

可信计算

实验报告

姓名：

学号：

教师：

2020 年 12 月

**实验一 加密综合实验**

**一、实验目的与配置**

1. 实验目的
2. 掌握加解密的原理和公钥体制
3. 了解PGP软件的功能和使用
4. 掌握PGP的加密原理
5. 建议实验环境

Win7或Win10系统

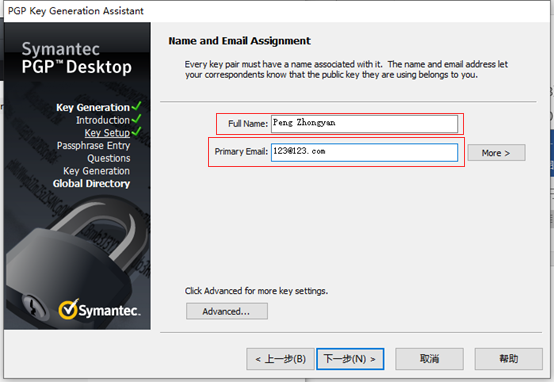
1. 建议实验工具
2. PGP加密软件
3. 客户机一台，安装Windows系统
4. 测试文件若干

**二、实验过程与步骤**

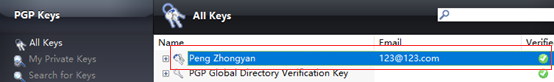
**1、安装PGP加密软件**

**2、生成密钥**

输入用户名和邮箱，新建一对密钥

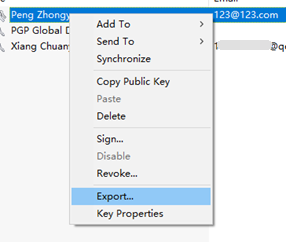


密钥窗口中可以看到新建的密钥：



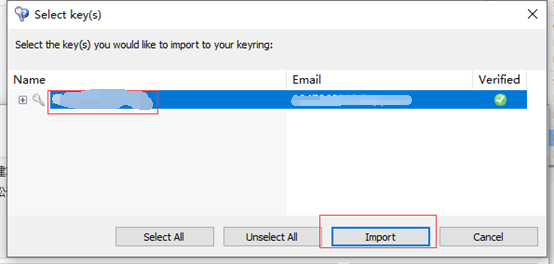
**3、导出并发送公钥**

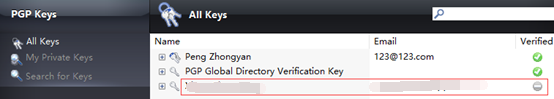
右键选择导出刚刚生成的密钥对中的公钥



**4.导入对方的密钥**

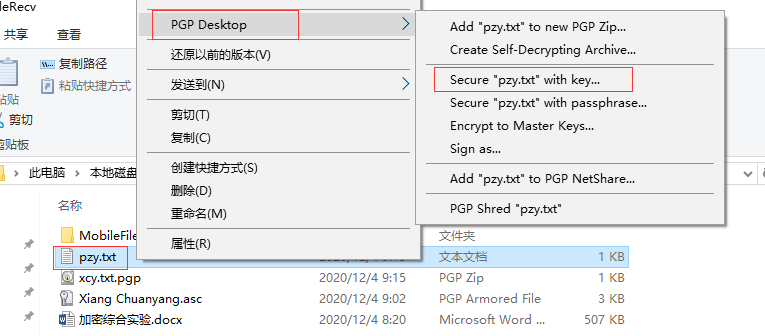
双击对方发送过来的公钥，选择导入



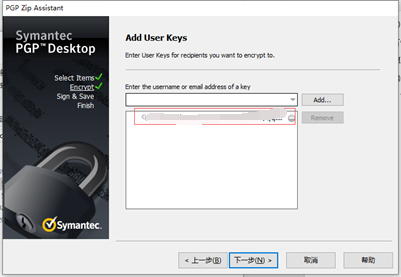


**5、文件加密**

选择一个文件，右键单击，选择“Secure “filename” with key



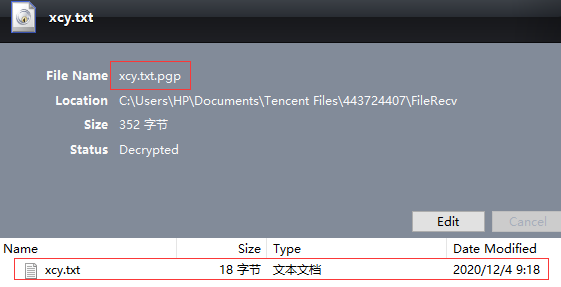
选择对方的公钥进行加密



然后得到一个名为“pzy.txt.pgp”的加密文件，将该文件发送给对方解密

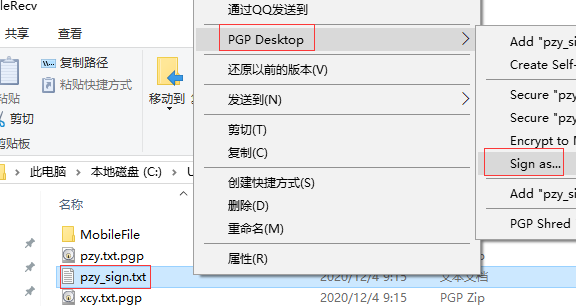
**6、文件解密**

对方收到加密文件后，右键单击加密后的文件，选择PGP Desktop，选择Decrypt & Verify “文件名”，即可得到原文件



**7、数字签名**

右键单击需要签名的文件，选择PGP Desktop—Sign as—选择私钥进行签名，将得到的签名文件和原文件发送给对方。



对方收到原文件和签名文件后，双击签名文件即可验证

