21世纪应用型本科计算机专业实验系列教材

网络安全实验教程

总主编　常晋义
主　编　乐德广

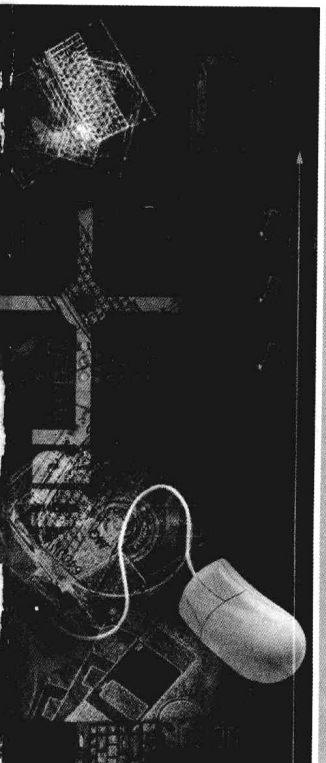
YINGYONGXINGBENKEJISUANJIZHUANYESHIYANXILIEJIAOCAI

南京大学出版社

21世纪应用型本科计算机专业实验系列教材

网络安全实验教程

总主编　常晋义
主　编　乐德广
主　审　屠立忠



南京大学出版社

图书在版编目(CIP)数据

网络安全实验教程/乐德广主编. —南京:南京大学出版社,2010.12
21世纪应用型本科计算机专业实验系列教材
ISBN 978-7-305-07912-2

Ⅰ. ①网… Ⅱ. ①乐… Ⅲ. ①计算机网络—安全技术—高等学校—教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2010)第239899号

出版发行 南京大学出版社
社　　址 南京市汉口路22号　　邮编 210093
网　　址 http://www.NjupCo.com
出 版 人 左　健

丛 书 名 21世纪应用型本科计算机专业实验系列教材
书　　名 网络安全实验教程
总 主 编 常晋义
主　　编 乐德广
主　　审 屠立忠
责任编辑 谢　靖　　编辑热线 025-83686531

照　　排 南京玄武湖印刷照排中心
印　　刷 南京紫藤制版印务中心
开　　本 787×960　1/16　印张 17.75　字数 370千
版　　次 2010年12月第1版　2010年12月第1次印刷
ISBN 978-7-305-07912-2

定　　价 31.00元
发行热线 025-83594756　83686452
电子邮箱 Press@NjupCo.com
Sales@NjupCo.com(市场部)

21世纪应用型本科计算机专业实验系列教材

序　言

实践教学是巩固基本理论和基础知识、提高学生分析问题和解决问题能力的有效途径，是应用型本科院校培养具有创新意识的高素质应用型人才的重要环节。

计算机专业课程的特点，使得实验教学无论在掌握计算机学科理论和原理，还是培养学生运用计算机解决应用问题的能力方面，都占有十分重要的位置。为了进一步推进实践教学质量的提高，由江苏省应用型本科院校联合组织来自计算机专业教学一线的教师，编写了“21世纪应用型本科计算机专业实验教材”。教材涵盖了计算机基础训练、软件基础训练、硬件基础训练、信息系统与数据库训练、网络工程训练、综合设计训练等六大重要实践体系，包括了实验指导和实验报告、实训练习等组成部分，为应用型本科计算机专业教学提供教学参考与交流平台。

实验指导和实验报告是教材的主体。实验指导用来指导学生完成一些基本功能的练习，为最后完成实验报告打下基础。在此基础上，通过实验教师的辅导，学生独立完成实验报告中综合性的实验任务。实验的安排按照“点—线—面”循序渐进的方式进行。“点”即验证性实验，实现课程中需要学生动手做的实验；“线”指设计性实验，应用一个知识点解决实际问题；“面”是综合性实验，应用几个知识点解决实际问题。

实训练习用于课外提高，题目内容提高了复杂性和综合性，注意了应用背景的描述，注重了知识的综合运用和应用环境的设计。结合学科领域新技术、新方法，增加综合性、设计性、创新性实验，将最新科技成果融入到实验教材和实验项目中，有利于学生创新能力培养和自主训练。

