COMPUTER

高等院校计算机技术

“十二五”规划教材

网络安全与管理技术实验教程

◎余斌霄 金 蓉 编著

ZHEJIANG UNIVERSITY PRESS
浙江大学出版社

高等院校计算机技术“十二五”规划教材

网络安全与管理技术实验教程

余斌霄　金　蓉　编著

ZHEJIANG UNIVERSITY PRESS
浙江大学出版社

图书在版编目（CIP）数据

网络安全与管理技术实验教程／余斌霄，金蓉编著.
—杭州：浙江大学出版社，2012.12
ISBN 978-7-308-10637-5

Ⅰ.①网… Ⅱ.①余…②金… Ⅲ.①计算机网络－安全技术－教材 Ⅳ.①TP393.08

中国版本图书馆 CIP 数据核字（2012）第 226103 号

网络安全与管理技术实验教程

余斌霄　金　蓉 编著

责任编辑　王元新
封面设计　刘依群
出版发行　浙江大学出版社
（杭州市天目山路 148 号　邮政编码 310007）
（网址：http://www.zjupress.com）
排　　版　杭州中大图文设计有限公司
印　　刷　浙江良渚印刷厂
开　　本　787mm×1092mm　1/16
印　　张　8.75
字　　数　202 千
版 印 次　2012 年 12 月第 1 版　2012 年 12 月第 1 次印刷
书　　号　ISBN 978-7-308-10637-5
定　　价　23.00 元

前　言

自20世纪50年代以来，计算机网络技术获得了日新月异的迅猛发展，使人类的生活方式产生了巨大变革，将人类社会带入了一个全新的信息化时代。在信息化社会，每个人生活的方方面面都与信息的产生、传输、存储和处理诸环节息息相关，信息在国民经济和社会生活中占据着举足轻重的地位。与此同时，计算机网络相关的安全和管理问题也日益突出，成为威胁计算机网络和信息安全及个人隐私安全的重大隐患。一方面，现有的互联网在设计之初主要是在科研机构中进行学术研究，网络环境较为纯净，并未充分考虑到大规模应用时可能面临的各类安全和管理问题，在网络安全和管理上存在先天缺陷和不足；另一方面，在信息化社会中某些重要信息的潜在价值远远超出了其他有形资产，攻击者更易于受灰色利益驱动对计算机网络展开攻击。这种针对性较强的、以获取灰色利益为目标的攻击行为已经不再局限于早期以发现系统漏洞并进行善意提醒为目的的纯技术性范畴，对计算机网络的危害广泛而深远。此外，计算机网络本身的发展也在一定程度上为提高攻击手段和传播攻击技术提供了交流平台，使得计算机网络安全和管理面临着更加严峻的局面。

为了适应信息化社会对于网络安全和管理人才的需求，培养学生在网络安全和管理方面的实践能力，结合我校“网络安全与管理技术”课程教学实际编写了这本实验指导教材。本教材内容取材于“网络安全与管理技术”课程实验，从实验原理入手，由浅入深，逐步细化，对实验过程进行了细致翔实的描述，并针对实验过程提出了若干思考问题，既使学生掌握了基本的实验原理和实验步骤，也为学生进一步巩固和提高预留了空间，旨在使学生能更好地理解和掌握理论知识，并将其应用到实践中去，通过理论与实际的结合，切实提高实践能力。

本教材主要内容分为两部分：第一部分（实验1～7）为网络安全实验，包括PGP数字签字（验证性）、Windows系统安全增强（综合性）、操作系统帐户安全（综合性）、网络漏洞扫描（验证性）、IPTABLES防火墙（设计性）、SNORT入侵检测系统（综合性），以及恶意程序及代码清除（研究创新性）七个实验内容；第二部分（实验8～12）为网络管理实验，包括网络设备SNMP代理的配置（验证性）、用Getif实现流量监测（验证性）、监视通信线路（验证性）、性能监视（综合性）以及用StarView实施网络管理（综合性）五个实验内容。附录一和附录二分别介绍了本教材所用的实验环境并给出了实验报告参考格式。

