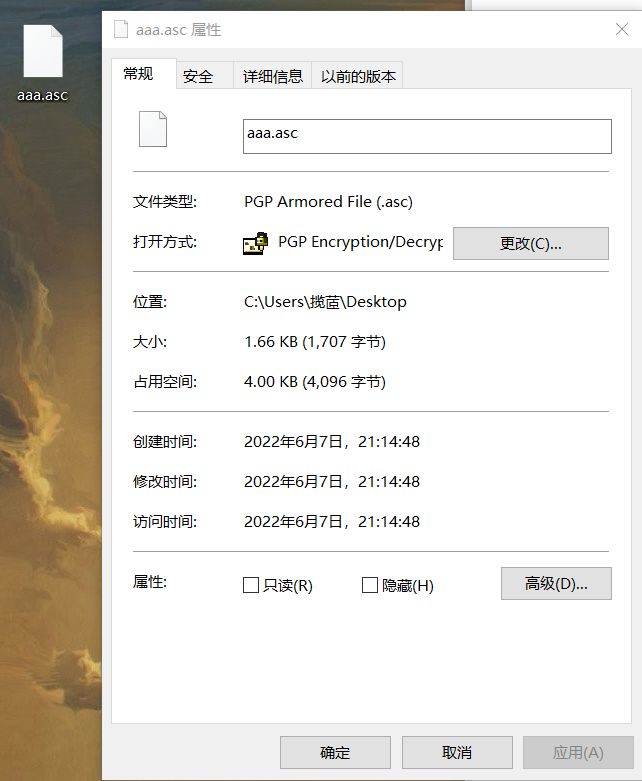
5.打开 PGP 的主界面，可以看见我们刚才创建的密钥



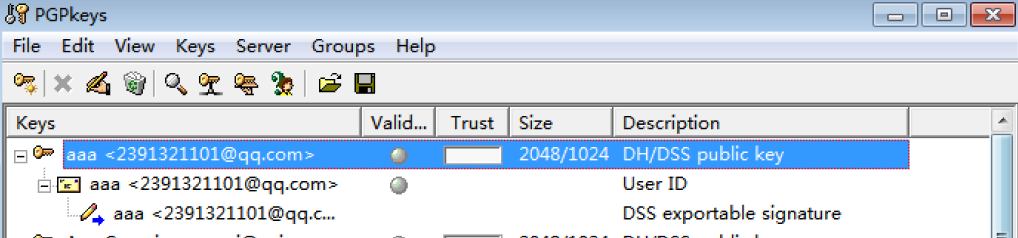
6.打开 File 菜单Export>Key 导出公钥，在 Export Key to File 对话框中，以 默认的文件名 wxf.asc 保存在桌面上:

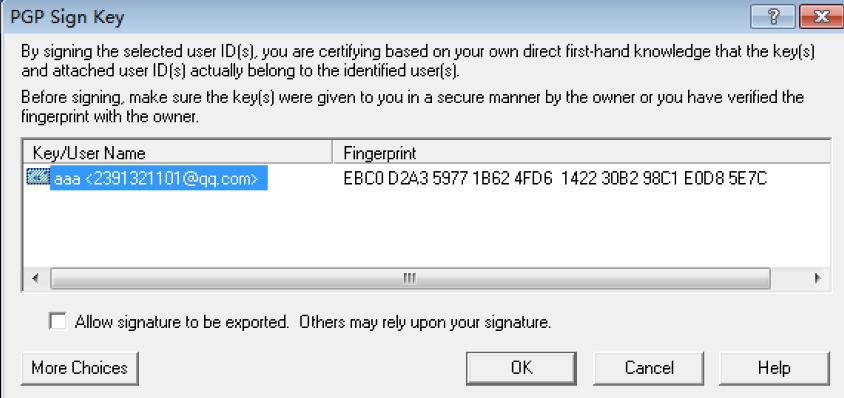


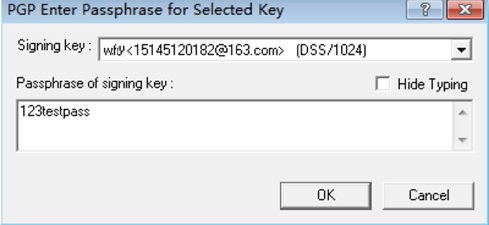
7.切换到另一台计算机，我们以相同的方式来创建另一对新密钥并且将其导 出。我们输入 aa 作为全名，2391321101@qq.com（根据自己拥有的实际邮箱地址 填写）作为邮件地址，导出的公钥文件名为 aaa.asc。步骤和前面的一样。

