



灵创职业教育 • 网络与信息安全系列教材

网络及信息安全 综合实验教程

田 华 李 剑 张少芳 主编



北京邮电大学出版社
www.buptpress.com

灵创职业教育·网络与信息安全系列教材

网络及信息安全综合实验教程

田 华 李 剑 张少芳 主 编

北京邮电大学出版社
· 北 京 ·

内 容 简 介

随着信息技术和计算机网络的普及,网络和信息安全对社会生产生活的影响越来越大。掌握必要的网络及信息安全操作技能是高职网络及信息安全专业学生必须具备的专业能力之一。本教材针对高职高专教育特点,结合应用案例介绍目前主流网络及信息安全管理、维护操作知识,有助于增强教学针对性、实用性。

本书共分5章,涵盖了网络及信息安全技术各个层次的主要知识。

本书适合于高等职业技术学校或大学专科信息安全相关专业的学生进行网络及信息安全实验方面的教育。

图书在版编目(CIP)数据

网络及信息安全综合实验教程/田华,李剑,张少芳主编. —北京:北京邮电大学出版社,2008

ISBN 978-7-5635-1875-3

I. 网… II. ①田…②李…③张… III. 计算机网络—安全技术—高等学校;技术学校—教材 IV. TP393.08

中国版本图书馆 CIP 数据核字(2008)第 153399 号

书 名: 网络及信息安全综合实验教程

作 者: 田 华 李 剑 张少芳

责任编辑: 张珊珊

出版发行: 北京邮电大学出版社

社 址: 北京市海淀区西土城路 10 号(邮编:100876)

发 行 部: 电话: 010-62282185 传真: 010-62283578

E-mail: publish@bupt.edu.cn

经 销: 各地新华书店

印 刷: 北京市梦宇印务有限公司

开 本: 787 mm×1 092 mm 1/16

印 张: 16.5

字 数: 408 千字

印 数: 1—3 000 册

版 次: 2009 年 1 月第 1 版 2009 年 1 月第 1 次印刷

ISBN 978-7-5635-1875-3

定 价: 28.00 元

• 如有印装质量问题,请与北京邮电大学出版社发行部联系 •

灵创职业教育·网络与信息安全系列教材

编委会

名誉主任 方滨兴 院士

主 任 杨义先

委 员 (排名不分先后)

周继军 陈 运 方 勇 韩 臻

李子臣 罗 平 姬东耀 陈绥阳

姚景平 刘吉强 马兆丰 范科锋

辛 阳 郑康锋 李祥学 王励成

李宝安 赵金满 刘海云 李同芳

田 华 李 剑

序

目前我国“职业教育”正值春天。在党和国家的大力支持和积极推动下,全社会对职业教育的关注空前高涨,职业教育蓬勃发展。值此大好时机,每个教育工作者都应认真贯彻落实科学的发展观,坚持以服务为宗旨,以就业为导向,以提高质量为重点,进一步解放思想、开拓进取、扎实有力地推进我国职业教育又好又快地发展,办好人民满意的职业教育。但出于历史原因,目前我国职业教育体系很不健全,职教专业、职教教材“本科简化型”现象比较普遍,真正“重实践,重应用,与职业技能培养紧密结合”的高质量精品教材非常紧缺。

鉴于上述情况,为促进我国职业教育的规范发展,特别是为了满足当前各级各类职业教育教师、学生对适配自身教育和实践教材的迫切需要,北京邮电大学出版社,灵创团队北京邮电大学信息安全中心,灵创团队北京邮电大学数字内容研究中心以及绵阳灵创电子信息技术学校的专家、领导,决定共同合作,团结全国相关领域专家,策划、撰写、出版多套覆盖“网络与信息安全”和“数字媒体创意”等领域的“灵创职业教育”系列教材。

在“灵创职业教育·网络与信息安全”系列教材策划过程中,我们组织安全和职教专家对国内目前“网络与信息安全”职教层次人才需求和“网络与信息安全”职教发展现状进行了全面调研分析。研究发现,社会对“网络与信息安全”职教层次的人才需求集中在“信息与网络安全管理”、“安全产品营销与服务”方面。下表显示了对这些岗位职业技能需求和学习领域进行研究分析的结果。