实验教材的编写出版得到了江苏省应用型本科院校的支持与积极参与，各院校精心挑选经验丰富的教师参与教材编写，并对选择的实验体系与实验内容进行了广泛讨论和系统优化，使其具有代表性、先进性和实用性。教材编写中力求简明实用、条理清晰，突出实验原理、实验方法，便于学生对实验原理的理解和指导实验操作。体现了认知上的循序渐进，利于教师因材施教和学生能力

培养，以适合应用型人才培养的需要。

实验教材的编辑出版凝聚了江苏省应用型本科计算机专业教学一线教师的经验和智慧，也是应用型本科计算机专业教学成果的一次展示。在出版、使用和教学中，编委会将广泛听取读者的意见和建议，不断探索，总结经验，逐步完善教材体系，不断更新教学内容，充分发挥实验教材在应用型人才培养中的作用。

真诚希望使用本系列教材的教师、学生和读者朋友提出宝贵意见或建议，以便进一步修订，使教材不断完善。编委会的邮箱是：testbooks@163.com。

编委会

2010 年 7 月

前　言

随着互联网的飞速发展，以及各种网络应用（如电子政务、电子商务等）的普及，网络安全问题日益突出，例如近年来多次在全球范围内爆发的各种蠕虫病毒及黑客攻击事件，对个人和社会经济造成了巨大的损失。为了保证互联网的安全通信，需要有大量的研究人员和工程师致力于网络安全的技术研究、产品开发和管理与维护，因此社会对网络安全专业人才的需求也与日俱增。

为了满足这种需求，目前国内外许多高等院校纷纷将网络安全作为计算机专业的必修专业课程，甚至开设了网络安全专业，以培养网络安全方面的专业人才。长期以来，编者一直从事网络安全方面的教学、科研及其技术产品开发工作，经过编者多年的网络安全教学实践发现网络安全不仅是一门理论性课程，也是一门具有很强实践性的课程，学生对于网络安全概念与原理的理解深度往往取决于其在实践操作中的感性认识程度。为此，我们在“21世纪应用型本科计算机专业实验教材编委会”的组织下编写了网络安全实验教程，以满足高校在网络安全专业人才培养中的实验教学需求。

网络安全作为一门综合性课程，课程内容覆盖面广，不同学院和专业开设的网络安全课程往往有不同的侧重点。为此，本书基于 P2DR 模型覆盖了网络安全的防御、检测和响应三大领域，以满足不同学院和专业的网络安全课程的实验教学需求。另外，本书的实验设计注意层次性，保证实验指导、实验报告和综合实训三位一体，有机结合，体现由浅入深、逐步提高的学习过程。其中，实验指导目的明确、原理清晰、内容具体，便于学生自学。实验报告要求在实验指导的基础上扩展和引深，引导和启发学生进一步的动手和思考，并提高学生的实际应用能力。实训中注重提高学生的网络安全技术综合运用能力和解决实际网络安全问题的能力，方便学生课外练习使用。因此，我们根据以上设计考虑将本书分 9 章共 18 个实验项目和 1 个综合实训项目。

第 1 章学习和掌握网络安全中的第一个环节，如何利用密码技术对计算机系统的各种数据信息进行加密保护实验，实现网络安全中的数据信息保密性服务。该章属于网络安全防御领域，包含 3 个实验项目。

第 2 章学习和掌握网络安全中的第二个环节，如何利用身份认证技术对计算机和网络系统的各种资源进行身份认证保护实验，实现网络安全中的信息鉴别性服务。该章属于网络安全防御领域，包含 2 个实验项目。

第 3 章学习和掌握网络通信中合法用户数据信息的安全传输，如何利用密码技术对网络通信中传输数据进行加密保护，并对通信用户和传输数据进行身份认证实验，实现网络安

全中的保密性、鉴别性和完整性服务。该章属于网络安全防御领域，包含 3 个实验项目。

第 4 章学习和掌握如何利用防火墙技术对网络通信中的各种传输数据进行鉴别和控制实验，实现网络安全中的保密性和鉴别性服务。该章属于网络安全防御领域，包含 2 个实验项目。

