21世纪应用型本科计算机专业实验系列教材

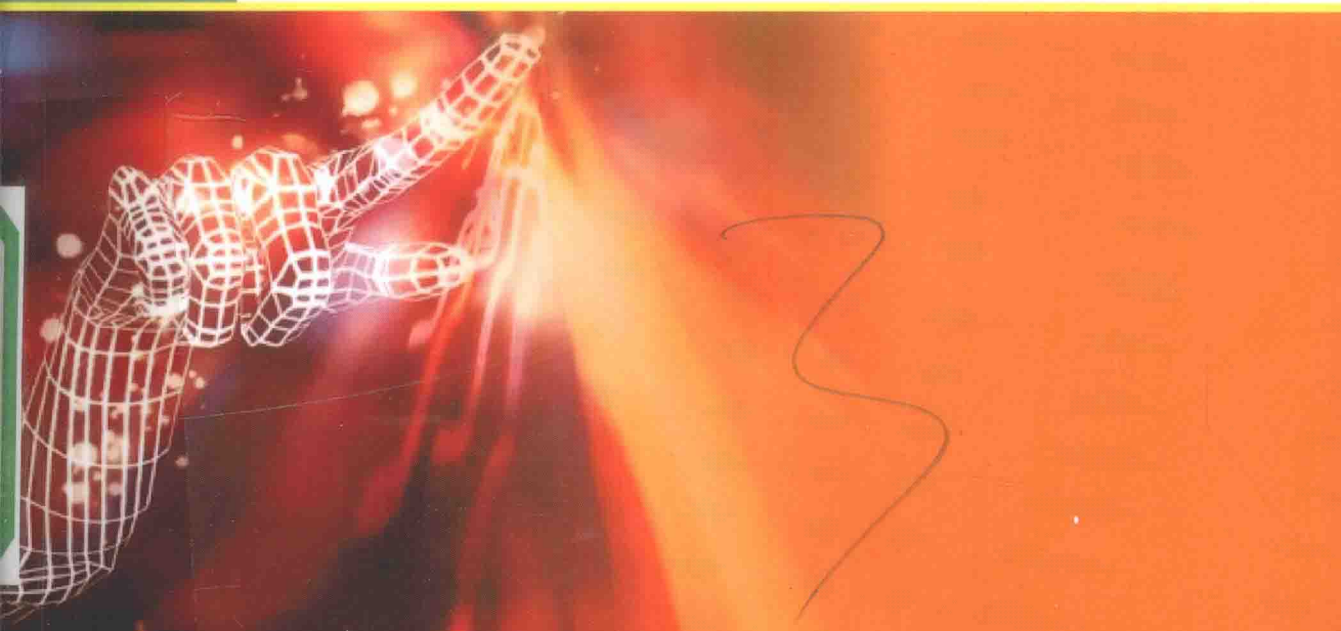
江苏省高等学校精品教材

网络安全实验教程

第二版

主编 乐德广

YINGYONGXINGBENKEJISUANJIZHUANYESHIYANXILIEJIAOC



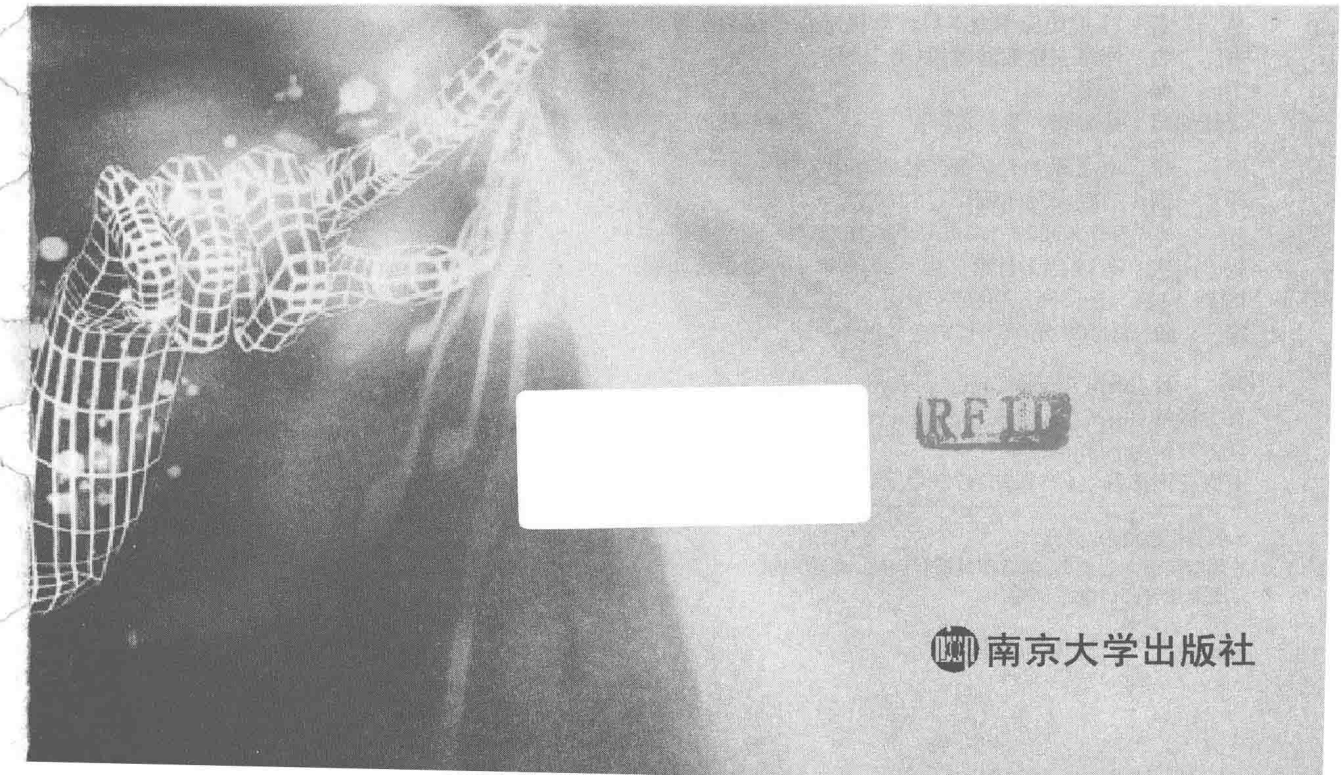
南京大学出版社

计算机专业实验系列教材
学校精品教材

网络安全实验教程

第二版

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. —2 版. —南京：南京大学出版社，2016.1

21 世纪应用型本科计算机专业实验系列教材

ISBN 978-7-305-16407-1

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(2016)第 009942 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
出 版 人 金鑫荣

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(第二版)
主　　编 乐德广
责任编辑 揭维光　吴　汀　　编辑热线 025-83686531

照　　排 南京理工大学资产经营有限公司
印　　刷 南京人民印刷厂
开　　本 787×960　1/16　印张 16.5　字数 360 千
版　　次 2016 年 1 月第 2 版　2016 年 1 月第 1 次印刷
ISBN 978-7-305-16407-1
定　　价 34.00 元

网　　址：http://www.njupco.com
官方微博：http://weibo.com/njupco
官方微信号：njupress
销售咨询热线：(025)83594756

* 版权所有，侵权必究
* 凡购买南大版图书，如有印装质量问题，请与所购图书销售部门联系调换

前　言

随着互联网安全的日益重要，对网络安全专业人才的需求也与日俱增。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综合性课程，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。

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。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和删除文件恢复等。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，及在一个实际网络通信系统中的综合运用与有效设计和部署。

在本书的每个实验项目中，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六个方面进行设计，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。