职业目标	岗位主要职责	职业技能要求	学习领域	
			知识	整合课程
信息与网络安全管理	管理、维护操作系统,保障操作系统级安全	1. 系统及应用安全风险评估 2. 系统及应用安全方案设计 3. 系统安全配置 4. 系统安全监控及审计 5. 数据安全 6. 应用系统运行安全	1. 信息安全法规/标准 2. 操作系统访问控制配置 3. 操作系统进程及服务配置 4. 操作系统性能、本地/网络访问监控 5. 系统日志管理 6. 数据备份恢复 7. 漏洞管理 8. 操作系统安全风险分析及工具	1. 信息安全法规与标准 2. 操作系统管理 3. 信息安全导论(操作系统安全部分) 4. 信息安全管理与工程(信息安全风险评估-操作系统)

续表

职业目标	岗位主要职责	职业技能要求	学习领域	
			知识	整合课程
信息与网络安全管理	管理、维护数据库,保障数据库系统安全运行及数据安全	1. 数据库安全风险评估 2. 数据库安全管理方案设计 3. 数据库安全管理	1. 数据库基本概念 2. 数据库基本管理操作 3. 数据安全操作(包括数据库访问控制安全、数据库备份恢复) 4. 数据库安全风险分析及工具	1. 信息安全导论(数据库安全部分) 2. 信息安全管理与工程(信息安全风险评估-数据库)
	管理、维护信息服务,保障信息服务安全运行	1. 安装、配置常见的网络服务 2. 制作网站	1. 常见网络服务器安装、配置、管理 2. 网站制作 3. 网络服务安全	1. 网站制作 2. 网络服务管理与维护 3. 信息安全导论(网络服务安全)
	病毒防护	1. 设计系统计算机病毒防范方案 2. 防毒软件采购 3. 安装和配置计算机病毒软件 4. 防毒软件维护	1. 操作系统原理 2. 计算机病毒原理 3. 防毒软件产品 4. 防毒软件安装、配置、升级管理	1. 计算机病毒防范 2. 信息安全产品与方案
	管理、维护网络,保障网络安全	1. 构建基础网络连接 2. 网络安全风险分析 3. 网络安全方案设计 4. 网络安全设备配置 5. 网络安全监控	1. 网络基础,包括局域网构建、网络协议、常见网络设备交换机、路由器配置管理 2. 网络安全与管理,包括防火墙、VPN、IDS 技术及配置管理基本操作,网络攻击与防护简介 3. 网络攻击与防范,包括各类网络攻击原理,防范手段(如入侵检测、防火墙、VPN 等防范手段的使用)	1. 网络安全与管理 2. 网络攻击与防范技术 3. 信息安全管理与工程(信息安全风险评估-网络安全) * 4. 入侵检测技术 * 5. 防火墙技术 * 6. 黑客防范
	保障物理和环境安全	1. 提出信息系统场地安全需求及建设方案,监控、审计场地安全方案实施情况 2. 提出信息系统自然防灾需求及建设方案,监控和审计防灾方案实施情况 3. 规划设计信息系统物理访问控制方案,监控和审计方案实施情况	1. 电路电工基础 2. 信息系统场地安全、防灾等相关法规、标准 3. 信息系统物理访问控制相关产品	1. 信息安全导论(信息系统物理与环境安全) 2. 信息安全管理与工程 3. 信息安全产品与方案
	信息保密管理	1. 制定信息系统信息保密与数字权益保护方案 2. 采购信息保密、数字权益保护产品 3. 信息保密、数字权益保护方案实施	1. 密码学基础 * 2. 信息隐藏、数字水印、数字权益保护	1. 信息安全导论 2. 信息安全产品与方案(信息隐藏) 3. 信息安全管理与工程(信息保密)
	信息安全工程	1. 设计信息安全体系 2. 采购信息安全产品 3. 管理控制信息安全工程 4. 制定信息安全管理方案	1. 信息安全体系架构 2. 信息安全法规、标准 3. 信息安全管理方案文档编制	1. 信息安全导论 2. 信息安全管理与工程

