高等学校信息安全系列教材

信息安全基础综合实验教程

程红蓉　聂旭云　王　勇　编著

高等教育出版社
HIGHER EDUCATION PRESS

高等学校信息安全系列教材

信息安全基础综合实验教程

Xinxi Anquan Jichu Zonghe Shiyan Jiaocheng

程红蓉　聂旭云　王　勇　编著

高等教育出版社·北京
HIGHER EDUCATION PRESS　BEIJING

内容提要

本书是一本内容丰富、特色鲜明、实用性强的信息安全实验教程。本书着眼于当前信息安全领域的基础问题，变配置型教学为分析设计型实验教学，书中不仅有基础理论的讲解与分析，还有相应的设计型实验。全书共分8章，主要内容包括信息安全综合实验概述、数论基础实验、伪随机数产生器实验、现代加密技术实验、数字签名实验、基于OpenSSL的安全实验、数据库安全实验以及信息系统安全综合实验。每章分别对相应的实验目的、实验环境、实验内容和任务、实验报告要求等进行了详细的阐述。

本书可以作为高等学校本科信息安全原理课程的配套实验教材，也可以作为信息安全领域工程技术人员的参考用书。

图书在版编目(CIP)数据

信息安全基础综合实验教程/程红蓉，聂旭云，王勇编著. —北京：高等教育出版社，2012.2

ISBN 978-7-04-034042-6

Ⅰ.①信… Ⅱ.①程…②聂…③王… Ⅲ.①信息系统-安全技术-高等学校-教材 Ⅳ.①TP309

中国版本图书馆CIP数据核字(2011)第279921号

策划编辑	武林晓	责任编辑	刘 艳	封面设计	于文燕	版式设计	王 莹
责任校对	刘 莉	责任印制	张福涛				

出版发行	高等教育出版社	咨询电话	400-810-0598
社 址	北京市西城区德外大街4号	网 址	http://www.hep.edu.cn
邮政编码	100120		http://www.hep.com.cn
印 刷	北京市鑫霸印务有限公司	网上订购	http://www.landraco.com
开 本	787mm × 1092mm 1/16		http://www.landraco.com.cn
印 张	14	版 次	2012年2月第1版
字 数	310千字	印 次	2012年2月第1次印刷
购书热线	010-58581118	定 价	21.00元

物 料 号 34042-00

前　言

随着计算机科学技术的不断发展，计算机和网络已经成为人们工作、生活的重要组成部分。随之而产生的信息安全问题也日益受到人们的关注，成为保障国家稳定、经济发展的重要因素。为了提高我国信息安全的建设水平，提升人们的信息安全防范意识，国内许多高校设置了密码学、网络信息安全、信息对抗等专业，并开设了信息安全实验课程。本书在前人工作的基础上，本着理论与实践相结合的指导思想，着眼于当前信息安全领域的基础问题，变配置型教学为分析设计型实验教学，并采用进阶模式逐步提高实验的复杂程度，此外，在总结信息系统安全整体框架的基础上，根据实际应用场景，设计了一个信息系统安全综合实验。本教程的主要目的是使学生熟练掌握信息安全基础算法，提高他们开发安全的信息系统的能力。

本书是一本内容丰富、特色鲜明、实用性强的信息安全实验教程。全书共分 8 章，主要内容包括信息安全综合实验概述、数论基础实验、伪随机数产生器实验、现代加密技术实验、数字签名实验、基于 OpenSSL 的安全实验、数据库安全实验以及信息系统安全综合实验。每章分别对相应的实验目的、实验环境、实验内容和任务、实验报告要求等进行了详细阐述。在本书的写作过程中，我们力求做到理论与实践相结合，以期达到活学活用的教学目的，从而提高学生的思考能力和实际动手能力。为了不断提升学生在信息安全方面的理论水平和实践能力，我们将陆续出版内容更加深入的高级实验教材，以提供更加深入的综合设计实验指导。

本书由电子科技大学计算机科学与工程学院的教师合作编写。第 2 章至第 5 章由程红蓉编写，第 6 章由聂旭云编写，第 7 章由王勇编写，第 1 章和第 8 章由程红蓉、王勇和聂旭云共同编写。本书部分实验程序由杨鹏博士完成。