第 5 章学习和掌握各种网络安全扫描技术的操作实验，并能综合运用网络安全扫描技术进行网络安全分析，有效避免网络攻击行为。该章属于网络安全检测领域，包含 2 个实验项目。

第 6 章学习各种网络监听技术的操作实验，以及掌握能够利用网络监听工具进行分析、诊断、测试网络安全性的能力。该章属于网络安全检测领域，包含 2 个实验项目。

第 7 章学习和掌握各种入侵检测系统的基本原理、操作与应用实验。该章属于网络安全检测领域，包含 2 个实验项目。

第 8 章学习并掌握数据恢复的基本操作和方法，包括磁盘克隆与镜像、以及删除文件恢复等。该章属于网络安全响应领域，包含 2 个实验项目。

第 9 章进一步学习和掌握网络安全的各种技术原理与应用，并通过在一个实际网络通信系统中的综合运用，实现有效设计和部署。

在本书具体的每个实验项目中，我们分别从实验目的、实验原理、实验环境、实验内容、实验步骤和实验报告 6 个方面进行设计，并力求做到实验目的明确、实验原理清晰、实验环境简单、实验内容具体、实验步骤详细和实验报告灵活。

首先，本书的每个实验项目通过明确的实验目的、清晰的实验原理、具体的实验内容和详细的实验步骤，指导学生有目的、有步骤地完成各项实验操作，由浅入深地引导学生发现问题和解决问题，加强其实践动手能力和对理论知识的理解。

其次，由于实验课程教学要与具体的实验环境和实验设备结合。因此，本书的编写注意到网络安全实验对实验环境和实验设备特殊需要的特点，充分考虑可用性和通用性。所设计的实验环境简单而又切合实际，每个实验项目所需的软硬件采用了普通的硬件设备和通用操作系统与应用软件，不但可以在其现有的网络实验环境上不加修改或只做少量调整就可用于网络安全实验课程中，而且便于在理论课堂中进行现场演示操作，使得教师乐于用，学生方便操作。另外，每个实验项目设计的实验任务合理，每个实验在时间上适合在课堂上完成。

最后，每个实验项目中的实验步骤和实验报告要求灵活，突出学生的主体性，引导和启发学生动手和思考，设置部分实验内容的步骤为间断型，留下学生思考的余地，特别在有多种途径的地方，留下让学生自己思考和选择的余地。

总之，本书以促进学生综合能力培养为出发点，符合网络安全专业人才培养目标及课程教学的要求，着重应用技能的培养。取材合适，深度适宜，篇幅恰当，符合教学规律，富有启发性，有利于激发学生学习兴趣，适应素质教育的需要，全面培养学生知识、能力和素质。

本书在编写出版过程中得到了“21 世纪应用型本科计算机专业实验教材编委会”各位主编和编委老师的大力支持和帮助，常晋义教授和徐文彬教授更给予编者深切的关怀与鼓励。特别要感谢屠立忠教授，他在百忙之中对该教材进行了仔细的审阅，并提出了许多宝贵的意见。此外，在本书的编写过程中还得到了其他众多网络安全专家的指导、审阅及宝贵的意见和建议，在此一并表示真诚的感谢。

本书的所有实验项目已经在相应的实验环境下测试通过，并已经在本科生的网络安全课程的实验教学中运用。本书作为教材，在具体实验授课中，实验教师可以根据具体的理论课程情况和课时安排进行取舍，选择一部分给学生做，也可以给不同需求的学生做不同层次的实验。为了便于教学和实验操作，本书配有各实验项目所需要的程序和代码，学生可以直接使用这些程序和代码来完成相应的实验项目操作。由于编者水平有限，书中难免疏漏和错误之处，如果发现书中有任何问题或者有改进意见，请读者和编者直接联系：ledeguang@gmail.com，给予批评指正，以期再版时修订。