与第一版教程相比，本书从以下几方面进行了改进：① 在实验内容方面，采用新的操作系统和应用，使本书的实验内容符合当前主流的操作系统与应用；② 在实验环境方面，采用虚拟化技术实现实验所需的网络环境，不但实验院校不需要网络安全实验设备等硬件投入，而且实验教师无需进行复杂的专业实验设备培训；③ 在实验步骤方面，学生在实验课中无需进行实验环境部署，把有限的实验课时间花在关键的实验步骤上，提高实验效率。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。

本书在编写出版过程中得到了各位编写老师的大力支持和帮助，常晋义老师和徐文彬老师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

2016年1月

试读结束，需要全本PDF请购买 www.ertongbook.com

目　录

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份子。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用户的计算机系统，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 2010 能为其文档提供哪些安全服务？
② Microsoft Word 2010 采用哪种加密算法？
③ Microsoft Word 2010 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叉学科，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，即防止非法获悉数据；二是数据的完整性，即防止非法修改数据。

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。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。

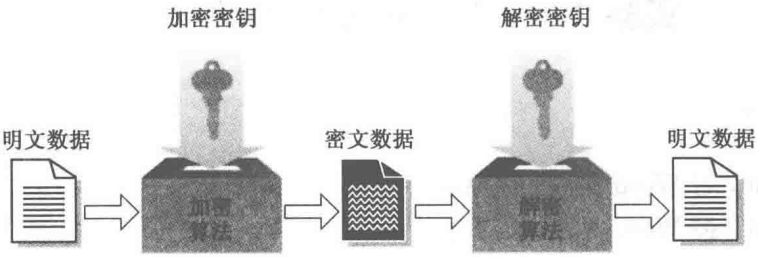


图 1.1.1 数据加解密基本原理

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；且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,例如,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)。对这些算法感兴趣的读者可在Schneier的Applied Cryptography:Protocals,Algorithms, and Source Code in C一书和会议论文集Fast Software Encryption中找到它们的详细论述。

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 2010默认采用密钥长度为128位的高级数据加密标准AES算法实现对Word数据的加密保护。AES加密是可用的业界最强标准算法,并由美国国家安全局(NSA)选择用作美国政府的标准。早期Microsoft Word 2003则采用RC4对称流加密技术实现对Word文档信息的加密保护。

(2) Microsoft Word文档的保护方式

Microsoft Word 2010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 2010 为文档提供的五种不同保护方式。

表 1.1.1 Microsoft Word 2010 文档保护类型

文档保护类型	描　　述
标记为最终状态	此保护可以令 Word 将文档标记为只读模式，Word 在打开一个已经标记为最终状态的文档时，将自动禁用所有编辑功能。
用密码进行加密	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。
限制编辑	限制编辑功能提供了三个选项：格式设置限制、编辑限制、启动强制保护。其中，格式设置限制可以有选择地限制格式编辑选项，用户可以点击其下方的“设置”进行格式选项自定义；编辑限制可以有选择地限制文档编辑类型，包括“修订”、“批注”、“填写窗体”以及“不允许任何更改(只读)”；启动强制保护可以通过密码保护或用户身份验证的方式保护文档。
按人员限制权限	按人员限制权限可以通过 Windows Live ID 或 Windows 用户帐户限制 Word 文档的权限。用户可以选择使用一组由企业颁发的管理凭据或手动设置“限制访问”对 Word 文档进行保护。
添加数字签名	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，限制编辑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 支持的加密类型及其描述。

表 1.1.2 Micorsoft Word 加密类型

加密类型	描　　述
密码保护的 Word 2007—2013 文件的加密类型	允许在可用的加密服务提供程序 (CSP) 中为 Word 2007—2013(Open XML)文件指定加密类型。Word 可用的加密算法取决于可通过 Windows 操作系统中的 API(应用程序编程接口)访问的算法。Office 2010 除了支持加密 API (CryptoAPI) 之外，还支持 CNG(CryptoAPI：下一代加密技术)。Word 2010 支持 CNG 以下加密算法：AES、DES、DESX、3DES、3DES_112 和 RC2。