本教材由余斌霄主持编写，网络安全实验部分由余斌霄编写，网络管理实验部分由金蓉编写，附录由金蓉、余斌霄共同编写。在本教材编写过程中得到了浙江工商大学信电学院领导的关心、鼓励和大力支持，课程组的同事也对书稿进行多次审阅并提出修改意见，

这些修改建议和关心支持提高了教材质量并促进了本书的顺利出版，作者向他们致以衷心的感谢。感谢2010年浙江省本科院校实验教学示范中心建设点“网络与通信技术实验教学中心”项目资助。

由于作者水平有限，加之时间仓促，书中难免存在疏漏和错误之处，敬请各位读者不吝指正。

作 者

2012年8月

目　录

网络安全实验

网络管理实验

网络安全实验

实验 1

PGP 数字签字

1. 实验目标

- 掌握 Windows 环境下 PGP 软件的安装和配置。
- 掌握 PGP 中密钥对的创建、使用、管理和维护方法。
- 学会使用 PGP 软件对文件进行数字签字和签字验证。

2. 实验环境

(1) 硬件环境。

- 处理器:最低 Intel 奔腾Ⅲ 500MHz,推荐 Intel 酷睿 1.8GHz 或以上。
- 内存:至少 256MB 内存,推荐 512MB 或以上。
- 硬盘:至少 100MB 可用磁盘空间,推荐 1GB 或以上。
- 网络:两台虚拟机处于同一局域网段,通过虚拟网络相互连接。

(2) 软件环境。

- 操作系统:Microsoft Windows 2000 Professional with SP4。
- 应用软件:PGP for Windows V.8.0.2(需自行安装)。

3. 实验要求

- 安装 PGP 软件并生成自己的密钥对。
- 对任意文本文件进行数字签字并相互验证。
- 充分认识 PGP 签字原理及验证流程,了解两种类型的数字签字。

4. 实验原理

以 RSA 签字体系为例：

- 选定两个大素数 p、q，计算 $n=pq$ 及 $\varphi(n)=(p-1)(q-1)$。
- 选取[1，$\varphi(n)$]间与 $\varphi(n)$互素的元素 e，计算 $d=e^{-1}\bmod \varphi(n)$。
- 销毁 p 和 q，d 作为签字私钥，而 n 和 e 作为验证公钥。
- 签字过程：$y=x^d \bmod n$，其中 x 为被签字的文件。
- 验证过程：根据欧拉定理：$x=y^e \bmod n=x^{de} \bmod n=x^{t\varphi(n)+1} \bmod n=x$。

数字签字原理图(杂凑签字方式)如图 1-1 所示。

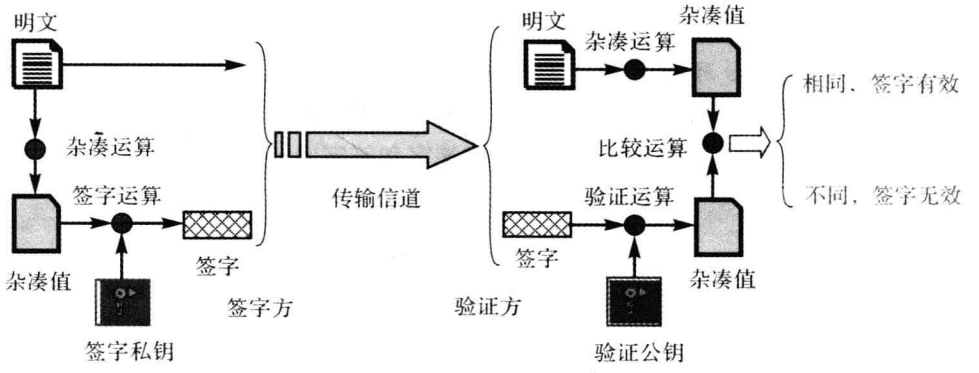

图 1-1 数字签字原理图(杂凑签字方式)

