教育部师资实践基地系列教材——信息与网络安全

神州数码网络安全岗位&认证系列

网络安全管理员

WANGLUO ANQUAN GUANLIYUAN

程庆梅　徐雪鹏　主编

全国职业技能大赛推荐参考书

神州数码网络安全岗位&认证系列教材

校企合作新课改教材

机械工业出版社
CHINA MACHINE PRESS

教育部师资实践基地系列教材——信息与网络安全

神州数码网络安全岗位&认证系列

网络安全管理员

主　编　程庆梅　徐雪鹏

副主编　杜婉琛

参　编　李东方　王　岳　王　博

郭　薇　田　弦

机械工业出版社

本书内容包括：企业网络信息安全与安全维护、网络终端的安全隐患、网络设备安全管理、终端信任计划、私有数据公网传递安全，共 5 章，40 个实训任务。内容涉及现代网络安全管理员在实际工作中遇到的各种典型问题及其主流解决方案和实施步骤。

本书是神州数码技能教学项目的配套指导教材，也是信息安全实践基地的指定训练教材。本书还适用于各类职业院校相关专业课程师生；各中小企业网络管理员等。

本书配有电子课件以方便教师教学，可到机械工业出版社教材服务网 www.cmpedu.com 以教师身份免费注册下载或联系编辑（010-88379194）咨询。

图书在版编目（CIP）数据

网络安全管理员/程庆梅，徐雪鹏主编. —北京：机械工业出版社，2012.9
教育部师资实践基地系列教材. 信息与网络安全
ISBN 978-7-111-39112-8

Ⅰ. ①网… Ⅱ. ①程… ②徐… 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 152727 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
策划编辑：梁 伟 责任编辑：梁 伟
封面设计：鞠 杨 责任印制：杨 曦
北京四季青印刷厂印刷
2012 年 8 月第 1 版第 1 次印刷
184mm×260mm · 7.75 印张 · 189 千字
标准书号：ISBN 978-7-111-39112-8
定价：20.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务
社服务中心：（010）88361066
销 售 一 部：（010）68326294
销 售 二 部：（010）88379649
读者购书热线：（010）88379203

网络服务
门户网：http://www.cmpbook.com
教材网：http://www.cmpedu.com
封面无防伪标均为盗版

前　言

1．读者对象

本书适合高等职业院校作为网络信息安全教材及课外辅导读物，也适合计算机网络与信息安全技术爱好者阅读。书中文字浅显易懂，也适合作为信息安全入门读物。

2．职业目标

网络安全管理员；网络安全工程师；网络安全测试人员。

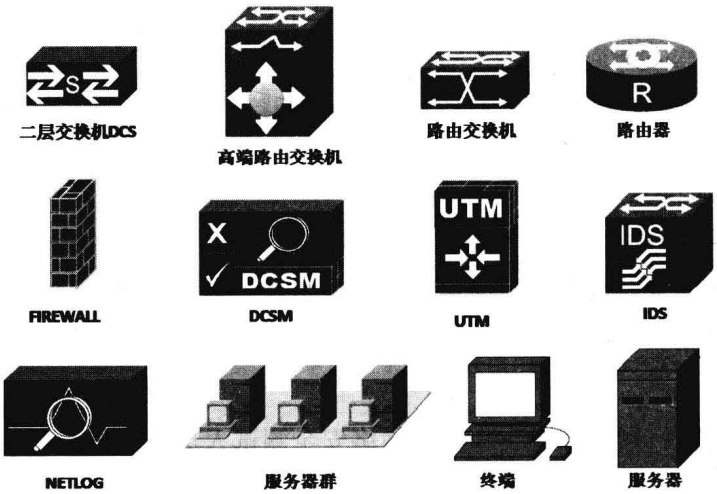
3．本书特点

本书包括5章，分别从不同的角度对企业和园区网的全局和局部进行阐述，并设计了相应的实训，内容涵盖了信息安全和网络安全管理的各个要素。与以往的安全管理员实训类教材不同之处在于：内容更加系统化；设备和终端安全并重；理论与实践相结合；更贴近岗位实际。

4．教学建议

序　号	章	节	理论课时	实训课时
第1章	企业网络信息安全与安全维护	信息安全现状	1	0
		信息安全隐患及安全策略		
		信息安全与园区网安全维护	1	
		加密与身份认证技术概述	3	
		信息安全策略与法律法规	1	
第2章	网络终端的安全隐患	系统漏洞	2	4
		MySQL数据库漏洞利用	1	2
		木马与病毒	1	2
		拒绝服务攻击	1	2
第3章	网络设备安全管理	认识网络设备	4	8
		安全维护交换机	1	2
		安全维护路由器	1	2
		安全维护防火墙	1	2
第4章	终端信任计划	有线网络终端的接入安全保障	3	4
		无线网络终端的接入安全保障	3	6
第5章	私有数据公网传递安全	点到网的数据安全保障	4	4
		网到网的数据安全保障	2	2
总　计			30	40

