软件学院

实验报告书

课 程 名 ： 网络安全技术

题　　目： PGP 软件应用实验

实验类别 【验证】

班　　级： 信息安全 193 班

学　　号： 8003119100

姓　　名： 丁俊

同组试验人姓名:

评语：

实验态度：认真（　）　一般（　）　较差（　）
实验结果：正确（　）　部分正确（　）错（　）
实验理论：掌握（　）　熟悉（　）　了解（　）生疏（　）
操作技能：较强（　）　一般（　）　较差（　）
实验报告：较好（　）　一般（　）　较差（　）

成绩：　　指导教师： 鄢志辉

1 实验内容或题目

使用 PGP 软件加解密文件，并进行数字签名。加深对非对称算法(RSA)的认识，并对公开密钥密码体制应用有较深刻的理解。

2 实验目的与要求

（1）掌握 PGP 软件产生密钥的过程。

(2) 导入对方公钥操作过程，掌握 PGP 软件加解密的方法。

（3）掌握 PGP 软件进行数字签名和验证的方法。

(4) 创建 PGPdisk 加密文件

3 实验步骤

（1）两人一组进行人员安排。

每个组内自行组成两人一个实验组，完成一次实验后，**双方交换再进行一次。**

（2）每台机器上安装 PGP 软件，熟悉 PGP 界面；

3.1 生成和导入密钥

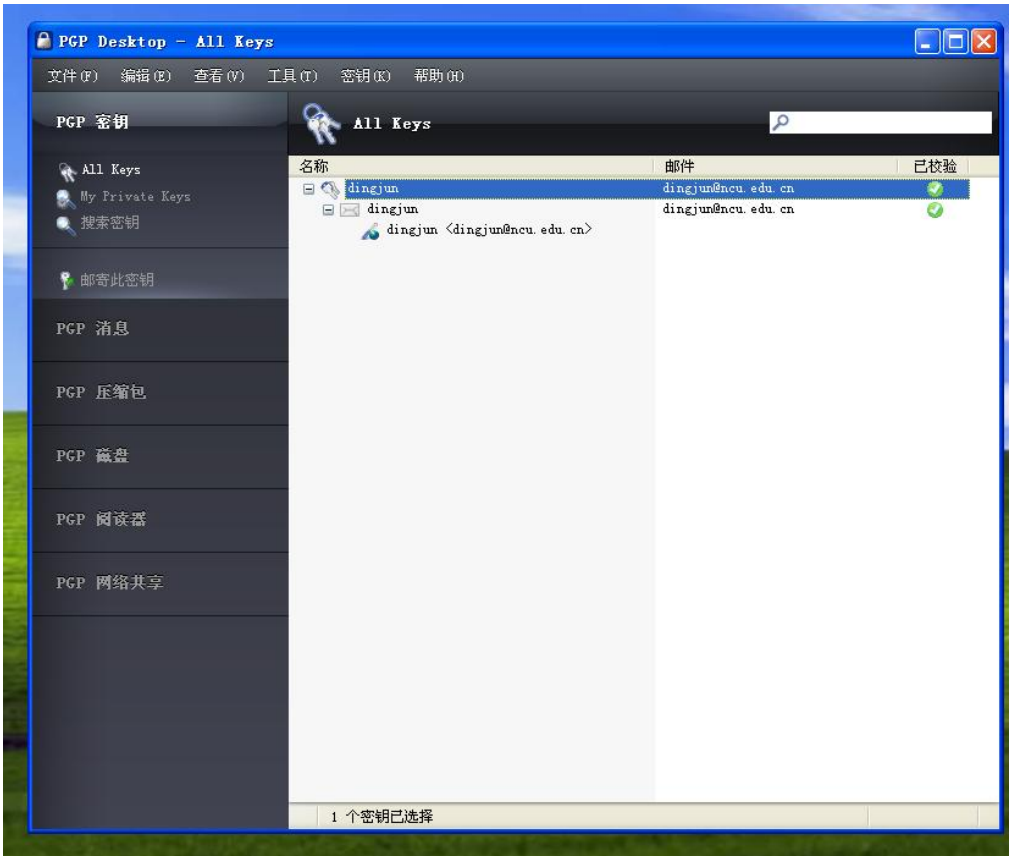
首先，要生成一对公钥和私钥。私钥接收方自己保管，而公钥公开。发送方用接收方的公钥加密文件，而接收方用自己的私钥解密。