在本书的编写和出版过程中，得到了电子科技大学秦志光教授、刘乃琦教授、郝玉洁教授和周世杰副教授的大力支持和帮助，西安电子科技大学张卫东老师为本书提出了宝贵建议，在此对他们深表感谢。由于作者水平有限，书中难免存在疏漏之处，恳请广大读者批评指正。

作　者

2011 年 10 月

目　录

第 1 章　信息安全综合实验概述

随着社会的发展，信息在社会中扮演着越来越重要的角色，从最初的只言片语到当代的信息爆炸，信息本身不仅承担着传递知识的功能，其社会经济价值、高附加值和增值特性也逐步显现。信息技术在生产、科研、教育、医疗保健、企业和政府管理等领域中的广泛应用对经济和社会的发展产生了巨大而深刻的影响，从根本上改变了人们的生活方式、行为方式和价值观念。而对信息安全的研究，也从原始的信息保密发展到当前形成了以密码学为基础，结合被动防范和主动防御的一体化理论和方法体系。信息安全已成为信息社会必须面对的重要社会问题。近年来的计算机病毒大爆发和频繁发生的“黑客事件”给国家和企业造成了巨大的损失，给人们的生活和工作带来了不便，让人们清醒地认识到信息安全的重要性。对信息安全的认识和掌控程度不仅会影响企业和个人的利益，而且还会影响一个国家的利益，同时也能够反映出一个国家的现代化程度。

本章主要介绍信息安全的基本概念，本教程应用到的知识体系以及基本的实验平台、环境和工具。建议本章分为 6 课时，具体安排如下：1.1~1.2 节为 1 个课时；1.3~1.4 节为 2 个课时；1.5 节为 3 个课时。

1.1　信息安全概念

信息是人类社会必需的重要资源。随着计算机和网络技术的发展，当前人们在处理、传输和存储信息时都离不开计算机和网络。这就使得信息安全的内容和技术与计算机出现以前相比有了很大的变化。

1.1.1　信息安全的定义

信息安全指的是保护信息财产，以防止非授权者对信息的恶意泄露、修改和破坏，从而导致信息不可靠或无法处理等。与信息安全息息相关的还有计算机安全和网络安全。计算机安全指的是保护一个自动化的信息系统，目标是保护信息系统资源的完整性、可用性和机密性，这些信息系统资源包括软件、硬件、固件、信息/数据等。从本质上讲，网络安全就是网络上的信息安全，是指保护网络系统的硬件、软件和系统中的数据，使它们避免由于偶然的或者恶意的攻击而受到破坏、更改和泄露，保证系统能够连续、可靠、正常地运行，网络服务不中

断。广义上讲，凡是涉及网络上信息的机密性、完整性、可用性、可靠性和不可否认性的相关技术和理论都是网络安全所要研究的内容。

信息安全包括5个基本要素，即机密性、完整性、可用性、可靠性和不可否认性。

1．机密性

机密性是指信息不会泄露给非授权用户、实体或进程，不会被非法利用。信息的机密性包括传输过程中的机密性和存储的机密性。

通常使用加密的方法来保证数据传输过程中的机密性。数据加密后，只有掌握解密密钥的合法用户才能由密文恢复出明文。非授权用户即使获得了密文，也无法了解信息的内容。数据存储时的机密性可以通过访问控制来实现，管理员可以将用户和数据进行分类，定义不同的安全级别来实现数据存储的机密性。

2．完整性

完整性是指维护信息的一致性，即信息在生成、传输、存储和使用过程中不应发生人为或非人为的非授权篡改，并且能够判别出信息是否已被修改。

信息的完整性包括两个方面：①数据完整性，数据没有被未授权篡改或者损坏；②系统完整性，系统未被非法操纵，能够按既定的目标运行。一般通过访问控制来阻止篡改行为，同时通过消息摘要算法来判断数据是否被更改。

3．可用性

可用性是指保障信息资源可随时提供服务的能力，即授权用户根据需要可以随时访问所需信息。可用性是对信息资源服务功能和性能可靠性的度量，涉及物理、网络、系统、数据、应用和用户等多方面的因素，是对信息网络总体可靠性的要求。通常用访问控制机制来阻止非授权用户进入网络。

4．可靠性

可靠性是指系统在规定条件下和规定时间内完成规定功能的概率。可靠性是信息安全最基本的要素之一，系统或设备不可靠，事故不断就谈不上信息系统是否安全。目前，对于可靠性的研究基本上偏重硬件方面，然而有许多故障和事故则与软件、人员以及环境有关，因此，信息的可靠性是一个综合而复杂的问题。