编 者

2010 年 10 月

目　录

第 1 章　数据安全与保密 …… 1

实验 1.1　Word 文件加解密实验 …… 1
实验 1.2　WinRAR 数据加解密实验 …… 9
实验 1.3　dsCrypt 数据加解密实验 …… 16

第 2 章　身份认证 …… 21

实验 2.1　Windows 系统中基于帐户/密码的身份认证实验 …… 21
实验 2.2　PAP/CHAP 网络身份认证实验 …… 32

第 3 章　网络安全通信 …… 46

实验 3.1　SSH 网络安全通信实验 …… 46
实验 3.2　基于 PGP 的 Email 安全通信实验 …… 60
实验 3.3　VPN 安全通信实验 …… 77

第 4 章　防火墙 …… 101

实验 4.1　基于 Windows 的 NAT 防火墙实验 …… 101
实验 4.2　基于 Linux 的 NAT 防火墙实验 …… 121

第 5 章　网络安全扫描 …… 141

实验 5.1　Ping 主机扫描实验 …… 141
实验 5.2　SuperScan 端口扫描实验 …… 155

第 6 章　网络监听技术 …… 172

实验 6.1　TCPdump 网络监听实验 …… 172
实验 6.2　Wireshark 网络监听实验 …… 191

第 7 章　入侵检测 …… 208

实验 7.1　Tripwire 网络入侵检测实验 …… 208

实验 7.2 Snort 网络入侵检测实验 …… 225

第 8 章 数据恢复 …… 240

实验 8.1 WinHex 磁盘克隆与镜像实验 …… 240
实验 8.2 EasyRecovery 删除文件恢复实验 …… 252

第 9 章 综合实训 …… 263

实验 9.1 网络安全系统设计与实现 …… 263

参考文献 …… 271

第 1 章　数据安全与保密

随着互联网时代的到来，计算机不再是以单机的形式存在，它已经是成为整个互联网的一分子。由于现有的互联网不是一个绝对安全的网络，各种病毒和木马就常常入侵我们的计算机系统，篡改、删除或窃取存储在计算机系统上的各种数据信息。因此，如何保护计算机系统上的数据信息是网络安全中需要面对和解决的基本问题。目前，对数据进行加密变换是对计算机系统的数据信息进行安全保护的最实用和最可靠的方法。在本章中，我们将学习和掌握网络安全中的第一个环节，如何利用密码技术对计算机系统的各种数据信息进行加密保护实验，实现网络安全中的数据信息保密性服务。

实验 1.1　Word 文件加解密实验

【实验目的】

(1) 了解和学习 Word 文件加密原理与技术。
(2) 学习和掌握 Word 文件加密方法。
(3) 思考：
① Microsoft Word 2003 能为其文档提供哪些安全服务？
② Microsoft Word 2003 采用哪种加密算法？
③ Microsoft Word 2007 采用的加密算法与 Word 2003 有什么不同？

【实验原理】

在现实网络通信中，威胁和攻击的形式一般分为两类：① 对通信实体的威胁和攻击；② 对数据信息的威胁和攻击。其中，对数据信息的人为故意威胁，称为信息攻击，简称攻击。常见的攻击主体包括黑客、未授权者和非法入侵者，他们的攻击手段随着能力、目的、时间和工具等的不同而千变万化。一般而言，攻击的主要目的是破坏数据信息的机密性、完整性、真实性、可用性和可控性。为此，我们常常利用密码技术来防止攻击者对数据信息的威胁和攻击。