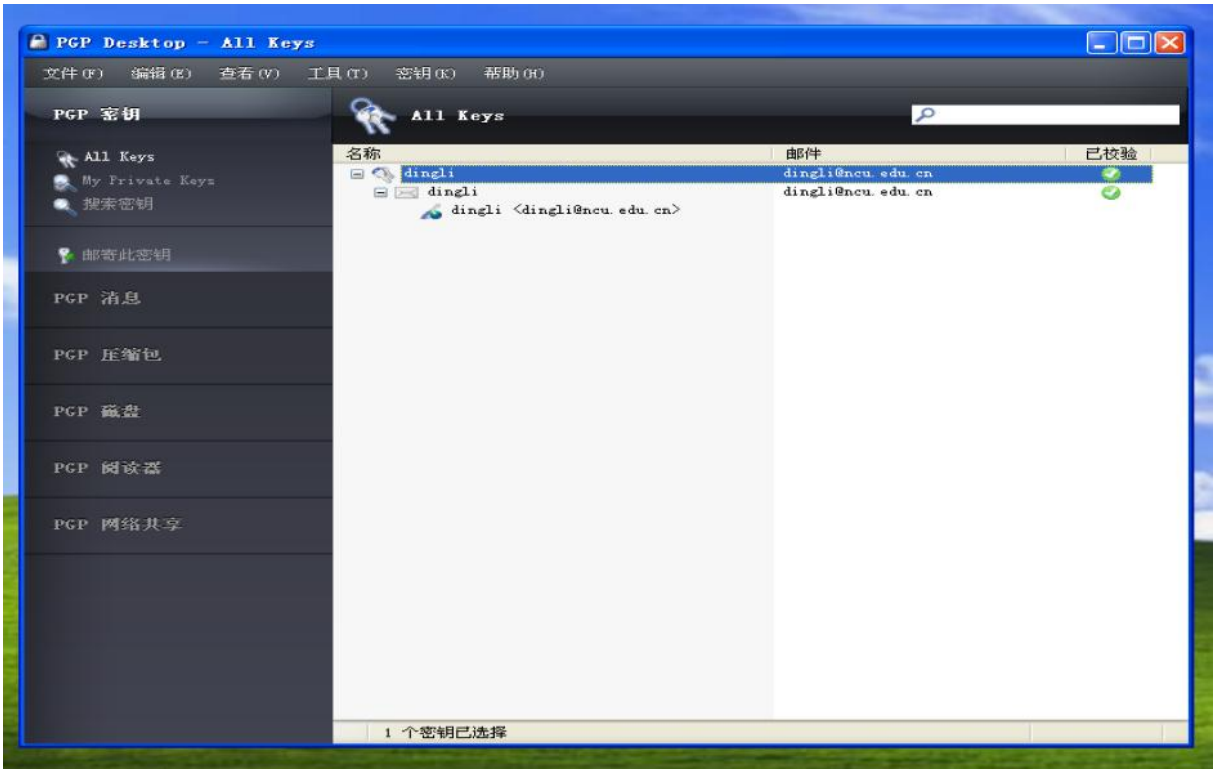
A 机器和 B 机器各自都生成一对加密和解密用的公钥和私钥文件，并分别保存好，文件名为张三加密公钥，张三解密私钥，密钥全名：张三加解密　Email 地址：张三加解密@ncu.edu.cn

A 机器和 B 机器各自都生成另一对数字签名用的公钥和私钥文件，并分别保存好。文件名为张三签名公钥，张三签名私钥，密钥全名：张三签名　Email 地址：张三签名@ncu.edu.cn

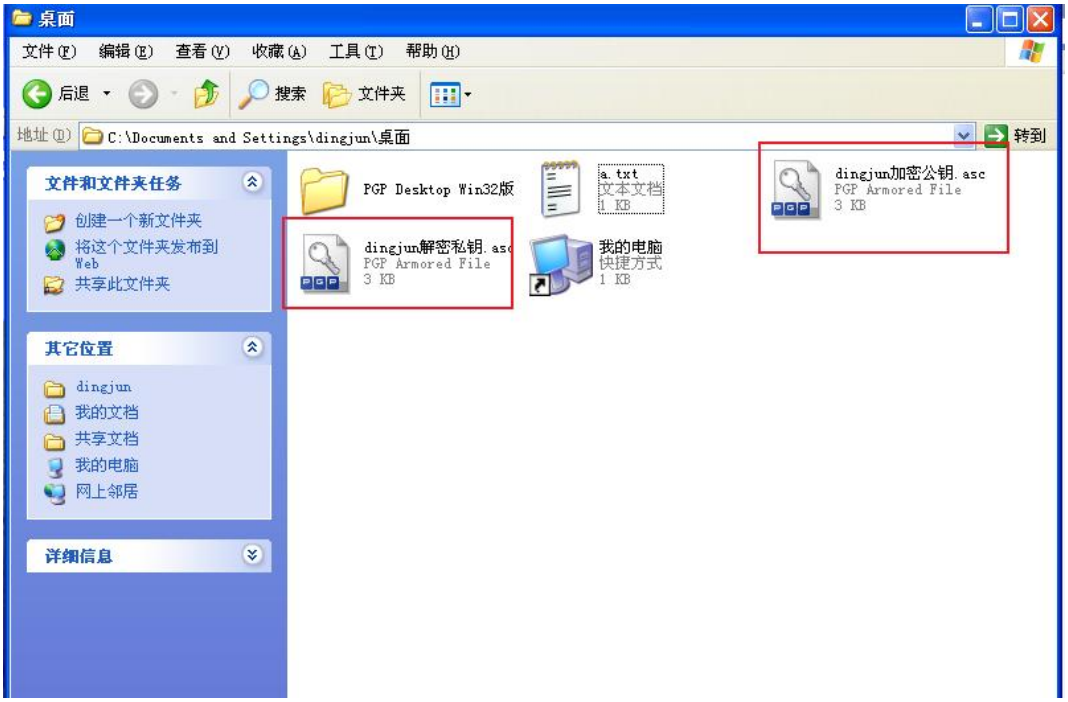
测试数据与实验结果（抓图粘贴，列出详细步骤）:

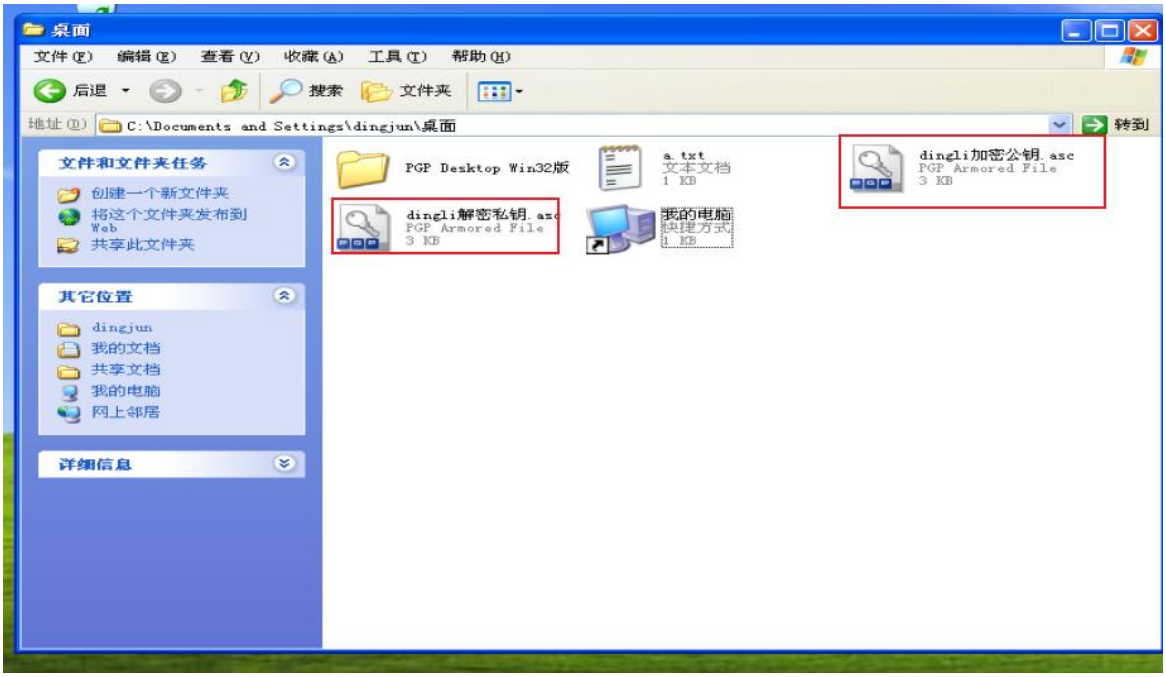
1、A 机器新建 PGP 密钥，用户名为 yangyang（杨洋），Email 地址：yangyang@ncu.edu.cn。B 机器新建 PGP 密钥，用户名为 yangtao（杨涛），Email 地址：yangtao@ncu.edu.cn。