续表

职业目标	岗位主要职责	职业技能要求	学习领域	
			知识	整合课程
信息与网络安全管理	信息安全策略、信息安全制度制定	1. 分析企业信息系统安全风险 2. 制定全面的安全管理策略和制度	1. 信息安全体系架构 2. 信息安全法规、标准 3. 信息安全管理方案文档编制	1. 信息安全导论(信息安全体系) 2. 信息安全管理与工程(安全管理制度、策略)
	*行业特色技能:计算机取证	信息系统取证	1. 信息安全法规 2. 信息系统取证方法、手段与工具使用	*计算机取证
	*行业特色技能:电子商务系统安全	1. 电子商务系统安全方案设计 2. 电子商务系统安全管理维护	1. 电子商务应用基础 2. 网上安全支付系统	*电子商务安全
安全产品营销与服务	安全产品营销与服务	安全产品营销包括: 1. 客户应用系统的安全风险分析 2. 用户系统安全风险防范方案简单设计 3. 安全产品推介方案、文档策划编写 4. 安全产品演示、讲解 安全产品服务包括: 1. 安全产品安装、使用培训 2. 安全产品故障响应咨询 3. 简易安全产品故障排除	1. 信息及网络安全基础 2. 软件开发基础 3. 硬件开发基础 4. 市场营销 5. 技术支持技巧	1. 信息安全导论 2. 网络安全与管理 3. 信息安全产品与方案 4. 信息安全标准与法规 5. 信息安全产品服务与营销

注:*为拓展课程。

基于以上分析,根据网络与信息安全学科体系的特点,在注重学生的“动手实践和技能专业化”职教原则的指导下,我们选定《信息安全标准与法规》、《网络攻击与防护技术》、《计算机病毒防护》、《网络及信息安全综合实验教程》、《信息安全产品与方案》、《信息安全管理与工程》等作为“灵创职业教育·网络与信息安全”系列教材的首批丛书。

从学科体系角度看,这些教材构成了下图所示网络与信息安全职业教育体系主体:

法律	技术与开发	管理
	产品与系统	
	评测与服务	
	使用与集成	
	营销与维护	
	培训与认证	

下表为以上课程教学参考学分。

专业课程名称	建议学分	学分分配	
		讲课	课内实验
信息安全标准与法规	4	2	2
信息安全导论	4	2	2
网络攻击与防护技术	5	3	2
计算机病毒防护	4	2	2
网络安全与管理	5	3	2
网络与信息安全综合实验	4	1	3
信息安全产品与方案	4	2	2
信息安全管理与工程	4	2	2
计算机取证与应急响应	3	2	1
合 计	37	19	18

为确保该套教材的质量,教材编委会由国内著名信息安全专家为主组成,每本教材尽可能由经验丰富的职业教育专家执笔。本套丛书主要定位在开设信息安全类专业的职业院校的教材、相应领域的社会培训教材、从业技术人员自学教材。教材既可适用于全国职业教育信息安全专业学生,又可适用于各类成人自考学生。

本套教材受到了国家 973 项目(2007CB311203,2007CB310704)、教育部高等学校博士学科点专项科研基金资助课题(20070013007,20070013005)、国家自然科学基金与香港研究资助局联合科研基金项目(No. 60731160626)和高等学校学科创新引智计划(No. B08004)的资助,在此特表感谢。

杨义先

教授、博导、长江学者特聘教授

2008 年 3 月

前 言

随着信息技术和计算机网络的普及,网络和信息安全对社会生产生活的影响越来越大。掌握必要的网络及信息安全操作技能是高职网络及信息安全专业学生必须具备的专业能力之一。本教材针对高职高专教育特点,结合应用案例介绍目前主流的网络及信息安全管理、维护操作知识,有助于增强教学针对性、实用性。

本书共分5章,涵盖了网络及信息安全技术各个层次的主要知识。

第1章信息保密实验,介绍了创建密钥对、分发/导入密钥、邮件加密传输、加密文件等信息保密常用实践操作。

第2章操作系统安全实验,从维护网络服务器、工作站的系统安全需求出发,分别介绍了在Windows、Linux两种平台上配置安全策略、保证账户和口令安全、进行访问权限、网络端口管理、系统安全审计、系统安全分析等操作技能知识。

第3章网络服务安全配置实验,结合校园网网络服务安全维护案例,介绍了IIS、Server-U、Apache和Vsftpd四种网络服务安全配置操作知识。

第4章网络应用系统安全实验,结合中、小企业应用层安全管理案例,介绍了应用层面安全配置管理操作的有关知识。包括SSL应用配置、如何进行集中的计算机病毒防护、如何在Windows和Linux系统上进行数据备份与恢复操作等。