5．不可否认性

不可否认性也称为不可抵赖性，即保证消息的发送者和接收者无法否认自己所进行过的操作。不可否认性通常用数字签名来实现。

现代信息安全是指信息和信息系统的安全。其内涵可以表述为：信息安全是指在秘密或关键信息的产生、传输、存储过程中不被对方获悉、修改或破坏，确保信息的可用性、机密性和完整性。其包含两层含义：一是系统安全，包括法律、政策的保护，如用户是否有合法权利，政策是否允许等；物理控制安全，如机房安全维护等；硬件运行安全；操作系统安全，如数据文件是否能够得到保护等；灾害的防范、故障的恢复；死锁的避免和解除；防止电磁信息泄露等。二是指系统中的信息安全，包括用户口令鉴别；用户存取权限控制；数据存取权限、

存取方式控制；审计跟踪；数据加密等。

1.1.2 OSI 网络安全体系结构

ISO（国际标准化组织）于 1989 年制定了 ISO 7498—2—1989《信息处理系统-开放系统互联-基本参考模型-第 2 部分：安全体系结构》。OSI（开放系统互联）安全体系结构根据 OSI 参考模型定义了安全服务、安全机制、管理及有关安全方面的其他问题，它还定义了各种安全机制及安全服务在 OSI 中的层位置。

1．安全服务

OSI 安全体系结构性地定义了 5 类安全服务：认证服务、访问控制服务、数据机密性服务、数据完整性服务和不可否认性服务。

（1）认证服务

认证服务包括对等实体认证服务和数据源认证服务。对等实体认证服务用于对两个开放系统同等层的实体建立连接，或在数据传输阶段对对方实体的合法性、真实性进行确认，以防假冒。这里的实体可以是用户或进程。数据源认证服务提供数据源的确认，即数据发送者身份的确认。它不提供防止数据中途被修改的功能。

（2）访问控制服务

访问控制服务提供防止非授权用户访问系统资源的保护服务。它既包括用户身份认证也包括用户权限认证。目前主要使用的访问控制包括自主访问控制和强制访问控制两种。实现机制具体有基于访问控制属性的访问控制表、安全标签或用户以及资源分档的多级访问控制等。

（3）数据机密性服务

数据机密性服务包括了多种保密服务。为了防止网络中系统之间交换的数据被截获或因非法存取而导致泄露，服务提供加密保护。具体包括：有连接的数据机密性保护和无连接的数据机密性保护，可选字段的数据机密性保护和业务流机密性保护。

（4）数据完整性服务

数据完整性服务用以阻止非法实体对交换数据进行修改、插入、删除以及防止在数据交换过程中的数据丢失。数据完整性服务分为可恢复的连接数据完整性、不可恢复的连接数据完整性、选择字段连接数据完整性、选择字段无连接数据完整性和无连接数据完整性。

（5）不可否认性服务

不可否认性服务用以防止发送方在发送数据后否认自己发送过此数据，或接收方在收到数据后否认自己收到过此数据或伪造接收的数据。不可否认性服务有两种：一种是针对发送方的带有数据源的不可否认性服务，即数据起源不可否认；另一种是针对接收方的带有交付证据的不可否认性服务，即数据传递不可否认。

2．安全机制

安全服务依赖于安全机制的支持。OSI 安全体系结构采用了以下 8 种安全机制：加密机

制、数字签名机制、访问控制机制、数据完整性机制、认证交换机制、业务流填充机制、路由选择控制机制和仲裁机制。

（1）加密机制

加密是确保数据安全的基本方法。在 OSI 安全体系结构中应根据加密所处的层次及加密对象的不同而采取不同的加密算法。

（2）数字签名机制

数字签名是确保数据真实性的基本方法。数字签名机制可以防止否认、伪造、篡改和冒充等安全问题。利用数字签名还可以进行用户身份认证。一般采用公钥签名体制。

（3）访问控制机制

访问控制机制是从计算机系统的处理能力方面对信息提供保护。访问控制是按照事先确定的规则决定主体对客体的访问是否合法有效。访问控制机制以如下内容为基础：访问控制表、验证信息、权力表、安全标记、试图访问的次数、试图访问的路径和访问持续的时间。