5. 考核要点

- PGP 的密钥及证书管理方式和相关操作。
- PGP 的两种签字方式：可分离签字和不可分离签字。

6. 注意事项

- 在使用 PGP 签字功能之前，必须首先创建或者导入自己的密钥对。
- 在使用 PGP 私钥之前需要输入保护密码，但该密码并非私钥本身。
- 在验证 PGP 签字之前，必须获得文件签字方公钥并调整信任级别。
- 导出密钥时是否包含私钥要根据导出目的确定，私钥不得泄露。

7. 实验步骤

(1) 安装 PGP 软件。

① 在宿主机上架设 Http 服务器，发布 PGP 安装软件 PGP for Windows。

② 启动虚拟机，进入 Windows 系统，从服务器下载 PGP 安装软件。

③ 双击 PGP 安装软件，在欢迎屏幕单击“Next”，同意许可协议。

④ 在用户类型界面，选择没有 PGP 密钥对的新用户类型，如图 1-2 所示。

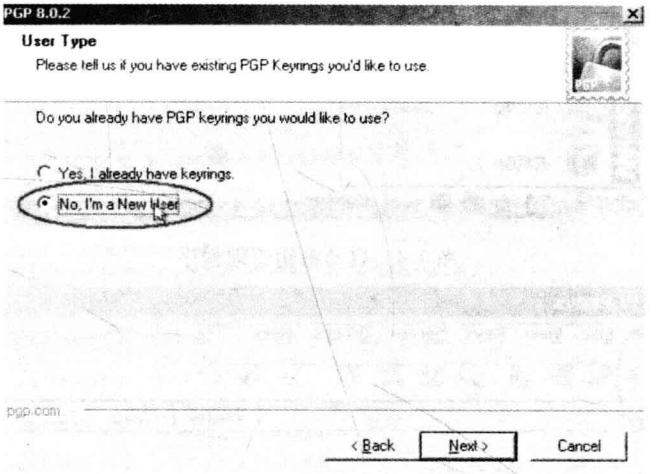

图 1-2　选择用户类型

⑤ 在后续界面选择安装目录及安装组件，并确认安装配置，如图 1-3 所示。

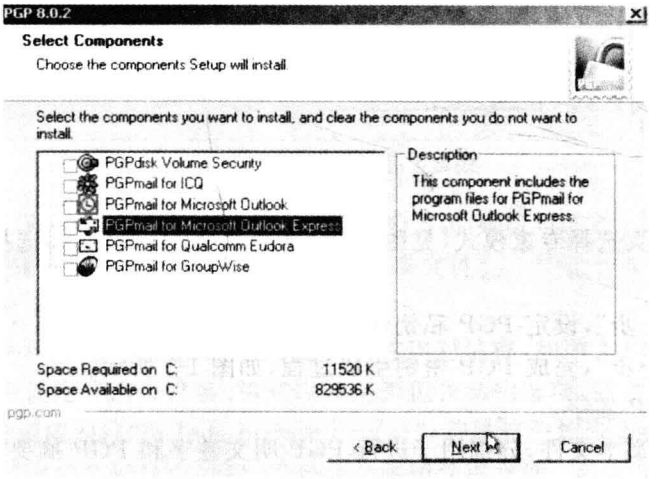

图 1-3　选择安装组件

⑥ 文件拷贝及配置过程结束后重启虚拟机，完成 PGP 软件的安装过程。

(2) 创建 PGP 密钥对。

① 虚拟机重启后，选择密钥管理程序及密钥向导开始创建密钥对，如图 1-4 和图 1-5 所示。

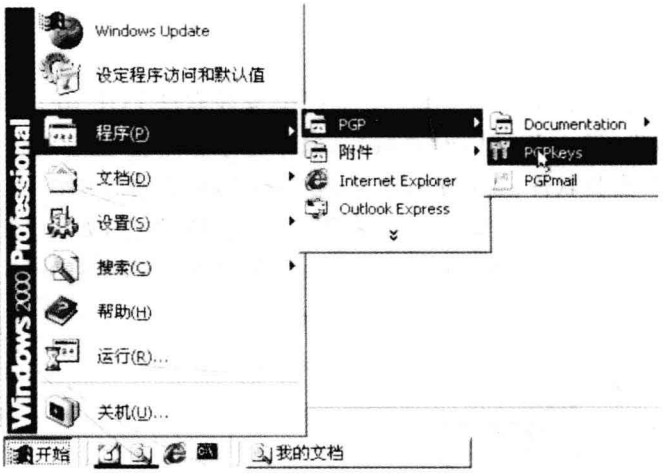