第5章网络安全配置管理实验,以规划设计实施一个中型企业网络安全方案为例,介绍了VLAN、NAT、ACL、VPN、防火墙、IDS等多种网络安全技术的配置方法。并结合目前虚拟技术发展趋势,介绍了利用模拟器搭建网络安全模拟实践环境的有关知识。

本书第1章由张少芳编写,第2章由李剑编写,第3章至第5章由田华编写。

本书的编写工作得到了北京邮电大学信息安全中心杨义先教授、钮心忻教授、马兆丰博士,石家庄邮电职业技术学院计算机系刘海云主任、李同芳副主

任、田庚林教授的大力支持和帮助,他们对本书的出版提出了宝贵的意见和建议,在此表示衷心的感谢和敬意!本书在编写过程中,参考了国内外网络及信息安全方面的文献,在此也向文献作者表示感谢!

由于本书作者水平有限,书中难免存在疏漏、不足,还请各位读者批评指正。

编 者

目 录

第 1 章 信息保密实验

1.1 创建密钥对	2
1.2 分发/导入密钥	7
1.3 邮件加密传输	11
1.4 加密文件	15
1.5 下载安装 PGP	18
1.6 实验报告及思考题	20

第 2 章 操作系统安全实验

2.1 Windows 操作系统安全管理实验	21
2.1.1 Windows 安全策略配置	22
2.1.2 账户和口令安全	30
2.1.3 权限管理	33
2.1.4 网络端口管理	42
2.1.5 系统安全审核配置与管理	44
2.1.6 Windows 系统安全分析	46
2.1.7 实验报告及思考题	49
2.2 Linux 操作系统安全管理实验	50
2.2.1 账户和口令安全	50
2.2.2 权限管理	53
2.2.3 网络端口管理	54
2.2.4 系统安全分析	55
2.2.5 系统审计配置与管理	62
2.2.6 实验报告及思考题	66

第 3 章 网络服务安全配置实验

3.1 Windows 网络服务安全配置实验	67
3.1.1 IIS 服务安全配置	68

3.1.2	Serv-U 服务安全配置	82
3.1.3	实验报告及思考题	87
3.2	Linux 网络服务安全配置实验	88
3.2.1	Apache 安全配置	88
3.2.2	Vsftpd 安全配置	91
3.2.3	实验报告及思考题	95

第4章 网络应用系统安全实验

4.1	SSL 应用配置实验	96
4.1.1	安装证书服务器、创建 Web 站点	97
4.1.2	配置 HTTPS	99
4.1.3	实验报告及思考题	113
4.2	计算机病毒防护实验	113
4.2.1	本地安装防病毒软件	114
4.2.2	安装防病毒远程管理、控制软件	124
4.2.3	推送安装防病毒软件	132
4.2.4	远程升级病毒库	142
4.2.5	实验报告及思考题	146
4.3	数据备份与恢复实验	147
4.3.1	数据备份恢复策略	147
4.3.2	Linux 数据备份与恢复	150
4.3.3	Windows 数据备份与恢复	159
4.3.4	实验报告及思考题	167

第5章 网络安全配置管理实验

5.1	企业网络结构案例分析	169
5.2	企业网络安全实施方案设计	171
5.2.1	设备选择	171
5.2.2	网络设备安全方案	172
5.2.3	企业 VLAN 划分方案	174
5.2.4	网络设备 IP 地址配置方案	176
5.2.5	内外网地址转换配置方案	176
5.2.6	基于 ACL 的访问控制方案	178
5.2.7	Internet 安全通信方案	181
5.2.8	网络攻击防护方案	184
5.3	网络安全配置实验	185

5.3.1	搭建基本网络环境、连接防火墙及 VLAN 配置	185
5.3.2	网络设备安全配置	202
5.3.3	NAT 配置	207
5.3.4	ACL 配置	212
5.3.5	VPN 配置	217
5.3.6	网络攻击防护配置	226
5.4	实验报告及思考题	231
5.5	利用模拟器搭建网络安全实践环境	232
5.5.1	网络模拟器软件简介	232
5.5.2	搭建模拟实践环境	232
参考文献		249