（4）数据完整性机制

数据完整性包括两种形式：一种是数据单元或域的完整性，另一种是数据单元或域的序列的完整性。破坏数据完整性的因素很多，比如信道干扰、非法入侵的篡改、遭到计算机病毒破坏等。对于不同的破坏因素可以采取不同的防范措施。

（5）认证交换机制

认证交换机制是通过交换信息来确认真实身份的机制。可用于认证交换的技术有：使用认证信息，例如口令，由发送实体提供而由接收实体验证；密码技术；利用实体的特征或其所有物；在一定条件下，选择认证机制，通常和时间标记与同步时钟、两方握手与三方握手（分别对应于单方认证和相互认证）、由数字签名与公证机制实现的不可否认性服务等技术共同使用。

（6）业务流填充机制

业务流填充机制提供对流量分析的多级保护，适用于对受到机密性服务保护的流量进行填充。通常是由保密装置在线路无信息传输时，连续地发出伪随机数序列信息，使入侵者不知道哪些是有用信息、哪些是无用信息。业务流填充机制主要用于对抗流量分析攻击。

（7）路由选择控制机制

路由选择控制机制可根据信息发送者的申请，选择特殊的安全路径，以确保数据安全。典型的应用为网络层防火墙。

（8）仲裁机制（公正机制）

在一个有多个节点进行通信的网络中，并非所有的用户都是可信任的，因此需要设置一个大家都信任的第三方——公证机构，由它提供相应的公证服务和仲裁。引入仲裁机制后，通信双方进行通信时必须经过这个公证机构来交换，以确保公证机构能得到所必需的信息，供日后仲裁使用。

3. 安全服务与安全机制的关系

安全服务和安全机制有着紧密的联系，具体而言，安全服务是由安全机制来实现的；一

种安全机制可以实现一种或者多种安全服务；一种安全服务可以由一种或者多种安全机制来实现。表 1-1 详细描述了安全服务与安全机制的关系。

表 1-1 安全服务与安全机制的关系

安全服务 \ 安全机制		加密	数字签名	访问控制	数据完整性	认证交换	业务流填充	路由选择控制	仲裁
认证	对等实体认证	√	√			√			
	数据源认证	√	√						
访问控制	自主访问控制			√					
	强制访问控制			√				√	
机密性	有连接的数据机密性	√						√	
	无连接的数据机密性	√							
	可选字段的数据机密性	√							
	业务流机密性	√					√	√	
完整性	可恢复的连接数据完整性	√			√				
	不可恢复的连接数据完整性	√			√				
	选择字段连接数据完整性	√			√				
	选择字段无连接数据完整性	√	√		√				
	无连接数据完整性	√	√		√				
不可否认性	数据源不可否认性		√		√				√
	传递过程不可否认性		√		√				√

1.2 信息安全的知识架构

信息安全技术涉及的范围比较广泛，本书主要介绍密码学、公钥基础设施、认证技术和数据库安全方面的内容。

1.2.1 密码学

密码学是信息安全最重要的基础理论之一。密码学是一门既年轻又古老的学科，它有着悠久而奇妙的历史。它在保护军事和外交通信方面的应用可追溯到几千年前。几千年来，密码学一直在不断地向前发展。而随着信息技术的飞速发展，密码学的作用也显得越来越重要。它的应用已不仅仅局限于军事、政治和外交领域，而更多的是与人们的生活息息相关，人们在网上进行购物，与他人交流，使用信用卡，进行匿名投票等，都需要密码学的知识来保护个人信

息和隐私。

密码学包括两个分支：密码编码学与密码分析学。密码编码学主要研究如何对消息进行编码，以保护信息在信道的传递过程中不被他人窃取、解读和利用；而密码分析学则恰恰相反，它主要研究如何通过密文获得相应的明文信息。这两个分支既相互对立，又相互促进。当前密码学的研究主要基于数学的有关理论与技术。基于数学理论的密码算法可分为对称密钥密码算法、公开密钥密码算法和散列函数，其中对称密钥密码体制包含了流密码和分组密码算法，公钥密码算法包括公钥加密算法和数字签名算法。

对称密钥密码算法在使用时需要预先共享密钥。对称密钥密码算法通常采用比特操作，因此比公钥密码更为高效。但公钥密码算法不用事先共享密钥，使用起来比对称密钥密码算法更为方便。通常情况下，可采用对称密钥密码算法来加密信息，而用公钥密码算法加密对称密钥密码算法的密钥，来实现密钥共享。