图 1-4 启动密钥管理程序

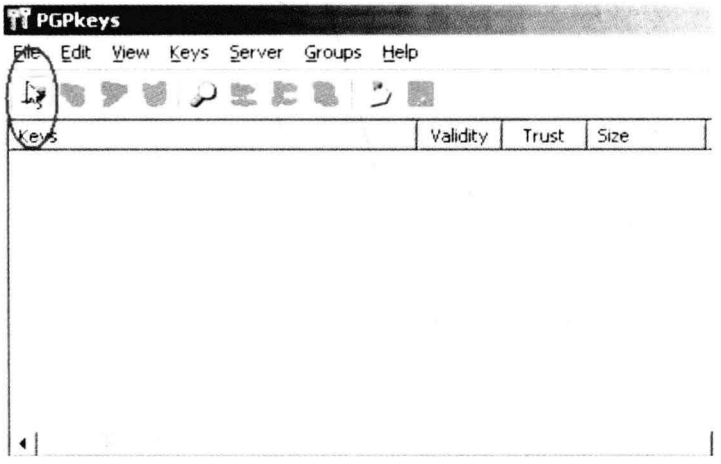

图 1-5 启动密钥向导

② 在向导首页选择专家模式(见图 1-6)，然后填入用户信息并选择签名方案及参数(见图 1-7)。

③ 单击“下一步”，设定 PGP 私钥保护密码，两次需一致，如图 1-8 所示。

④ 单击“下一步”，完成 PGP 密钥生成过程，如图 1-9 所示。

(3) 创建 PGP 签字。

① 新建两个文本文件，分别用于进行 PGP 明文签字和 PGP 摘要签字。

② 鼠标右键单击待签名文件，从快捷菜单中选择签名项，如图 1-10 所示。

③ 在下一对话框选择签名私钥、输入保护码，并选择签名类型。如果针对明文本身签名，

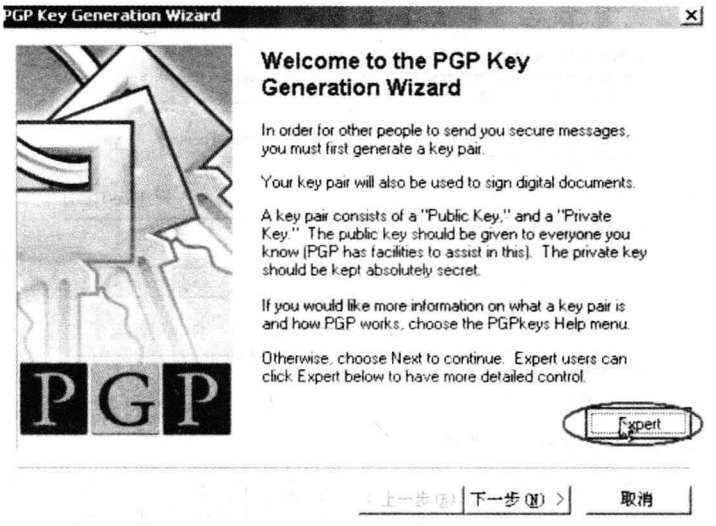

图 1-6　选择专家模式

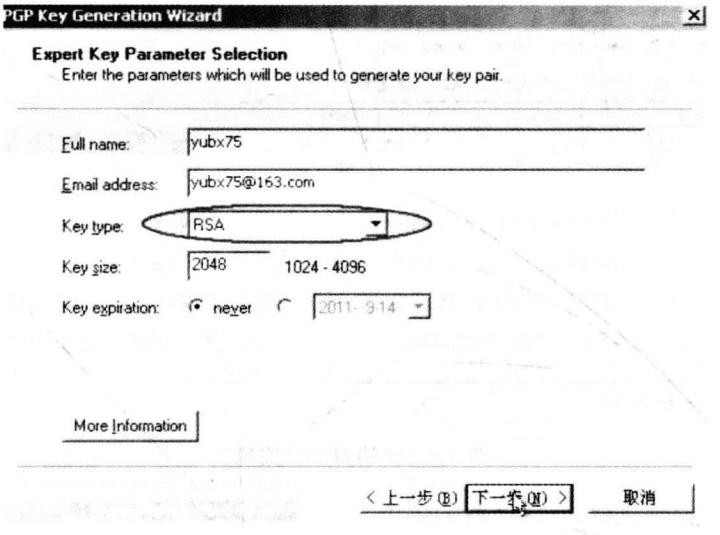

图 1-7　用户信息及签名参数

请勿勾选“Detached Signature”选项；如果针对明文摘要签名，则应勾选之。如图 1-11 所示。

④ 单击“OK”完成数字签字过程，得到两个签字文件。

(4) 导出 PGP 公钥。

① 选择密钥菜单中的导出菜单项，打开密钥导出对话框，如图 1-12 所示。

② 在对话框中设定导出文件名、格式以及是否包含私钥选项，后者视导出目的而定：若进行密钥对备份则应勾选“include private key(s)”，若进行公钥发布则不应勾选。