第 1 章

信息保密实验

在网络通信中,防止信息被窃取的方法之一是使用加密技术将信息变为密文,使其仅能被正确授权的用户读取。PGP 是目前较为流行的邮件加密软件之一,本章实验选择用 PGP 软件加密邮件作为主要实验内容,通过实验来增进学生对加密技术的理解,使学生掌握利用加密软件保护信息安全的基本操作技能。

【实验目的】

通过本实验,加深对公钥加密机制的理解,了解 PGP 软件的安装步骤,掌握 PGP 软件创建密钥对、加密/解密邮件和文件等基本操作。

【建议学时】

本部分实验学时建议安排为 4 课时。

【实验环境】

安装有 Windows 操作系统、Foxmail 和 PGP 软件的 PC。

【工具及准备工作】

教师或实验助手应按实验环境要求为每个学生准备一台装有 Windows 系统的 PC,该 PC 应已安装有实验要用到的 Foxmail 邮件程序和 PGP 软件;参加实验的学生应事先准备好两个邮件账户 A 和 B,并已事先掌握 Foxmail 中配置电子邮件账户的操作。

【实验流程】

本部分实验流程如图 1-1 所示,包括:(1)创建通信密钥对;(2)分发密钥对;(3)导入密钥对,并为对方密钥对签名;(4)使用密钥加密信息。

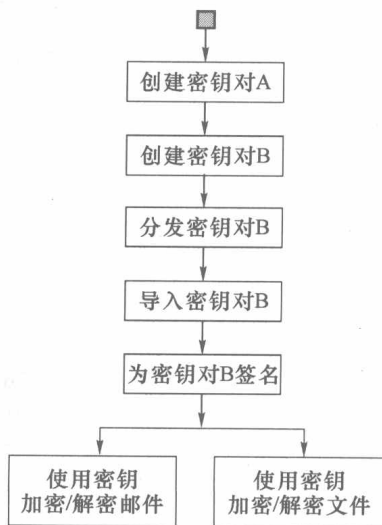


图 1-1 PGP 信息保密实验流程



1.1 创建密钥对

本部分实验为通信双方创建密钥对,主要操作包括:(1)启动 PGP Services;(2)为邮件账户 A 创建密钥对;(3)为邮件账户 B 创建密钥对。

(1) 启动 PGP Services

如果 PGP Services 尚未启动,则在 Windows 桌面,单击任务栏【开始】|【程序】|【PGP】|【PGP Desktop】,打开 PGP Desktop 窗口。此时会出现如图 1-2 所示对话框,提示是否启动所有 PGP 服务。单击【是(Y)】按钮启动 PGP 服务。

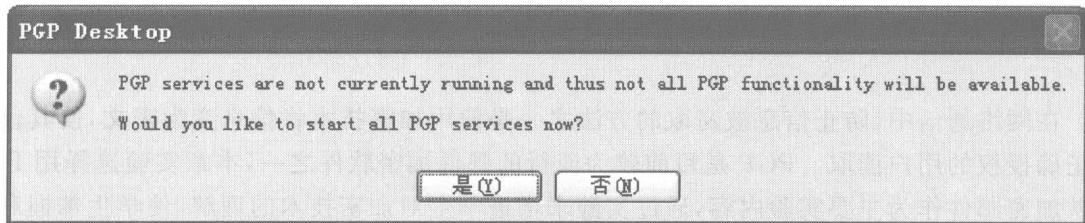


图 1-2 要求启动 PGP Services 的提示信息

如果 PGP Services 已经启动,则在 Windows 桌面用右键单击任务栏托盘中的图标,在如图 1-3 所示弹出菜单中单击【Open PGP Desktop】,打开如图 1-4 所示的“PGP Desktop”主窗口。