5．本书所用的图标



6．编写队伍

本书由神州数码网络公司企业网职教行业部总经理程庆梅、神州数码网络大学总经理徐雪鹏任主编，神州数码网络大学教学专业经理杜婉琛任副主编。参与编写的人员还有神州数码网络大学的全体讲师，其中李东方负责第 1 章和第 2 章的编写，王岳负责第 3 章和第 5 章的编写，王博负责第 4 章的编写以及整体技术审校工作，郭薇和田弦负责本书的文字校对和整体市场调研工作。

本书的编写得到了神州数码技术团队的大力支持，同时在审核校对的过程中得到了杭州职业技术学院、北京信息职业技术学院等多所院校师生的大力协助，在此表示由衷的感谢。

本书的编写虽经多方合作，但由于编者水平有限，疏漏之处在所难免，敬请广大读者批评指正，编者邮箱：dcnu_2007@163.com。

编　者

2012 年 4 月

目　录

第1章 企业网络信息安全与安全维护

学习目标

- 了解当前企业网络信息安全的发展现状。
- 了解常见的网络攻击手段以及安全威胁，熟悉基础网络安全防护方法。
- 理解数据加密和身份认证对于数据安全的重要意义。
- 了解我国计算机信息安全相关法律法规。

重点及难点

- 不同网络攻击方法的原理和区别。
- 针对不同的网络攻击的防护方法。
- 对称加密和非对称加密的区别以及密钥对的使用规则。

1.1 信息安全现状

1. 国际信息安全现状

信息化程度比较高的发达国家非常重视国家信息安全的管理工作。美、俄、日等国家都已经或正在制订本国的信息安全发展战略和发展计划，以确保信息安全沿着正确的方向发展。美国国土安全局是美国信息安全管理的最高权力机构，美国国家安全局、美国联邦调查局、美国国防部等机构分担信息安全管理和执行，他们主要是根据相应的方针和政策结合本部门的情况实施信息安全保障工作。2000年初，美国出台了《电脑空间安全计划》，旨在加强关键基础设施和计算机系统网络免受威胁的防御能力。2000年7月，日本信息技术战略本部及信息安全会议拟定了信息安全指导方针。2000年9月，俄罗斯批准了《国家信息安全构想》，明确了保护信息安全的措施。

美、俄、日三个国家均以法律的形式规范信息安全工作，对有效实施安全措施提供了有力保证。2000年10月，美国的电子签名法案正式生效。2000年10月，日、美参议院通

过了《互联网网络完备性及关键设备保护法案》。2000 年 6 月，日本公布了旨在对付黑客的《信息网络安全可靠性基准》的补充修正方案。2000 年 9 月，俄罗斯实施了关于网络信息安全的法律。

国际信息安全管理已步入标准化与系统化管理时代。在 20 世纪 90 年代之前，信息安全主要依靠安全技术手段与不成体系的管理规章来实现。在 20 世纪 80 年代，随着 ISO9000 质量管理体系标准的出现及在全世界的推广应用，系统管理的思想被借鉴与采用，信息安全管理在 20 世纪 90 年代也步入了标准化与系统化管理的时代。1995 年，英国率先推出了 BS7799《信息安全管理标准》，该标准已经于 2000 年被国际标准化组织认定为国际标准 ISO/IEC17799。现在该标准已经引起许多国家与地区的重视，并且在一些国家已经被推广应用。组织贯彻实施该标准可以对信息安全风险进行安全系统地管理，从而实现组织信息安全。另外，其他国家及组织也提出了很多与信息安全管理相关的标准。

2．国内信息安全现状

我国已经初步建立了国家信息安全组织保障体系。国务院信息办专门成立了网络与信息安全领导小组，各省、市、自治州也设立了相应的管理机构。2003 年 7 月，国务院信息化领导小组通过了《关于加强信息安全保障工作的意见》。同年 9 月，中央办公厅、国务院办公厅转发了《国家信息化领导小组<关于加强信息安全保障工作的意见>》，把信息安全提到了促进经济发展、维护社会稳定、保障国家安全、加强精神文明建设的高度，并提出了“积极防御，综合防范”的信息安全管理方针。2003 年 7 月，我国成立了国家计算机网络应急技术处理协调中心，专门负责收集、汇总、核实、发布权威性的应急处理信息。2001 年 5 月，我国成立了中国信息安全产品测评认证中心和开展信息安全测评认证工作的职能机构，建立了依据国家产品质量认证和信息安全管理相关法律法规进行管理和运行的国家信息安全测评认证体系。