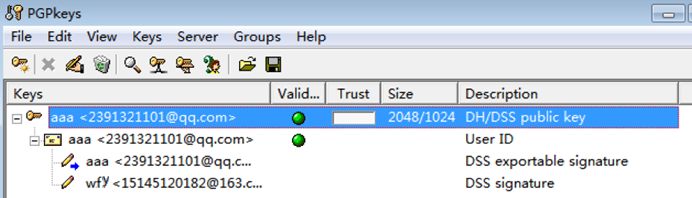


8．接下来我们来对导出的密码进行导入，打开 File 菜单，选择 Import ,在 Select File Containing Key 对话框中，选择另一台计算机的公钥文件（aaa.asc），然后 单击打开按钮（假设我们已经将两台计算机的公钥都通过共享的方式复制了桌面）,在弹出的 Select key(s)对话框中，选中要导入的公钥文件，然后单击 Import， 返回到主界面后会看见多了一个密钥，证明刚才的密钥已经导入成功了。

9.打开 Keys 菜单，选择 Sign，对导入进来的公钥进行签名确认。选中刚才导入的公钥文件（aaa），单击 OK 按钮。

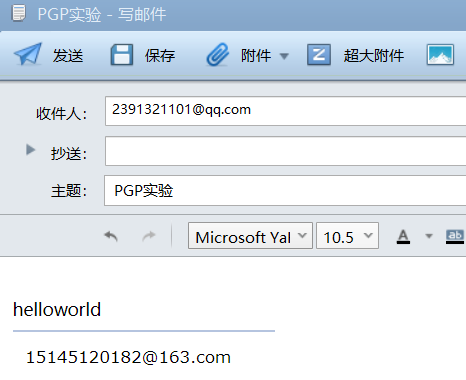




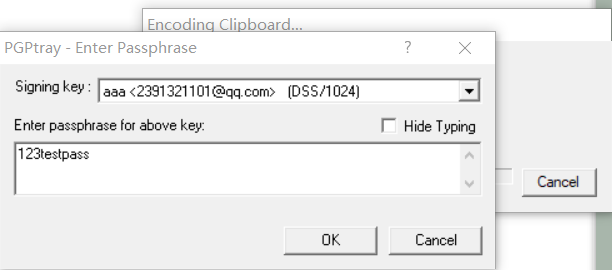


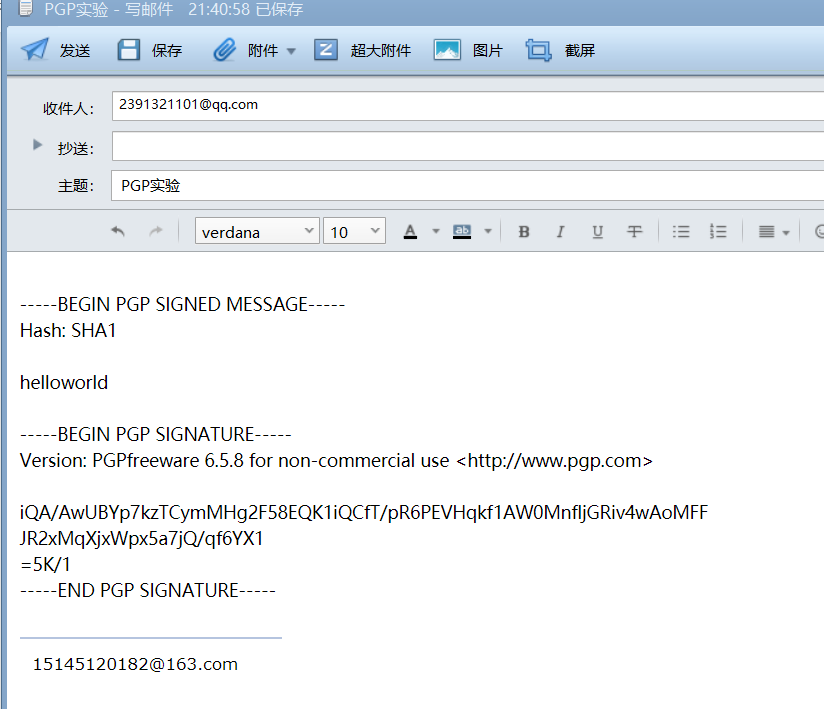
10。切换回第一台计算机，以相同的方式将第二台计算机的公钥(bill.asc)导入并签名。用 PGP 加密邮件，并发送邮件。