试读结束，需要全本PDF请购买 www.ertongbook.com

（续表）

加密类型	描　　述
受密码保护的 Word 97—2003 文件的加密类型	允许在可用的加密服务提供程序（CSP）中为 Word 97—2003（二进制）文件指定加密类型。在使用此设置时支持的加密算法是 RC4。

【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 i7 4790 3.6GHz；主板：Intel Z97；内存：8G DDR3 1333
系统	Windows
应用软件	Vmware Workstation；Microsoft Office 2010

2. 实验环境

本实验的环境如图 1.1.2 所示。

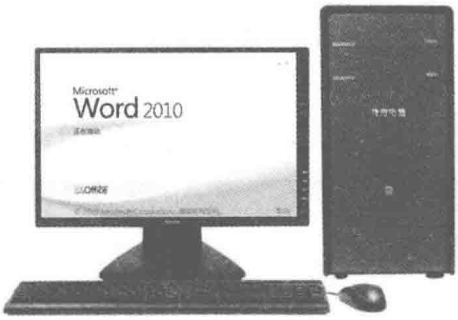


图 1.1.2　Word 文件加解密实验环境

【实验内容】

（1）Microsoft Word 文档加密保护。

（2）Microsoft Word 文档编辑保护。

（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 2010 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. docx”,如图 1.1.3 所示。