数字签名体制由公钥密码算法发展而来，广泛地应用于网络安全中。数字签名使用私钥进行签名，而采用公钥验证签名，私钥仅由签名者掌握，因此，可用数字签名来解决身份认证、数据完整性、不可否认性以及数据机密性等方面的安全需求。

散列函数又称为哈希（Hash）函数，是一种有效的计算函数，它把任意长的二进制字符串变换成固定长的二进制字符串，变换结果称为散列值。为了用于密码学，散列函数必须满足以下性质：①单向性，即对于任意给定的散列值 z，找到满足 $h(x) = z$ 的 x 在计算上是不可行的；②抗弱碰撞性，即已知 x，找到 y ($y \neq x$)满足 $h(y) = h(x)$在计算上是不可行的；③抗强碰撞性，即找到任意两个不同的输入 x 和 y，满足 $h(x) = h(y)$在计算上是不可行的。

散列函数主要用于数字签名和数据完整性。在数字签名中，通常先对较长的消息进行散列变换，然后对散列值进行签名。接收消息的一方同样先对消息作散列变换，再验证签名是否符合散列值。这与直接对消息进行签名相比，节省了时间和空间，因为后者通常要将消息分割为适当长度的分组，然后分别对每一分组进行签名。需要注意的是，由于散列函数满足单向性、抗弱碰撞性和抗强碰撞性，因此不可能找到两个具有相同散列值的不同消息。为保证数据完整性，首先对要保护的数据进行散列变换，然后再将散列值存储起来。当要验证数据完整性时，计算当前数据的散列值，看是否等于原先的散列值，以此验证数据的完整性，通常可用于病毒防范和软件发布。

密码学算法的实现涉及很多基本的数学算法，如大数模幂运算、求乘法逆元运算、素性检测、随机数发生器、矩阵运算等。因此，在实现密码算法之前，必须掌握这些数学算法的实现。

1.2.2 公钥基础设施

在公钥密码体制的应用当中，为保证公钥的真实性，人们引入了公钥证书。公钥基础设

施（Public Key Infrastructure，PKI）是一个普适性的系统，用来签发和管理数字证书。PKI 是一种用公钥概念与技术来实施和提供安全服务的普遍适用的安全基础设施（Carlisle Adams）；PKI 是产生、管理、存储、分发和撤销基于公开密钥密码学的公钥证书所必需的软件、硬件、人力资源、策略和处理过程的集合（IETF）；PKI 是由硬件、软件、策略和人力资源组成的系统，在其被完全并且正确地实施后，能够提供一整套的信息安全保障，这些保障对保护敏感的通信和交易是非常重要的。

使用基于公开密钥技术平台的用户建立安全通信信任机制的基础是，网上进行的任何需要提供安全服务的通信都是建立在公钥的基础之上的，而与公钥成对的私钥只掌握在通信的对方手中。这个信任的基础是通过使用公钥证书来实现的。公钥证书就是用户的身份与之所持有的公钥的结合，在结合之前，由一个可信任的权威机构——认证机构（CA）来证实用户的身份。然后由可信任的 CA 对该用户身份及对应公钥相结合的证书进行数字签名，用来证明证书的有效性。

PKI 首先必须具有可信任的认证机构，然后在公钥加密技术基础上实现证书的产生、管理、存档、发放以及撤销等功能，并包括实现这些功能的硬件、软件、人力资源、相关政策和操作规范以及为 PKI 体系中的各成员提供全部的安全服务，例如，身份认证、数据机密性、数据完整性以及不可否认性等服务。

构建实施一个 PKI 系统主要包括以下内容。

（1）认证机构

认证机构是证书的签发机构，它是 PKI 的核心，是 PKI 应用中权威的、可信任的、公正的第三方机构。

（2）证书库

证书库是证书的集中存放地，可以提供公众查询。

（3）密钥备份及恢复系统

密钥备份及恢复系统对用户的解密密钥进行备份，当丢失时可对其进行恢复，而签名密钥不能备份和恢复。

（4）证书撤销处理系统

由于某种原因需要作废、终止使用证书，可通过证书撤销列表（CRL）来实现。

（5）PKI 应用接口系统

为各种各样的应用提供与 PKI 交互的安全、一致、可信任的方式，确保所建立起来的网络环境安全可靠，并降低管理成本。

综上所述，PKI 是一种新的安全技术，它基于公开密钥密码技术，通过数字证书建立信任关系。PKI 是一种利用公钥技术实现电子商务安全的体系，是一种基础设施，可以保证网络通信、网上交易的安全。