③ 单击“保存”完成公钥导出过程，得到一个密钥导出文件。

④ 将上述明文文件、签字文件和密钥导出文件发送给签字验证方。

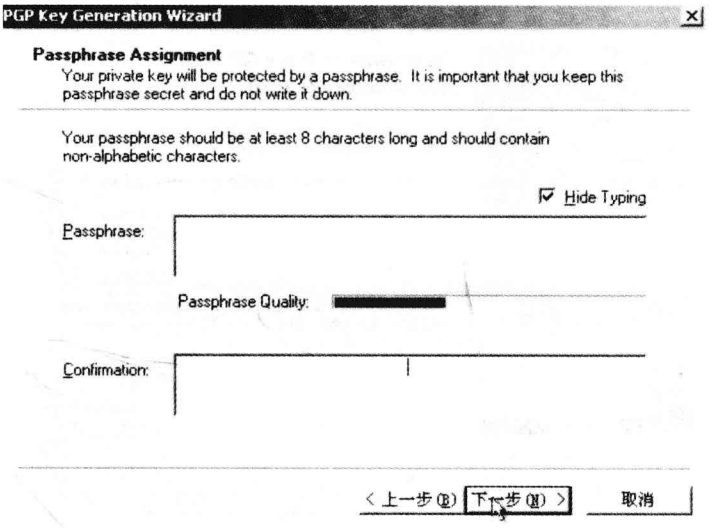

图 1-8 设定私钥保护密码

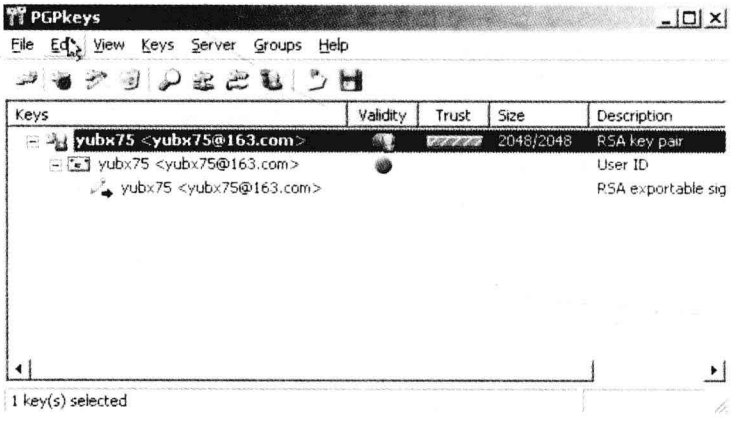

图 1-9 密钥对创建完成

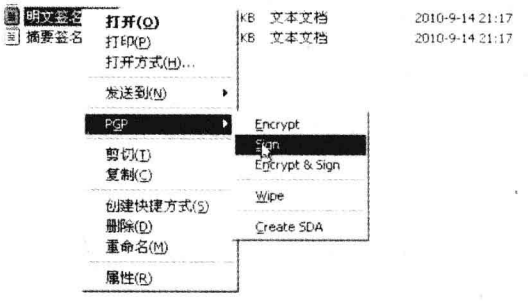

图 1-10 选择签名菜单项

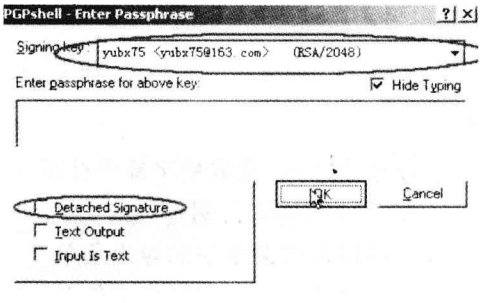

图 1-11 输入私钥保护码

(5) 导入 PGP 公钥。

① 验证方双击收到的密钥导出文件,打开导入对话框,如图 1-14 所示。

② 在对话框中选中对应公钥,点击“Import”进行导入,如图 1-14 所示。

图 1-12　选择导出菜单项

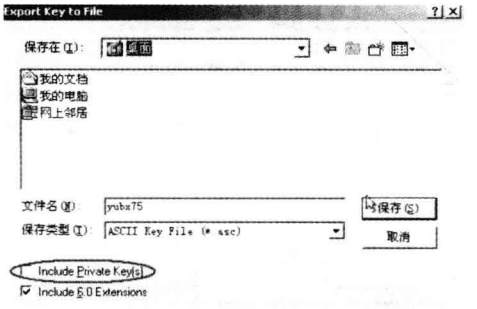

图 1-13　设定导出信息