1. 打开foxmail，点击创建新邮件，撰写一封邮件。

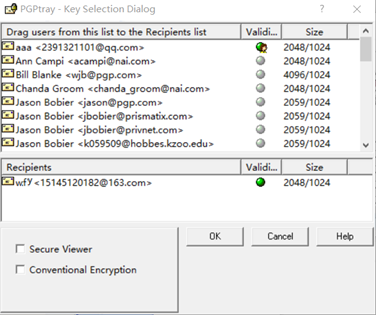


12．在发送之前，对邮件内容进行签名，如下图所示选择 Sign

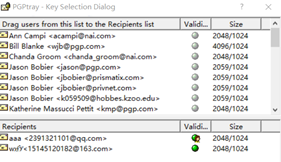




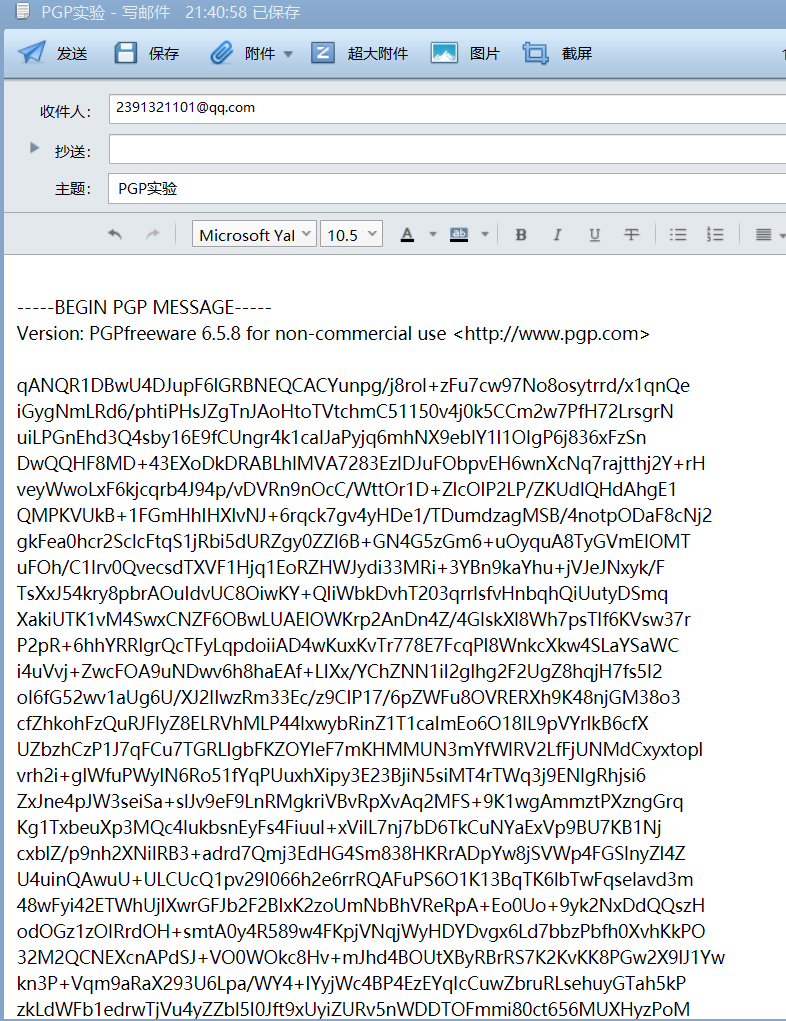
13.对邮件内容加密：按下图所示选择 Encrypt



14.将 aaa 拖到下面的窗口，如下图：



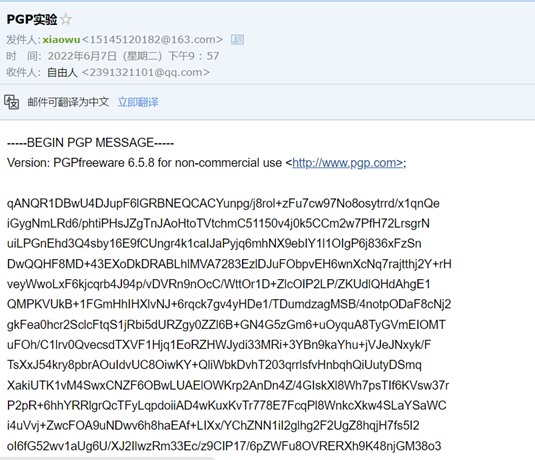
15．按 OK 键后就对邮件加密，如下图：



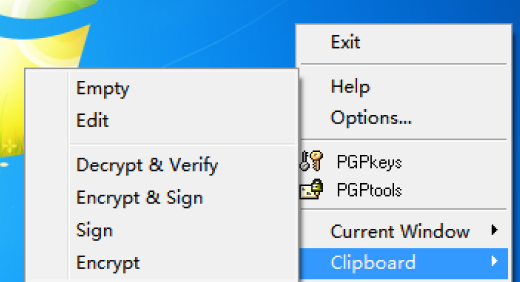
16．按发送键发送邮件。

17．转到另一台计算机继续实验。

邮件成功收到



18．aa 需要对加密邮件进行解密和验证签名，按下图所示选择 Descrypt & Verify



19．输入私钥：123testpass，按 OK 键进行解密和验证签名