1. *数据保密原理与技术*

计算机密码学是研究计算机信息加密、解密及其变换的科学，是数学和计算机的交义学科，也是一门新兴的学科。随着计算机网络安全和计算机通讯技术的发展，计算机密码学得

到前所未有的重视并迅速普及和发展起来。目前，它已成为计算机安全主要的研究方向，也是计算机安全课程教学中的主要内容。

(1) 数据保密安全基本原理

计算机系统中存储的数据信息及其在网络信道中传输的数据信息的安全问题，主要是数据信息的保密性，即防止非法地获悉数据；二是数据的完整性，即防止非法地修改数据。

解决上述问题的基础是现代密码学。现代密码学所采用的加密方法通常是用一定的数学计算操作来改变原始信息。用某种方法伪装消息并隐藏它的内容，称作加密(Encryption)。待加密的消息称作明文(Plaintext)，所有明文的集合称为明文空间；被加密以后的消息称为密文(Ciphertext)，所有密文的集合称为密文空间。而把密文转变成明文的过程，称为解密(Decryption)。其中，加解密运算是由一个算法类组成的，这些算法的不同运算可用不同的参数表示，这些参数称作密钥，密钥空间是所有密钥的集合。因此，一个密码系统包含明文空间、密文空间、密钥空间和算法及其密钥。简单加密和解密过程如图 1.1.1 所示。

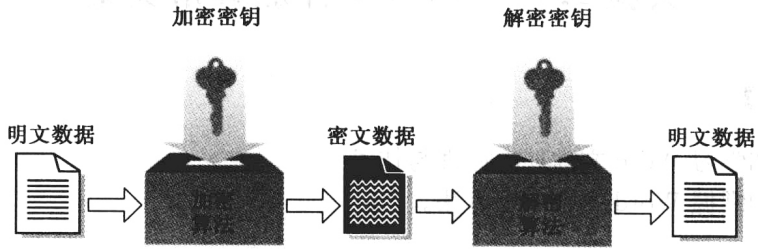


图 1.1.1 数据加解密基本原理

从图中可以看出，密码系统的两个基本单元是算法和密钥。其中，算法是相对稳定的，视为常量；密钥则是不固定的，视为变量。密钥安全性是密码系统安全的关键。为了密码系统的安全，频繁更换密钥是必要的；在密钥的分发和存储时，应当特别小心。发送方用加密密钥，通过加密算法或设备，将信息加密后发送出去。接收方在收到密文后，用解密密钥通过解密算法将密文解密，恢复为明文。如果传输中有人窃取，他只能得到无法理解的密文，从而对信息起到保密作用。

(2) 数据加密技术

在密码系统中，算法与相应的密钥构成一个密码体制。根据密钥的特点，密码体制分为对称密钥密码体制与公钥密码体制。其中，对称密钥密码体制也称为私钥密码体制或单密钥密码体制。在对称密钥密码体制中，加密密钥与解密密钥是相同的或从一个容易推出另一个。公钥密码体制也称为非对称密钥密码体制或双密钥密码体制。在公钥密码体制中，加密密钥与解密密钥是不同的或从一个很难推出另一个。

根据加密的不同方式，对称密钥密码可分为分组密码(Block Cipher)和流密码(Stream Cipher)。其中，分组密码将明文按一定的位长分组，输出也是固定长度的密文。明文组经过加密运算得到密文分组。解密时密文分组经过解密运算还原成明文分组。分组密码的优点是密钥可以在一定时间内固定，不必每次变换，因此给密钥配发带来了方便。DES(Data Encryption Standard)密码是 1977 年由美国国家标准局公布的第一个分组密码。目前，国际上公开的分组密码算法有 100 多种，比如，Lucifer、IDEA、SAFER 等，以及 2000 年 2 月制定和评估的高级数据加密标准 AES(Advanced Encryption Standard)。

流密码又称序列密码，它将明文信息按单个字符(一般以二进制位 bit 为单位)一个一个地进行加密运算产生密文。在流密码中，通常使用称为密钥流的一个位序列作为密钥对明文逐位应用“异或”运算。有些序列密码基于一种称作线形反馈移位寄存器(Linear Feedback Shift Register，LFSR)的机制，该机制生成一个二进制位序列。常用的流密码算法包括 RC4、A5、软件优化加密算法(Software Optimized Encryption Algorithm，SEAL)、SNOW2.0、WAKE 和 PKZIP 等算法。与分组密码相比，序列密码具有更快速度。