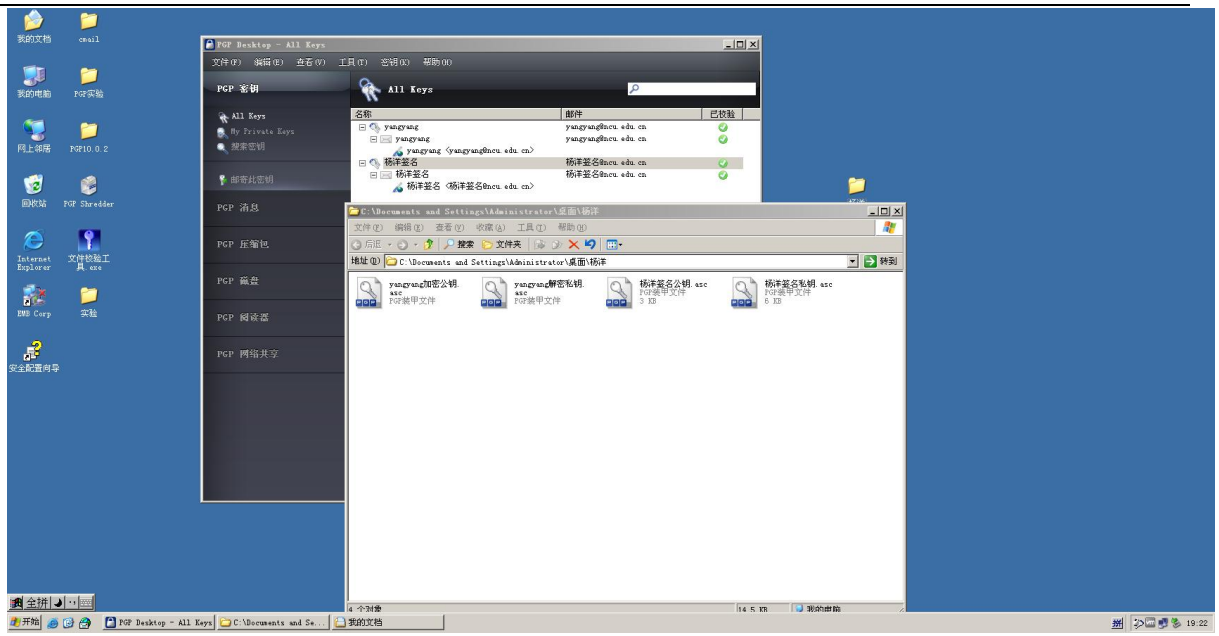


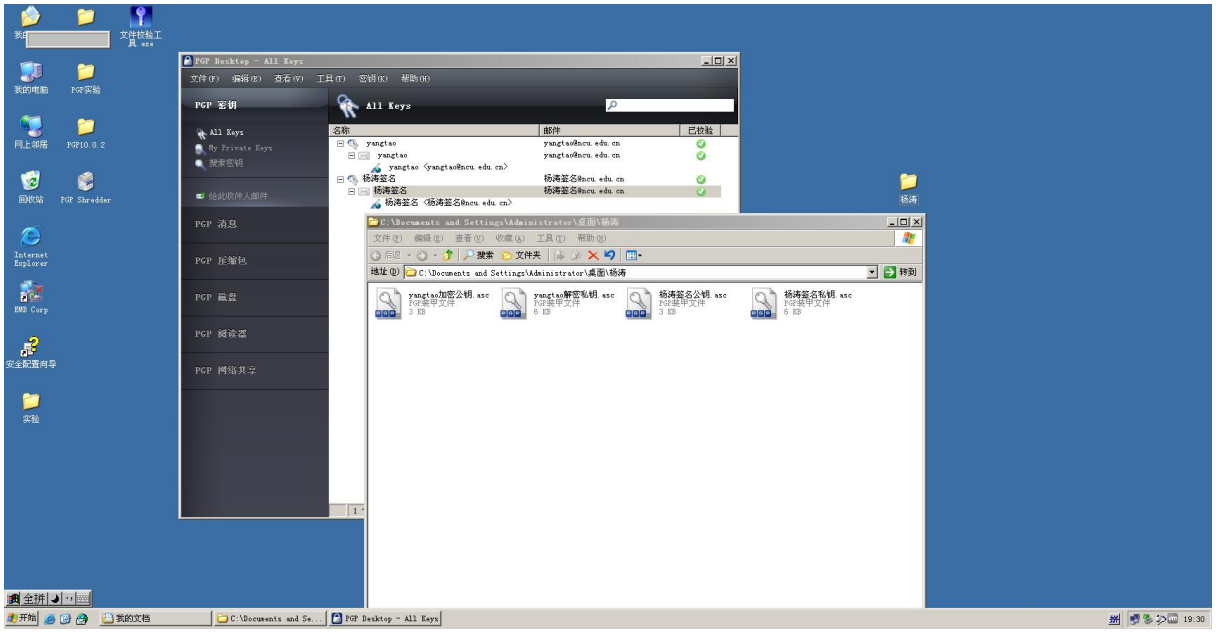
2、A 机器和 B 机器各自都生成一对加密和解密用的公钥和私钥文件，并分别保存好，A 机器中，文件名为 yangyang 加密公钥，yangyang 解密私钥。B 机器中，文件名为 yangtao 加密公钥，yangtao 解密私钥。





3、A 机器和 B 机器各自都生成另一对数字签名用的公钥和私钥文件，并分别保存好。A 机器文件名为杨洋签名公钥，杨洋签名私钥。B 机器文件名为杨涛签名公钥，杨涛签名私钥。