③ 打开密钥管理器，选中导入的公钥，选择签字菜单项，如图 1-15 所示。

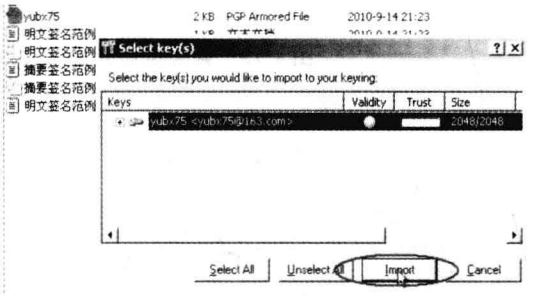

图 1-14　导入验证公钥

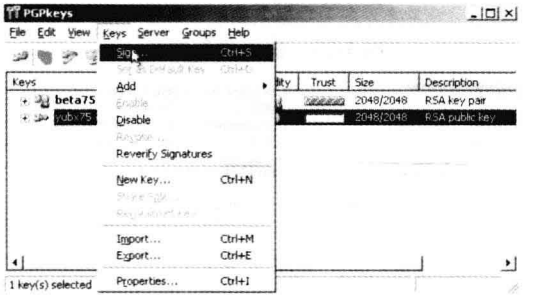

图 1-15　选择公钥签字

④ 在确信该公钥来源可靠的前提下，确认对其进行签字，如图 1-16 所示。

⑤ 输入验证方的私钥保护码，完成对该公钥的签字过程，如图 1-17 所示。

⑥ 再次选中上述签字完成的公钥，选择密钥属性菜单项，如图 1-18 所示。

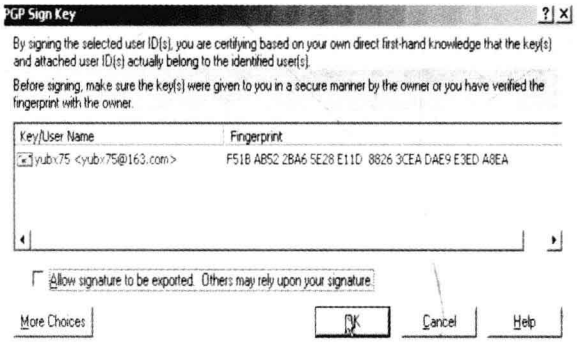

图 1-16　确认公钥签字

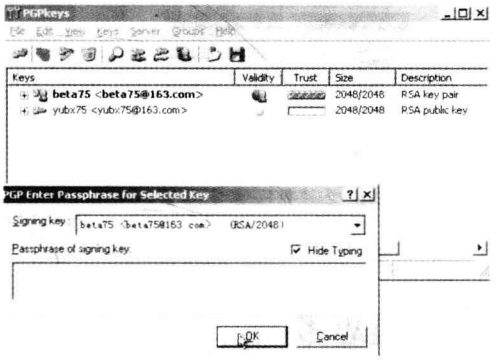

图 1-17　输入私钥保护码

⑦ 在该公钥的通用属性选项卡中调整信任级别为信任，如图 1-19 所示。

(6) 验证 PGP 签字。

① 对于明文签字，右键单击签名文件并选择解密验证，如图 1-20 所示。