在对称密钥密码体制中，解密密钥与加密密钥相同或容易从加密密钥推导出，加密密钥的暴露会使系统变得不安全，因此使用对称密钥密码体制在传送任何密文之前，发送者和接收者必须使用一个安全信道预先通信传输密钥，称为安全密钥交换，这在实际通信中做到这一点很困难。公钥密码体制能很好地解决对称密钥密码体制中的安全性问题。在公钥密码中，解密密钥和加密密钥不同，从一个难于推出另一个，解密和加密是可分离的，加密密钥是可以公开的。公钥密码系统的观点是由 Diffie 和 Hellman 在 1976 年首次提出的，称为 Diffie-Hellman 算法，它使密码学发生了一场革命。1977 年由 Rivest，Shamir 和 Adleman 提出了第一个比较完善的公钥密码算法，这就是著名的 RSA 算法。自那时起，人们基于不同的计算问题，提出了大量的公钥密码算法，代表性的算法有 DSA 算法、Merke-Hellman 背包算法和椭圆曲线算法等。

2. Microsoft Word 加密安全保护

Microsoft Word 软件是经常用的办公软件之一，它除了可以编辑文档外，还可以对 Word 文档自身进行加密，以确保文档的安全。

(1) Microsoft Word 加密原理与技术

Microsoft Word 采用 RC4 对称流加密技术实现对文档信息的加密保护。RC4 是 Ronald Rivest 在 1987 年为 RSA Data Security，Inc. 开发的一种流加密对称密钥算法。RC4 使用可变密钥长度来初始化 256 字节的状态表。状态表将用于随后生成伪随机字节，然后再用于生成伪随机流。状态表中的每个元素至少交换一次。RC4 能够使用 1 到 2048 位的密钥。由于过去的出口限制，RC4 密钥常常被限制在 40 位，但有时也用作 128 位密钥。RC4 在许多商业软件包中广泛使用。

(2) Microsoft Word 文档的保护方式

Microsoft Word 2003 程序提供了多种不同的方法来保护文档。这些方法是操作系统级别功能的补充，并与系统级功能一起使用。表 1.1.1 列出了 Microsoft Word 2003 为文档提供的 4 种不同保护方式。

表 1.1.1 Micorsoft Word 2003 文档保护类型

文档保护类型	描　　述
文件打开保护	此保护需要用户输入密码才能打开文件。文档被加密，因此只有知道密码的用户才能阅读文档。
文件修改保护	在此保护模式下，用户不输入密码便可打开文档，但必须输入密码才能执行或保存对文档的更改。
建议采用的只读保护	在用户打开文件时，系统会提示用户以只读状态打开文件，但用户可以选择以不带密码的只读/写入模式打开文件。
数字签名	利用数字签名技术对文件、文档、表达式、工作表及其他数据文件进行签署。如果对整个文件进行签署，则可保证文件在签署后不能再进行修改。

在表 1.1.1 中，“文件修改保护”和“建议只读保护”选项不对文档进行密码加密。因此，此安全性有可能遭到攻击。如果存在此风险，建议加密文档。

(3) Microsoft Word 支持的加密类型

表 1.1.2 列出了 Micorsoft Word 2003 支持的加密类型及其描述。

表 1.1.2 Micorsoft Word 2003 加密类型

加密类型	描　　述
不可靠的加密(XOR)	此算法快速而且简单，但无法提供最好的安全性。密钥长度：该算法不支持更改密钥长度。
Microsoft Office 97/2000 兼容加密	它是 Word 2003 默认密码算法，从而确保向后兼容性和国际性的文档可移植性。密钥长度：该加密方法不支持更改密钥长度。
Microsoft Base Cryptographic Provider	它是一个通用的加密服务提供程序，支持数字签名和数据加密。密钥长度：40—56(默认 40)。
Microsoft Base DSS and Diffie-Hellman Cryptographic Provider	支持 Diffie-Hellman (D-H)密钥交换(40 位数据加密标准派生品)、安全哈希算法(SHA)哈希、数字签名标准(DSS)数据签名和 DSS 签名验证。密钥长度：40—56(默认 40)。