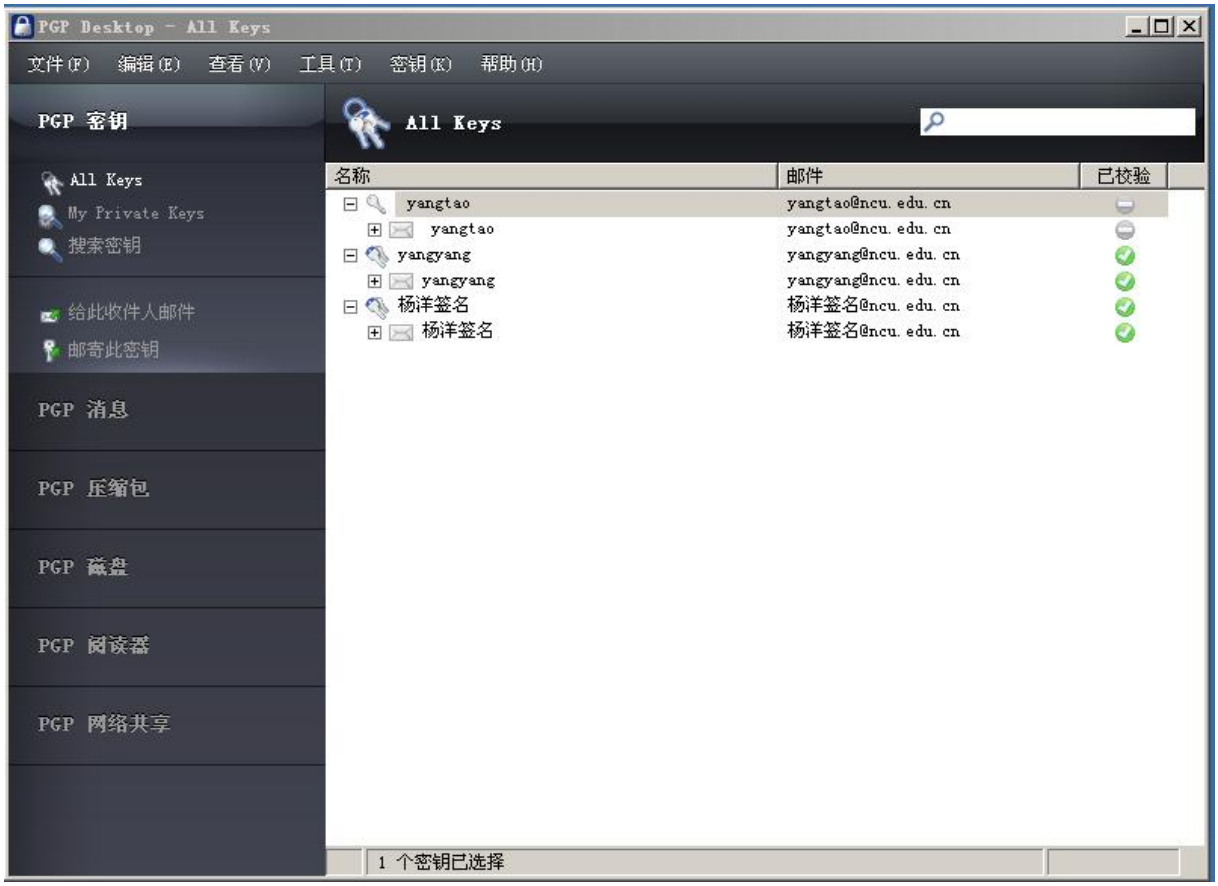


3.2 倒入公钥，加解密文件

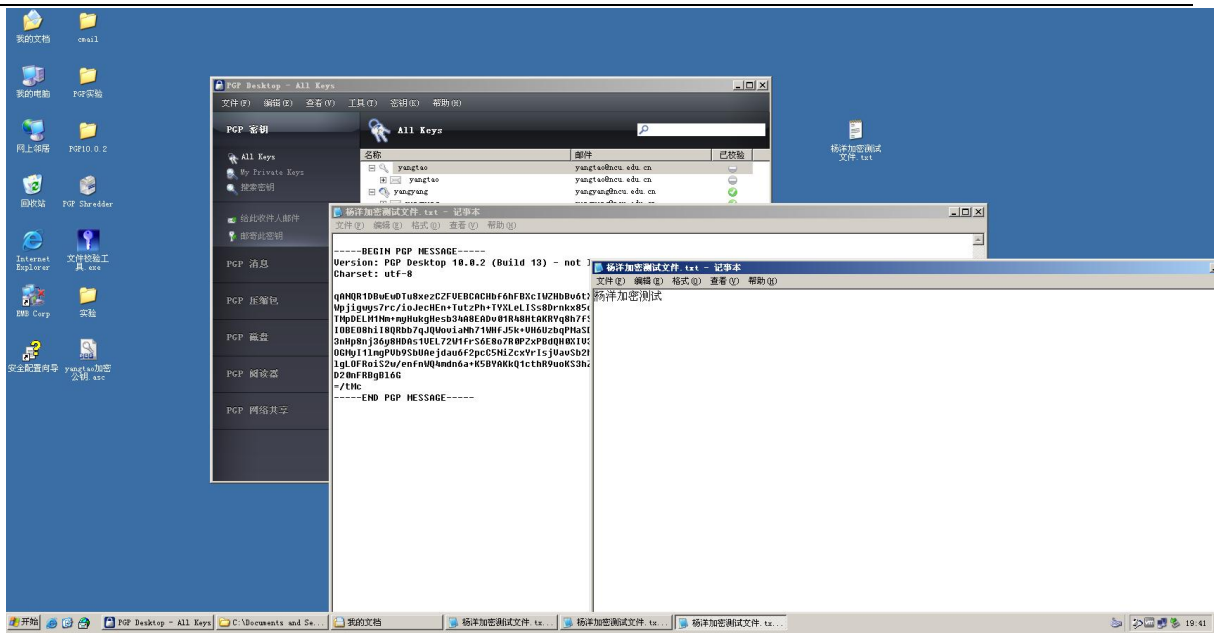
张三导入李四的加密公钥， 张三作发送方，李四作接收方。张三用李四公钥加密一个文件（文件名为：张三加密测试文件.txt，文件内容“张三加密测试），生成密码文件，用传输工具发送到李四；李四接收到此密码文件，并用自己的解密用的私钥文件进行解密，看是否还原成明文文件，李四应该能看到文件内容“张三加密测试”。