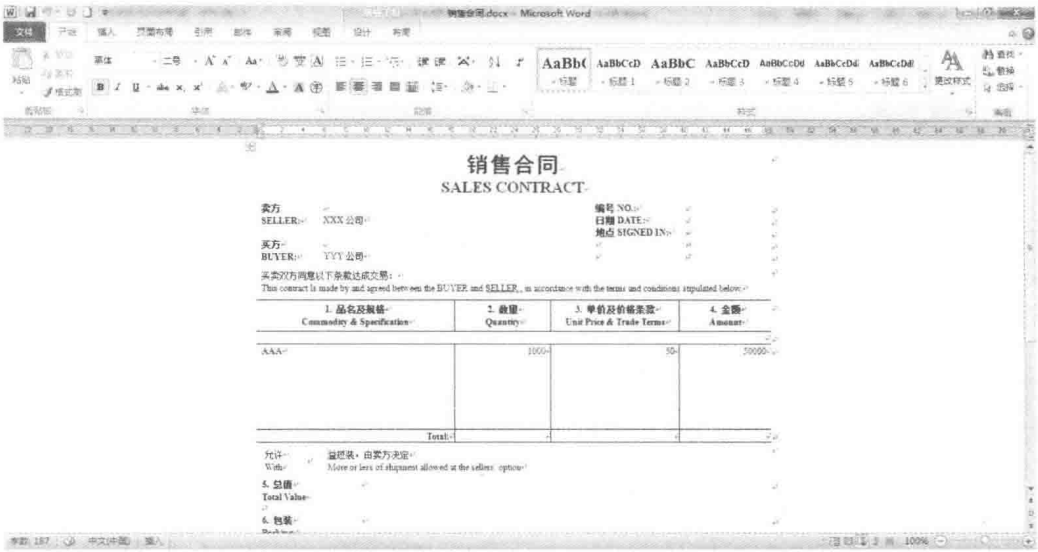


图 1.1.3 保密文档

(3) Word 选项设置

在 Word 操作界面的“文件”菜单上,单击“信息”子菜单,如图 1.1.4 所示。

图 1.1.4 Word 文档信息子菜单

(4) Word 安全性设置

在 Word 文档“信息”子菜单中，单击“文档保护”按钮，弹出文档保护类型列表，如图 1.1.5所示。

图 1.1.5　文档保护类型列表

(5) 选择文档包含类型

在“文档保护类型”列表中，单击“用密码进行加密”保护类型，弹出如图 1.1.6 所示的对话框。

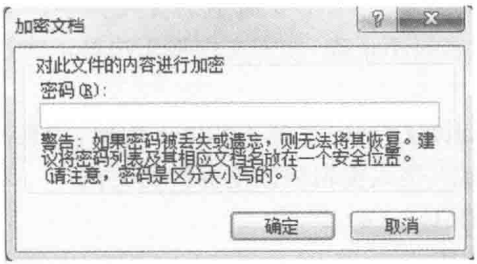


图 1.1.6　加密文档对话框

(6) 设置“打开文件”密码

在“加密文档”对话框中键入密码 desedfj，如图 1.1.7 所示，然后单击“确定”按钮。

在弹出的“确认密码”对话框中再次键入该密码，如图 1.1.8 所示，然后单击“确定”按钮。

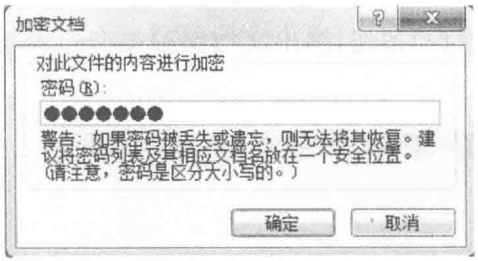


图 1.1.7 “加密文档”密码设置

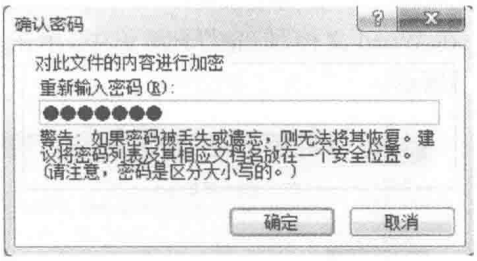


图 1.1.8 确认密码

保存加密文档，并退出。

(7) 验证

在 Windows 下用鼠标双击加密后的文档“销售合同. docx”，出现如图 1.1.9 所示的对话框。

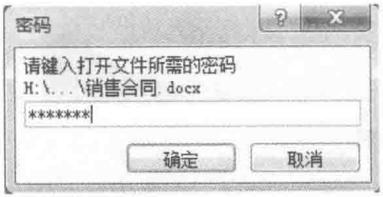


图 1.1.9 密码验证对话框

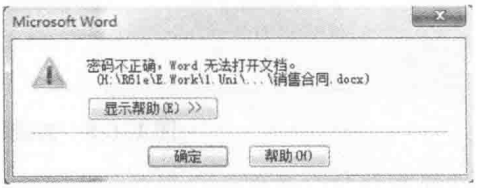


图 1.1.10 密码不正确，Word 无法打开文档提示框

在图 1.1.9 所示的密码验证对话框中输入打开该文档所需的正确密码 desedfj，然后点击“确定”按钮。这时就可打开如图 1.1.3 所示的文档内容。如果密码不正确，则出现图 1.1.10所示的提示框，提示密码不正确，加密文档将无法被正确打开。

2. Word 文档修改保护

如果需要允许其他人阅读文档，但是禁止其他人编辑，或篡改文档内容，可以通过设置“修改文件时的密码”来限制其他人编辑修改受保护的文档。

(1) 重复实验内容 1 的(1)～(4)步

(2) 设置“限制编辑”密码

在图 1.1.5 的“文档保护类型”列表中，单击“限制编辑”保护类型，弹出如图 1.1.11 所示的对话框。

在图 1.1.11 中选择“限制对选定的式样格式设置”和“仅允许在文档中进行此类型的编辑”复选项，然后点击“是，启动强制保护”按钮。在弹出的“启动强制保护”对话框中，选择密码单选项，并输入密码“erbvty”，如图 1.1.12 所示，然后单击“确定”按钮。