（续表）

加密类型	描　　述
Microsoft Enhanced DSS and Diffie-Hellman SChannel Cryptographic Provider	支持哈希、DSS 数据签名、生成 Diffie-Hellman(D-H)密钥、交换 D-H 密钥以及导出 D-H 密钥。此加密服务提供程序支持针对 SSL3 和 TLS1 协议派生密钥。密钥长度：40—128(默认 40)。
Microsoft DSS Cryptographic Provider	通过使用安全哈希算法(SHA)和数字签名标准(DSS)算法来支持哈希、数据签名和签名验证。密钥长度：40—56(默认 40)。
Microsoft Enhanced Cryptographic Provider	支持与 Microsoft Base Cryptographic Provider 相同的功能。增强提供程序通过更长的密钥和其他算法来提供更强的安全性。密钥长度：40—128(默认 128)。
Microsoft Strong Cryptographic Provider	它将用作默认的 RSA Full 加密服务提供程序。它支持 Microsoft Enhanced Cryptographic Provider 的所有算法和所有相同的密钥长度。为了向后兼容，它使用与 Microsoft Base Cryptographic Provider 相同的默认密钥长度。密钥长度：40—128(默认 128)。

【实验环境】

1. 实验配置

本实验所需的软硬件配置如表 1.1.3 所示。

表 1.1.3　Word 文件加解密实验配置

配　置	描　　述
硬件	CPU：Intel Core i5 750 2.66GHz；主板：Intel P55；内存：2G DDR3 1333
系统	Windows 操作系统：Windows XP Professional SP3
应用软件	Microsoft Office 2003

2. 实验环境

本实验的环境如图 1.1.2 所示。

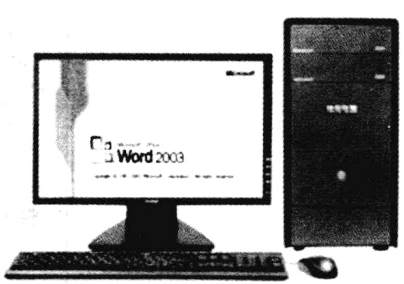


图 1.1.2　Word 文件加解密实验环境

【实验内容】

（1）Microsoft Word 文档加密保护。

（2）Microsoft Word 文档修改保护。

（3）加密 Microsoft Office 其他类型文档。

【实验步骤】

1. Word 文档加密保护

(1) 检查安装 Microsoft Office 2003 软件

(2) 打开需要加密的 Word 文档

在 Windows 系统下用鼠标双击需要加密的 Word 文档，例如："销售合同. doc"，如图 1. 1. 3所示。

图 1. 1. 3 保密文档

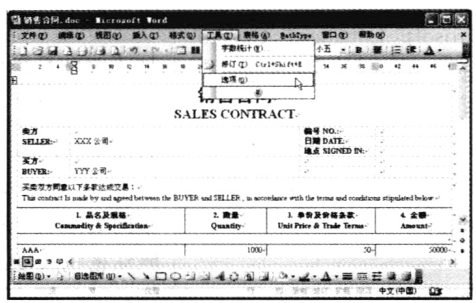


图 1. 1. 4 Word 工具选项

(3) Word 选项设置

在 Word 操作界面的"工具"菜单上，单击"选项…"，如图 1. 1. 4 所示。

(4) Word 安全性设置

在弹出的"选项"对话框里，单击"安全性"选项卡，如图 1. 1. 5 所示。

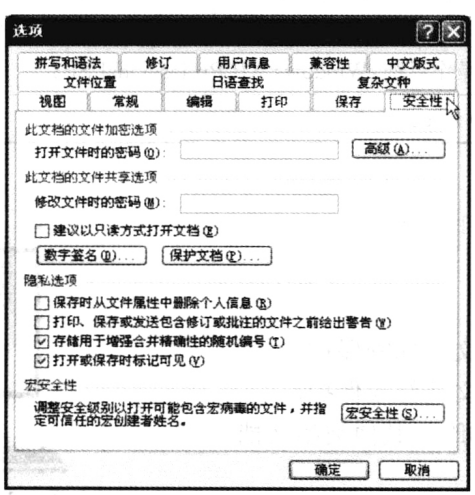


图 1. 1. 5 选项对话框