测试数据与实验结果（抓图粘贴，列出详细步骤）：

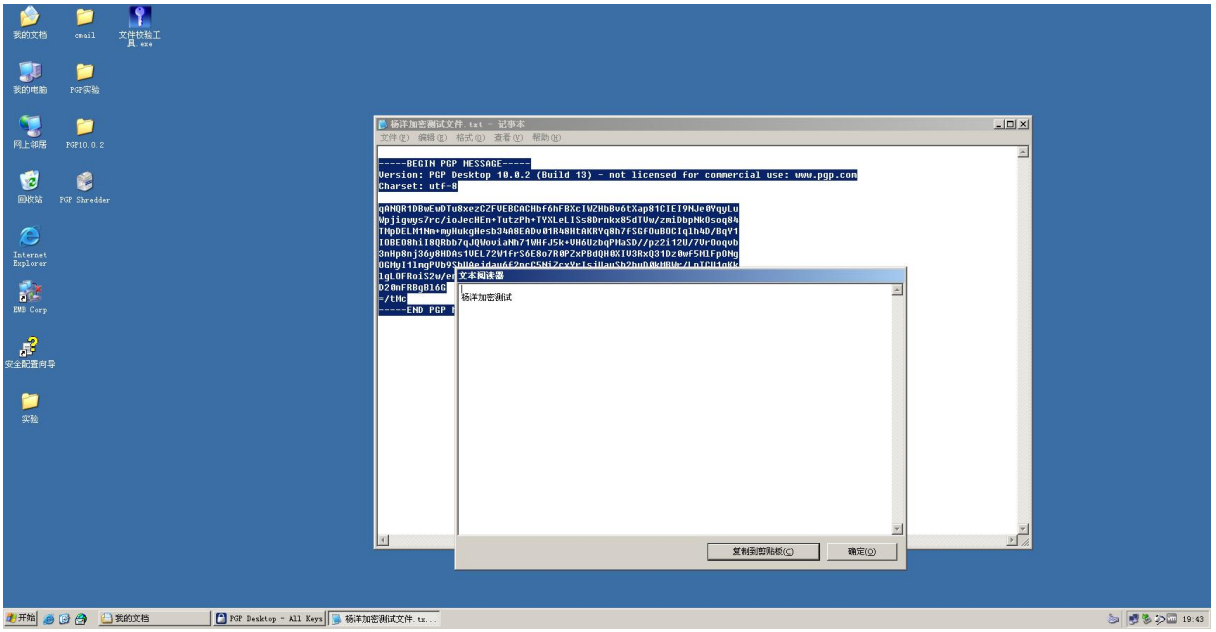
1、**杨洋导入杨涛**加密公钥， 杨洋作发送方，杨涛作接收方。



2、**杨洋**用杨涛公钥加密一个文件（文件名为：**杨洋**加密测试文件.txt，文件内容“**杨洋**加密测试），生成密码文件，用传输工具发送到杨涛；



3、杨涛接收到此密码文件，并用自己的解密用的私钥文件进行解密，看是否还原成明文文件，杨涛应该能看到文件内容“**杨洋**加密测试”。