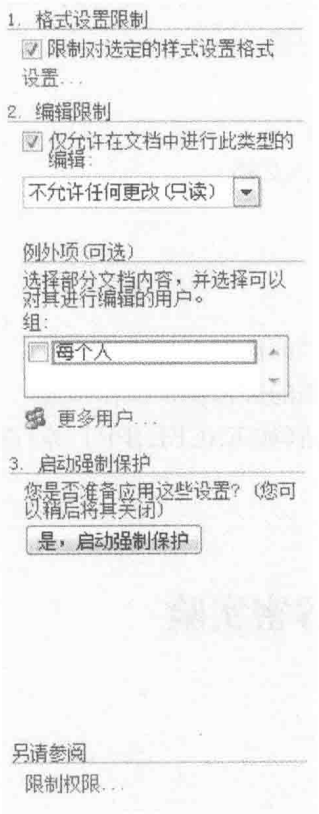


图 1.1.11　“限制编辑”设置

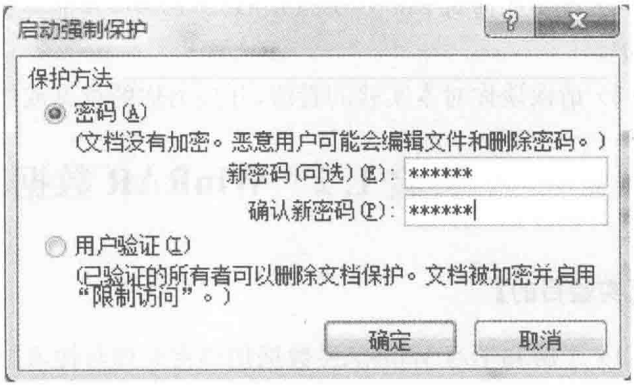


图 1.1.12　密码设置对话框

(3) 验证

在 Windows 下用鼠标双击加密后的文档，例如“销售合同. docx”，出现如图 1.1.3 所示的文档内容，该文档可以浏览，但是不能被编辑修改。如果需要进行文档编辑，在“限制格式和编辑”对话框中点击“停止保护”按钮，出现如图 1.1.13 所示的对话框。

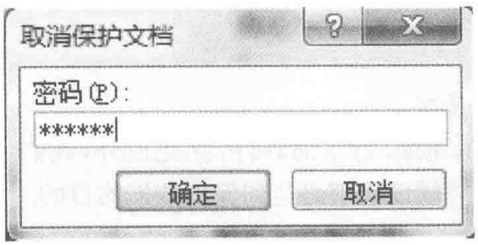


图 1.1.13　取消保护文档对话框

在图 1.1.13 所示的取消文档保护对话框中输入编辑该文档所需的正确密码“erbvty”，然后点击“确定”按钮，这时就可编辑如图 1.1.3 所示的文档内容。

3. 加密 Microsoft Office 其他类型文档

(1) 参考本节实验内容 1 和 2 加密 Microsoft Excel 文档

(2) 参考本节实验内容 1 和 2 加密 Microsoft PowerPoint 文档

【实验报告】

(1) 请回答实验目的中的思考题。

(2) 说明在 Microsoft Word 2010 中对文件进行打开文档的加密保护操作步骤。

(3) 说明在 Microsoft Word 2010 中对文件进行修改文档的加密保护操作步骤。

(4) 说明如何对 Microsoft Office 2010 中，其他类型文档(如 EXCEL、PPT 等)进行加密保护。

(5) 请谈谈你对本实验的看法，并提出你的意见或建议。

实验 1.2 WinRAR 数据加解密实验

【实验目的】

(1) 了解和学习 WinRAR 数据加解密原理与技术。

(2) 学习和掌握 WinRAR 数据加解密方法。

(3) 思考：

① WinRAR 能为其文档提供哪些安全服务？

② WinRAR 采用哪种加密算法？

【实验原理】

1. 数据保密原理与技术

参见实验 1.1。

2. WinRAR 加密安全保护

WinRAR 是一种常用的压缩/解压缩软件，除此以外，我们还常常把 WinRAR 当作加密工具使用，在压缩文件的时候设置密码达到保护数据的目的。

(1) WinRAR 简介

WinRAR 是由 Eugene Roshal 开发的一款功能强大的压缩包管理器。该软件可用于备份数据，缩减数据大小。由于其压缩效率高、速度快、安全可靠，无论是数据资料的交流与

试读结束，需要全本PDF请购买 www.ertongbook.com