图 1-3 PGP 托盘图标的弹出菜单

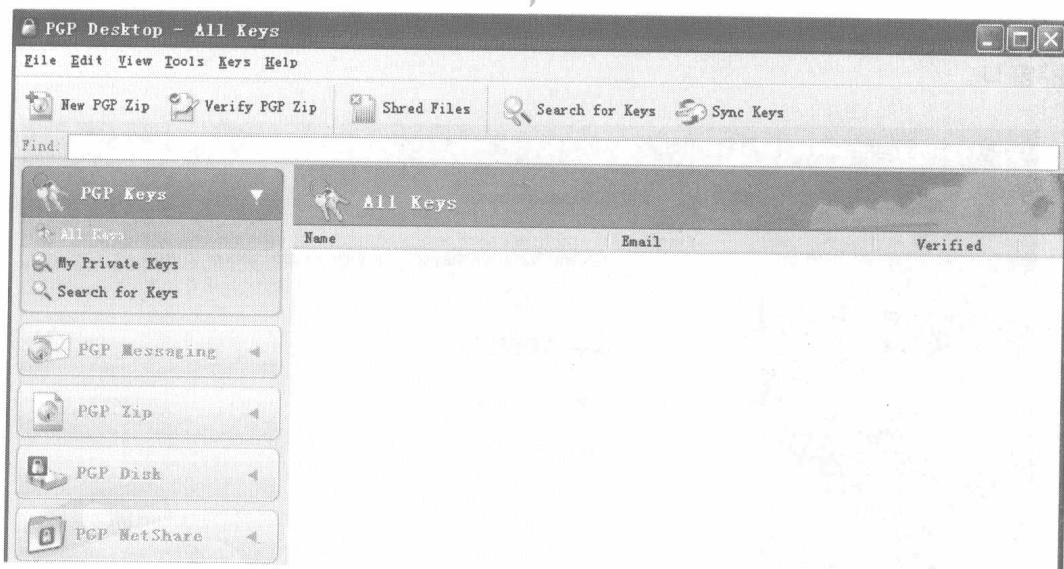


图 1-4 PGP Desktop 主窗口

(2) 创建密钥对

在“PGP Desktop”窗口中,单击菜单【File】|【New PGP Key】,在如图 1-5 所示的“新建 PGP Key 向导”窗口中,单击【下一步(N)...】按钮继续。

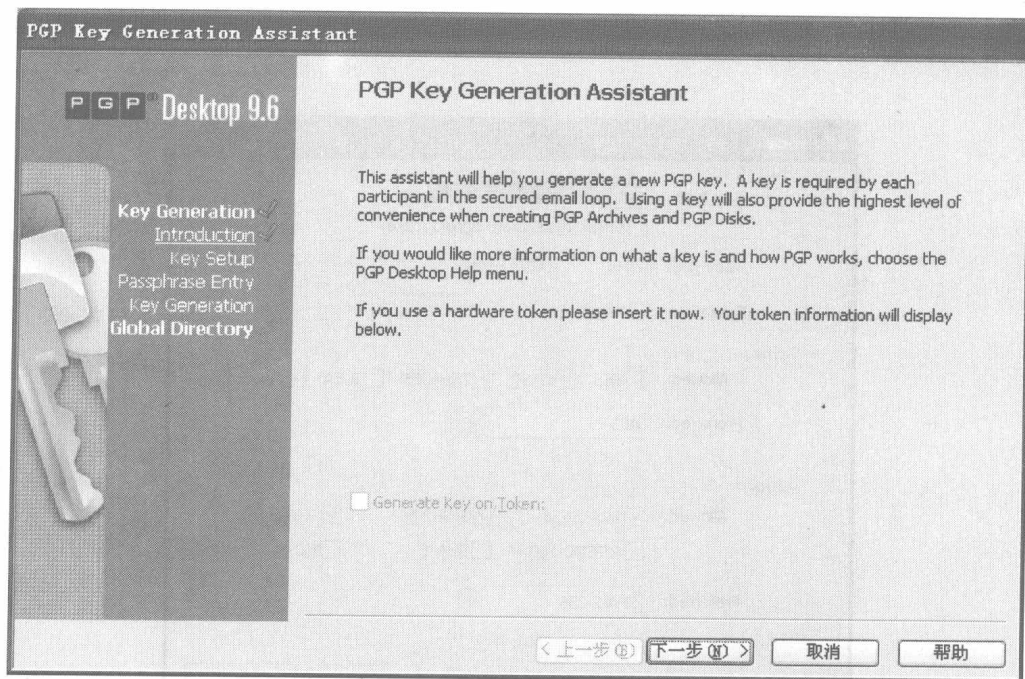


图 1-5 PGP 新建密钥向导欢迎界面

在密钥所有者“姓名和邮件”窗口中输入自己姓名和邮箱 A 的地址,如图 1-6 所示。

在“姓名和邮件”窗口中单击【Advanced...】按钮,进入如图 1-7 所示的“密钥高级配置”窗口。在如图 1-7 所示的“密钥高级配置”窗口中,设置密钥类型,支持的 HASH 算法、加密