PKI 公钥基础设施是提供公钥加密和数字签名服务的系统或平台，目的是为了管理密钥和证书。一个机构通过采用 PKI 框架管理密钥和证书可以建立一个安全的网络环境。PKI 主要包

括 4 个部分：X.509 格式的证书（X.509 v3）和证书撤销列表 CRL（X.509 v2），CA/RA 操作协议，CA 管理协议，以及 CA 政策制定。具体来说，一个典型、完整、有效的 PKI 应用系统至少应包括以下几个部分。

① 认证中心。认证中心（Certificate Authority，CA）是 PKI 的核心，CA 负责管理 PKI 结构下的所有用户（包括各种应用程序）的证书，把用户的公钥和其他信息捆绑在一起，在网上验证用户的身份。CA 还要负责用户证书的撤销登记和证书撤销列表发布。

② X.500 目录服务器。X.500 目录服务器用于发布用户的证书和证书撤销列表信息，用户可通过标准的 LDAP 协议查询自己或其他人的证书和下级证书撤销列表信息。

③ 具有高强度密码算法（SSL）的安全 WWW 服务器。进口到我国的 WWW 服务器，如 Microsoft 的 IIS、Netscare 的 WWW 服务器等，受有关限制，其 RSA 算法的模长最高为 512 位，对称算法为 40 位，不能满足对安全性要求很高的场合的需要。为解决这一问题，必须开发具有自主知识版权的 SSL 安全模块，并且把 SSL 模块集成在 Apache WWW 服务器中，Apache WWW 服务器在 WWW 服务器市场中占有 50%以上的份额，其可移植性和稳定性很高。

④ Web。Web 有 Web 客户（Client）端和 Web 服务器（Server）端两部分，分别安装在客户端和服务器端，通过具有高强度密码算法的 SSL 协议保证客户端和服务器端数据的机密性、完整性和身份认证。

⑤ 自开发安全应用系统。自开发安全应用系统是指各行业自行开发的各种具体应用系统，例如银行、证券的应用系统等。

OpenSSL 是一个开放源程序的 SSL 协议，最早由加拿大人 Eric A.Yang 和 Tim J. Hudson 开发。通过调用 OpenSSL 的库函数，可以实现一个完整的 PKI 系统，用于基于公钥证书的认证。

1.2.3 身份认证

在现实生活中，每个人的身份主要是通过各种证件来确认的，例如身份证、户口本等。认证是对网络中的主体进行验证的过程，用户必须提供他是谁的证明，例如，他是某个雇员、某个组织的代理，还是某个软件过程（如交易过程）。认证（Authentication）是证明一个对象的身份的过程，虽然与访问控制不同，但是可以与访问控制结合起来使用。

对用户进行身份认证的基本方法可以分为以下三种。

（1）根据用户所知道的信息来证明用户的身份，如口令、数字证书相应的私钥等。

（2）根据用户所拥有的物品来证明用户的身份，如智能卡、令牌卡等。

（3）直接根据独一无二的身体特征来证明用户的身份，如指纹、声音、视网膜等。

下面主要关注基于口令的身份认证和基于数字证书的身份认证。

基于口令的身份认证是最简单、最普遍的身份认证，常用于系统登录时的身份认证。早

期基于口令的身份认证的流程为：用户设置用户名和口令，并将口令存储在服务器当中。用户登录时，输入用户名和口令，服务器得到用户名和口令后与系统中存储的用户名进行比较，相同则通过认证，反之，拒绝登录。这种方式并不安全，因为口令在传输和存储过程中均采用明文的形式，极易造成口令的泄露。目前，常采用的做法是传输和存储过程中的口令均为口令的散列值，或者采取口令加验的做法。

在基于数字证书的身份认证中，用户的公钥与其身份利用数字证书绑定，用户掌握与证书上公钥相对应的私钥。认证过程中，服务器首先向用户提供一个随机数；用户以其私钥对随机数进行签名，并将签名和自己的证书提交给服务器；服务器验证证书的有效性，从证书中获得用户公钥，以用户公钥验证用户签名的随机数。