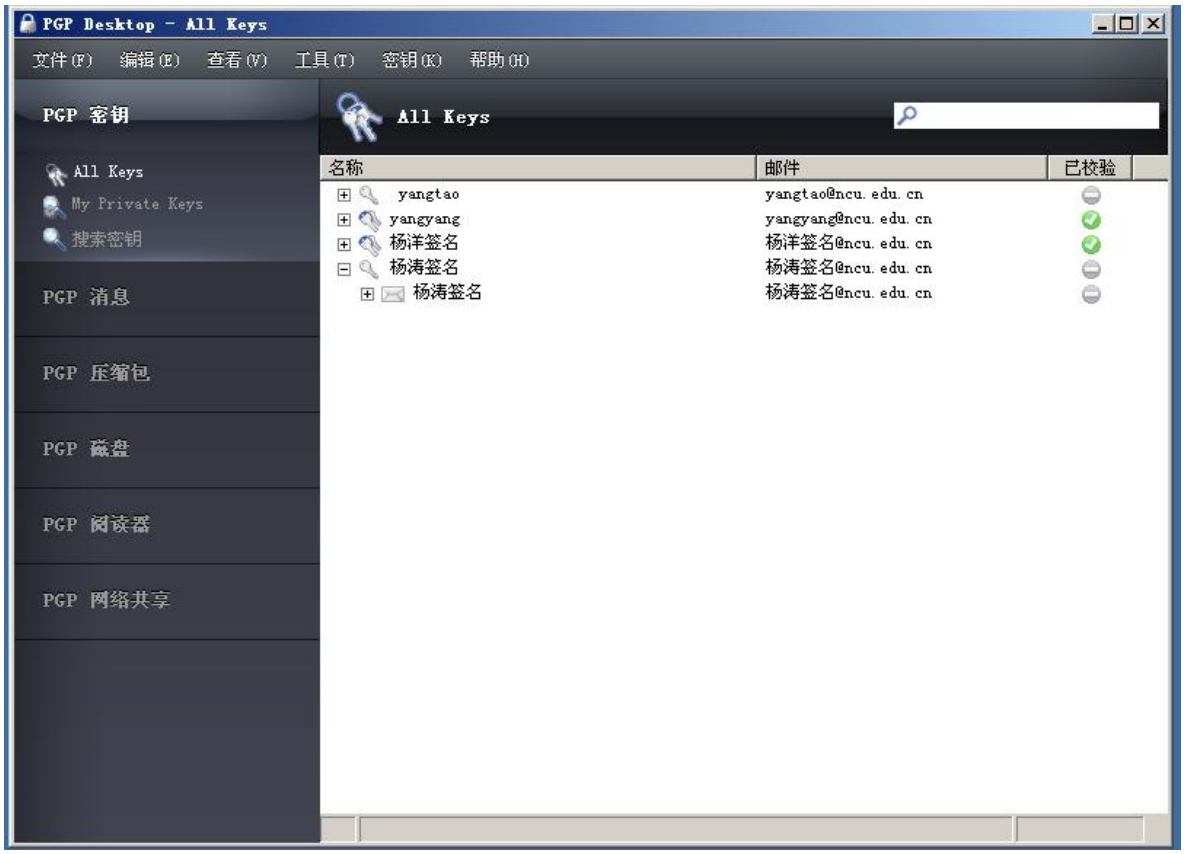


3.3 PGP 软件进行数字签名和验证的方法。

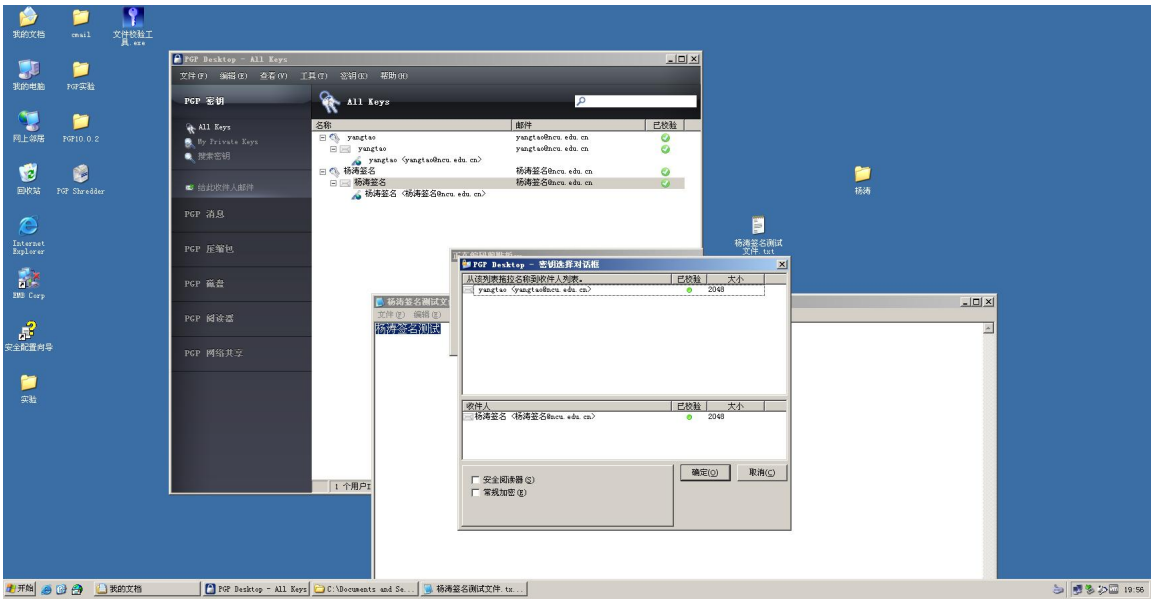
李四导入张三的签名公钥，张三用自己的签名私钥签名一个文件(文件名为：张三签名测试文件.txt，文件内容“张三签名测试)，生成签名密文文件，用传输工具发送到李四；然后李四接收此签名密文文件，并用张三的签名用的公钥打开文件进行验证。