算法等参数。复选 SHA_1, 以使密钥对支持该摘要算法。单击【OK】按钮确定退回“姓名和邮件”窗口。

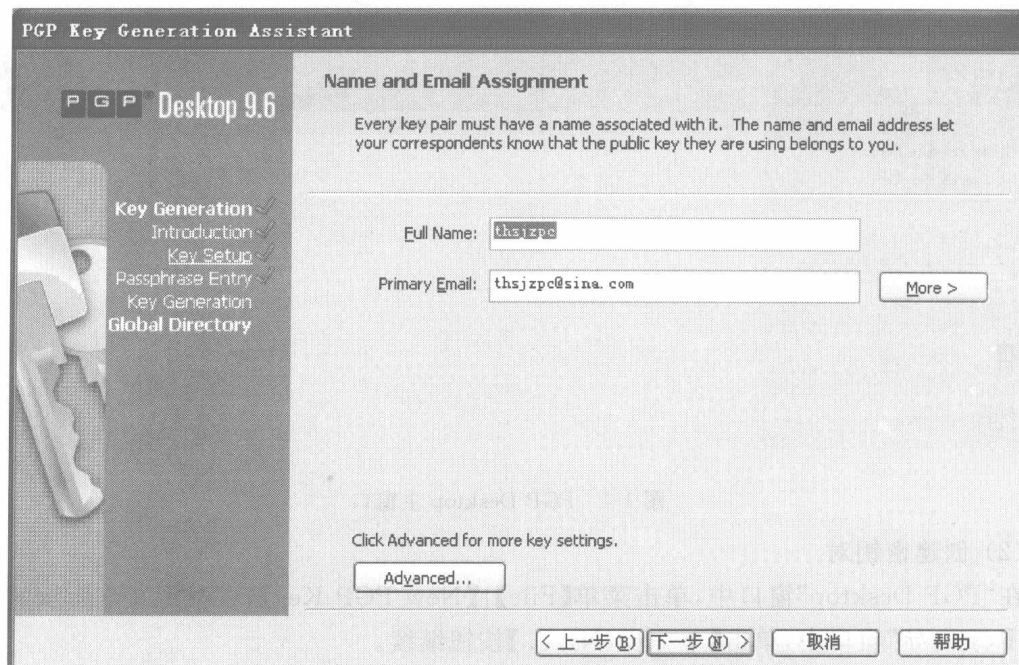


图 1-6 配置密钥所有者姓名和邮件地址

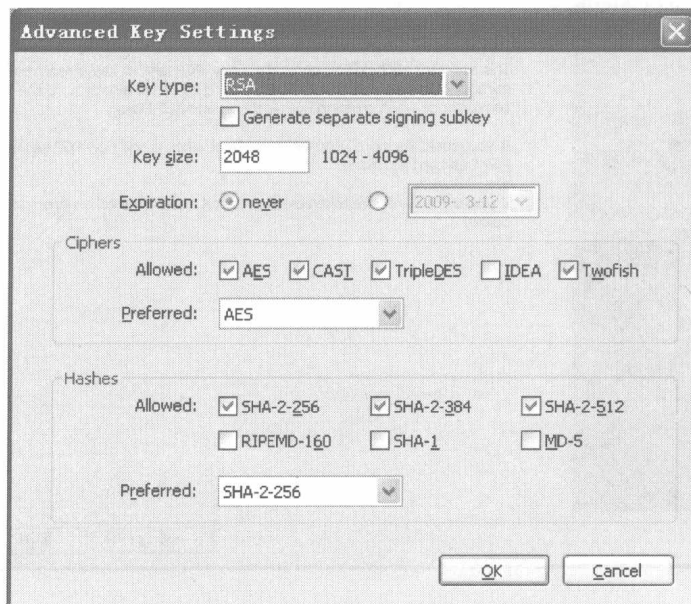


图 1-7 密钥高级配置窗口

在如图 1-6“姓名和邮件”窗口中单击【下一步】按钮, 进入如图 1-8 所示的密钥对管理密码配置窗口。