1.3 实验平台与环境

1.3.1 Windows 系统的安装和配置

1. 准备工作

① 如果计算机上已经装有 Windows 操作系统，请先确认计算机目标安装盘是否需要备份数据，一般来讲，在安装过程中原来的系统盘和桌面的数据将会被全部覆盖。

② 准备好计算机的随机光盘（品牌机自带或购买主板时的自带驱动光盘），在随机光盘里至少要包括网卡驱动程序。因为 Windows XP 已发布多年，所以很多新的网卡驱动程序未必会被集成在其中，因此应先准备好随机光盘或驱动光盘，如果都没有（例如惠普笔记本电脑就不带随机光盘），建议提前到官方网站下载对应型号的 Windows XP 网卡驱动程序，保存在 U 盘中，以防止安装完 Windows XP 后找不到网卡驱动程序。

③ 准备好 Windows XP 的安装光盘。

④ 设置 BIOS 中的启动顺序为从光盘启动，然后重启计算机。

2. 开始安装 Windows XP

① 把 Windows XP Professional 安装光盘放入光驱，设置从光驱启动后，可以看到安装选择界面有 3 个选项：安装、修复和退出。以后如果 Windows XP 遇到启动问题等就可以使用修复选项进行修复。这里需要全新安装 Windows XP，故选择第一项，按 Enter 键即可。接着出现 Windows XP 许可协议，选择接受。按 F8 键表示同意，进入如图 1-1 所示的界面。

图 1-1 所示的界面也有 3 个选项：安装（按 Enter 键）、创建分区（按 C 键）、删除分区（按 D 键），如果用户的磁盘已经分好区，就不需要再次创建或删除了。图 1-1 所示的界面表示的是未划分空间，要创建两个分区，只需要按下 C 键即可开始利用空闲空间创建分区。