测试数据与实验结果（抓图粘贴，列出详细步骤）：

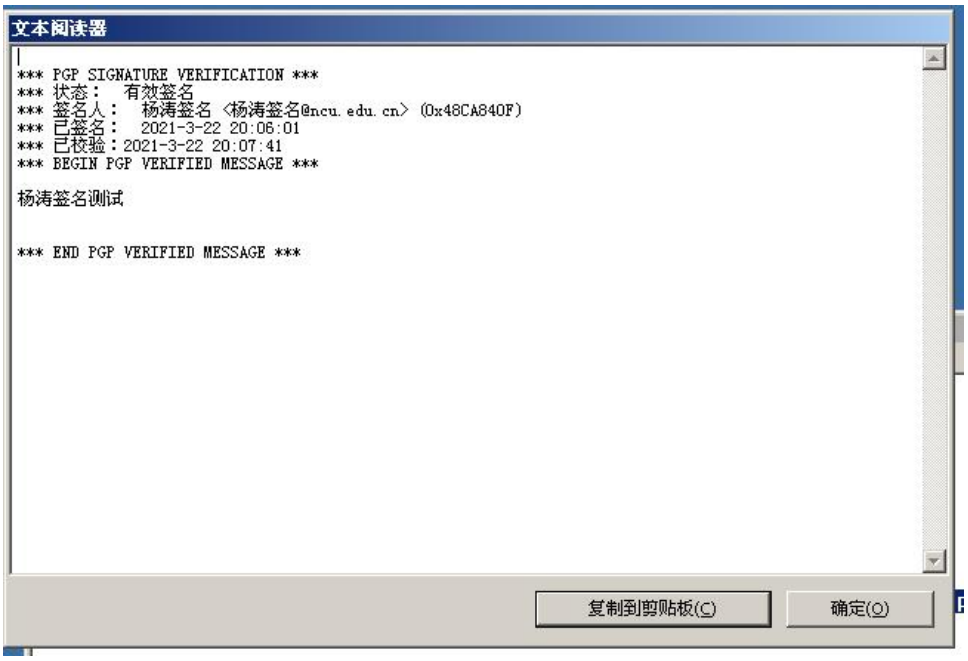
1、**杨洋导入杨涛**签名公钥， 杨洋作发送方，杨涛作接收方。



2、杨涛用自己的签名私钥签名一个文件(文件名为：杨涛签名测试文件.txt，文件内容“杨涛签名测试)，生成签名密文文件，用传输工具发送到杨洋；



3、然后杨洋接收此签名密文文件，并用杨涛的签名用的公钥打开文件进行验证。



3.4 创建 PGPdisk 加密文件

创建一个 PGPdisk 卷，位置为在 D：\张三.pgd 文件,并把卷装配为一个虚拟磁盘。

测试数据与实验结果（抓图粘贴，列出详细步骤）：

4 实验中碰到的问题

一、实验中碰到的问题--数字签名

在数字签名的时候，发现当我更改了内容时，它将会显示失效，我还以为自己出现了问题，原来是内容不可以更改。

二、创建 PGPdisk 加密文件因为未注册软件所以不会做。

5 结果分析与实验体会

实验总结通过这次试验, 我掌握 PGP 软件的安装方法, 掌握公钥与私钥生成，第一次尝试软件进行加密验证，之前学过的密码学知识终于得到巩固。从而也了解到：PGP 不是加密方法，是一个软件。由于 RSA 算法是公钥加密算法，计算过程涉及到很大的幂指数运算，计算量极大，在速度上不适合加密大量数据，所以 PGP 实际上用来加密的不是 RSA 本身，而是采用传统加密算法 IDEA，IDEA 加解密的速度比 RSA 快得多。PGP 随机生成一个密钥，用 IDEA 算法对明文加密，然后用 RSA 算法对密钥加密。收件人同样是用 RSA 解出随机密钥，再用 IEDA 解出原文。这样的链式加密既有 RSA 算法的保密性（Privacy）和认证性（Authentication），又保持了 IDEA 算法速度快的优势