② 在选择解密路径之后即可看到签字验证结果，如图 1-21 所示。

③ 对于摘要签字，右键单击签名文件并选择签字验证，如图 1-22 所示。

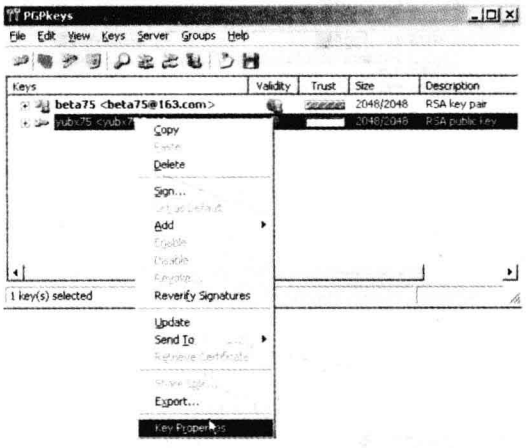

图 1-18 选择密钥属性

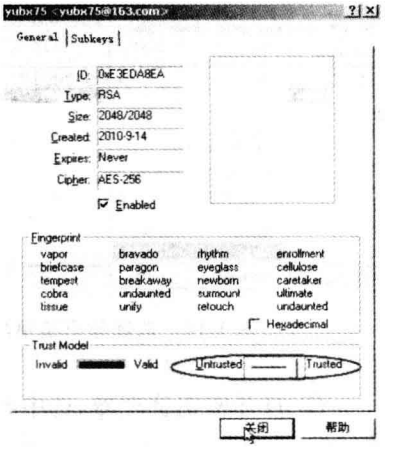

图 1-19 调整信任级别

图 1-20 选择解密验证

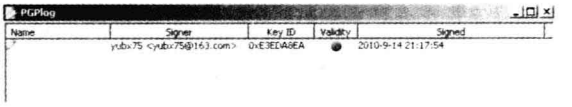

图 1-21 明文签字验证结果

④ 可直接看到签字验证结果，如图 1-23 所示。

图 1-22 选择签字验证

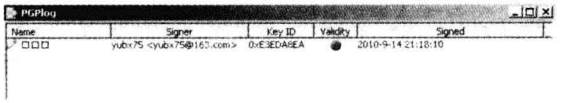

图 1-23 摘要签字验证结果

8. 实验思考

(1) 跳过公钥导入和信任调整，直接进行签字验证，结果如何？试分析原因。

(2) 分别修改两种签字方式的明文文件，再次对原签名结果进行验证，结果如何？试分析原因，并比较两种签字方式的差异。

实验过程记录