我国制定和发布了一系列信息安全管理国家标准和规范，包括：GB 17895-1999《计算机信息系统安全保护等级划分准则》、《信息系统安全等级保护基本要求》、GB/T 20269-2006《信息安全技术信息系统安全管理要求》、GB/T 20282-2006《信息安全技术信息系统安全工程管理要求》、《信息系统安全等级保护基本要求》等。另外，还引入了国际上著名的 ISO17799:2000《信息安全管理实施准则》和 BS7799-2:2000《信息安全管理体系实施规范》等信息安全管理标准。

我国还制定了一系列信息安全管理相关的法律法规。从 20 世纪 90 年代初起，为了满足信息安全管理的需要，国家有关部门和地方政府制定了《中华人民共和国计算机信息网络国际联网管理暂行规定》、《商用密码管理条例》、《互联网信息服务管理办法》、《计算机信息网络国际联网安全保护管理办法》、《电子签名法》等有关信息安全管理的法律法规。

在我国信息安全风险评估工作也很早就已经开展，并且已经成为信息安全管理工作的主要内容。由国家信息中心组织的对北京、广州、深圳和上海四个城市十几个行业的 50 多家单位深入细致的调查与研究，最终形成了《信息安全风险评估调查报告》、《信息安全风险评估研究报告》和《关于加强信息安全风险评估工作的建议》，依据这些成果制定了 GB/T 20984-2007《信息安全技术信息安全风险评估规范》。

目前我国的信息安全管理工作仍然存在许多问题：

1）信息安全管理比较混乱，缺乏国家层面上的整体策略，在实际工作中管理力度、政策执行和监督力度不够。

2）动态的和涵盖组织机构、文件、控制措施、操作过程和程序及相关资源等要素的信息安全管理体系还未建立起来。

3）信息安全风险评估标准体系不够完善，信息安全的需求难以确定，缺乏系统的信息安全风险评估和评价体系以及完善的信息安全保障体系。

4）缺乏信息安全意识，普遍存在“重产品、轻服务，重技术、轻管理”的思想。

5）专项经费投入不足，管理人才极度缺乏，基础理论研究和关键技术薄弱，严重依赖国外相关技术。

6）技术创新不足，信息安全管理产品质量不高。

7）缺乏权威、统一、专门的管理机构，现有的一些有关信息安全管理的法律法规层次不高，执法主体不明确，多头管理，规则冲突，缺乏可操作性，执行难度较大，有法难依。

1.2　信息安全隐患及安全策略

在信息时代，互联网已成为人们日常生活中不可缺少的一部分，但伴随而来的黑客、木马等网络安全隐患也成为用户的心头大患。

中国信息产业经历了 20 多年的发展历程，如今已经成为国民经济的基础性、支柱性、先导性和战略性产业。但是随着信息技术的发展，信息安全隐患也日渐暴露。黑客猖獗、木马肆虐、网站被黑、信息被盗等案例时常见诸报端。

虽然立法和监管是不可或缺的一环，但网络违法犯罪行为具有传播速度快、范围广、互动性强、隐蔽性高等特点。因此，改进相关防范技术以加强信息安全至关重要。

随着信息技术和信息产业的发展，以 Internet 为代表的全球性信息化浪潮使得信息网络技术的应用日益普及，应用层次逐渐深入，应用领域从传统的、小型业务系统逐渐向大型、关键业务系统扩展，如党政部门信息系统、金融业务系统、企业商务系统等。越来越多的企业建立了自己的企业网络，并与 Internet 相连。在网络中传输了许多重要的信息，如政府宏观调控决策、商业经济信息、银行资金转账、股票证券、能源资源数据、科研数据等。其中有的是敏感性信息，有的甚至是国家机密。所以不可避免会受到各种主动或被动的攻击，如信息泄露、信息窃取、数据篡改、数据增删、计算机病毒等。近年来，垃圾邮件日益增多、企业网页不时遭到黑客篡改、计算机病毒泛滥成灾，网络信息系统中的各种犯罪活动已经严重危害了企业的安全和社会的发展，给企业造成了巨大的损失。计算机网络犯罪案件数量急剧增加，已经成为国际性的普遍问题。形形色色的安全问题不仅给企业带来了巨额的经济损失，也严重阻碍了我国的信息化进程。根据国家计算机病毒应急处理中心的调查显示，2003 年中国计算机病毒感染率高达 85.57%。因此，在企业信息化过程中，加强企业信息安全建设采取相应的防范措施已经迫在眉睫。