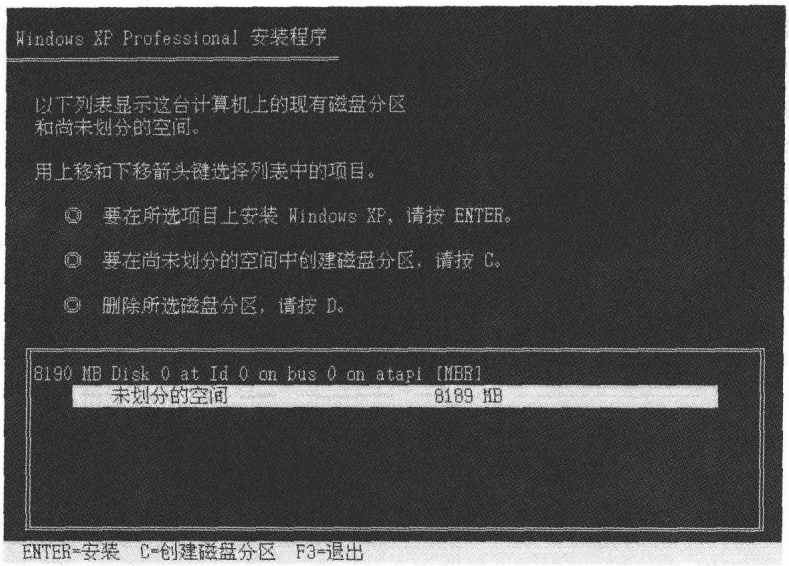

图 1-1　Windows XP Professional 安装分区选择界面

② 创建分区界面如图 1-2 所示，只需要输入分区大小并按 Enter 键即可创建一个分区。如果不需要创建分区，可直接跳过本步骤。

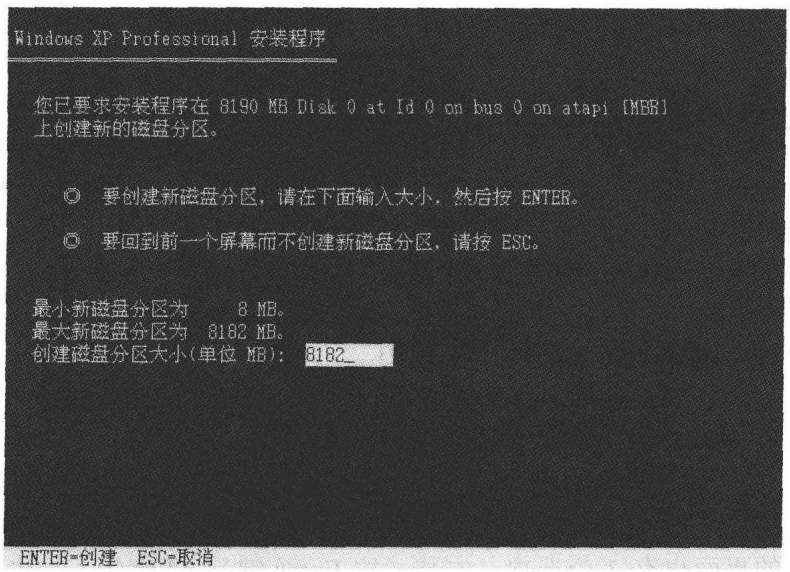

图 1-2　Windows XP Professional 创建分区界面

③ 用上、下方向键选择安装在 C 盘（注意：请再次确认 C 盘没有重要数据，如有请退出安装进行备份）。选择 C 盘后按 Enter 键即可。

④ 这时，安装程序将会格式化 C 盘，格式化完成后会开始复制安装文件。复制完成后，安装程序会自动重启机器，进入界面安装模式。安装过程中会陆续弹出设置或选择对话框。

⑤ 在如图 1-3 所示的对话框中，选择区域和语言。

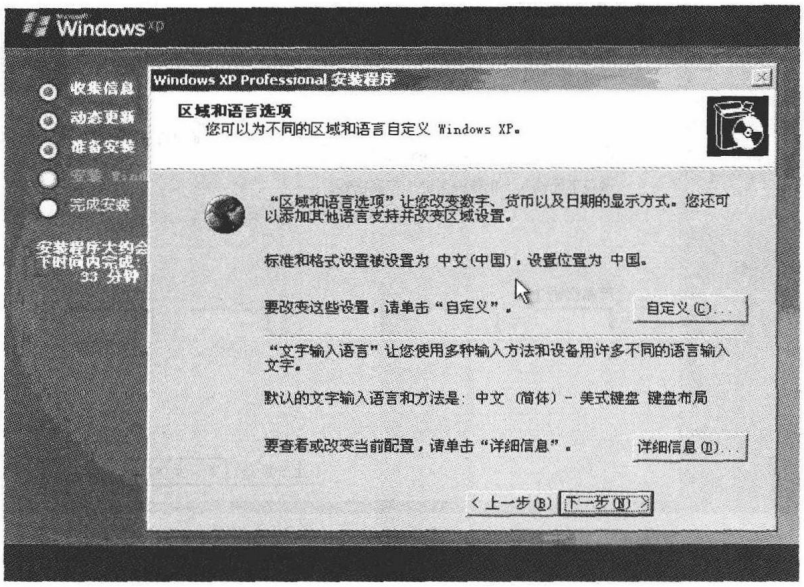

图 1-3 “区域和语言选项”对话框

⑥ 在如图 1-4 所示的对话框中，输入姓名和单位。

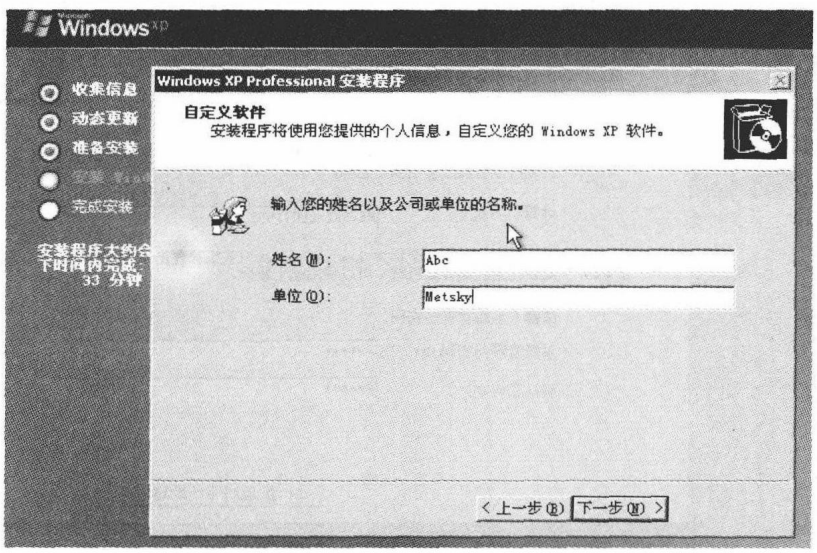

图 1-4 “自定义软件”对话框