当前，企业的信息安全隐患来自于两个方面，即外来攻击和内部泄密。

1．外来攻击

大部分外来攻击可分为 3 类：闯入、拒绝服务和信息窃取。

（1）闯入

最常见的攻击方法就是闯入，攻击者闯入计算机内，就像合法用户一样使用被攻击者的电脑。闯入的手段比较多，常见的是利用社会工程学攻击，如攻击者打个电话给 ISP 谎称是某个用户，为了做某些工作要求立即改变密码。一种最简单的方式是猜测用户的密码，在有些情况下这是比较容易的，有许多用户并不太重视自己的密码或认为麻烦担心忘记密码而将密码设置得容易被猜测到。另外一种方法是搜索整个系统，发现软件、硬件的漏洞（Bug）或配置错误，以获得系统的进入权。

（2）拒绝服务

拒绝服务（Denial of Services）是一种将被攻击机器的功能或服务远程摧毁或中断的攻击方式，其攻击的手段也是多种多样的。最早出现的是“邮包炸弹”，攻击者用一个程序不断地向被攻击者的邮箱发出大量邮件并匿藏自己的地址信息，致使被攻击者几乎无法处理邮件，甚至导致邮件服务器因为大量的服务进程而崩溃，而被攻击者也无法确认攻击者的身份。还有一些攻击手段是利用软件漏洞进行远程攻击，其中比较著名的是对微软的 OOB（Out Of Bond）漏洞的攻击，攻击者向运行 Windows 95 或 Windows NT 的 139 端口发送一个非法数据包，导致操作系统被迫中断网络连接，甚至死机或重启。

（3）信息窃取

有一些攻击手段允许攻击者即使不操作被攻击的电脑也能窃取到想要的数据。比较典型的是用网络嗅探器（Sniffer）监听网络中的数据包信息，从中发现有用的信息，如用户名、密码、交易信息等。Sniffer 的工作有点类似于现实社会里装电话窃听装置。在共享式网络环境里 Sniffer 是很可怕的，它可以监听大量的网络信息。

2．内部泄密

随着各行各业信息化建设的推进，内部泄密已经成为威胁企业信息安全的最大隐患。FBI 和 CSI 对 484 家公司的信息安全情况做了调查，结果发现：有超过 85%的公司遭受过来自企业内部的安全威胁；有 16%的公司遭受过来自内部未授权的访问；有 14%的公司遭受过专利信息被窃取；有 12%的公司遭受过内部人员的财务欺骗；有 11%的公司遭受过资料或网络的破坏；其中，大陆地区的公司中有 80%的网站存在安全隐患，20%的网站存在严重安全问题。

从上述数据中可以看出，面对来自于公司内部的安全威胁，必要的安全措施对企业是何等重要，而这又恰恰是最容易被企业忽视的“盲区”。随着移动存储设备小型化和电子邮件等技术的发展，许多企业、事务所、学校、金融机构、高科技研究所等单位的重要资料很容易流失到网络外部。在信息就是生产力的竞争环境中，这些威胁给单位造成无法估计的损失。

从另一种角度，安全隐患则存在于如下几个方面：

1）现有网络系统具有内在安全的脆弱性。

2）对网络的管理思想麻痹，没有重视黑客攻击所造成的严重后果，没有投入必要的人力、财力、物力来加强网络安全性。

3）没有采取正确的安全策略和安全机制。

4）缺乏先进的网络安全技术、工具、手段和产品。

5）缺乏先进的系统备份、恢复技术和工具。

网络攻击的方式：

1）通过发动“拒绝服务”（DoS）攻击破坏公司的网络，使网络的合法用户无法正常接入网络。

2）侵入使用宽带互联网连接的“永远在线”远程工作台位（例如，通过“后门”入侵），暴露公司的 IP，使其受到进一步攻击。

3）在网络上插入一个未经授权的设备，并将其伪装成网络上的一个合法设备。

4）在公共 Web 服务器和电子商务服务器上发动入侵攻击。

5）精心策划并发动病毒攻击，破坏数据和应用。

数据攻击是攻击在网络上传输的数据（专用 IP、客户记录、员工信息等）、存储在数据服务器上的数据以及在网络上进行存取的各种应用（电子邮件、Web、ERP、CRM 等）。

数据攻击的方式包括：

1）蓄意破坏在网络上传输的信息或者无意中窃取以有线或者无线的方式在网络上传输的密码以及其他保密信息。

2）窃取硬件并访问内嵌在设备上的（如设备 MAC 地址等）或者存储在设备硬盘上的保密信息。

3）用户攻击是攻击访问网络的用户（终端用户和远程用户等）和用户设备（笔记本电脑和台式电脑等）。

用户攻击的例子包括：

1）盗窃合法网络用户的身份，获取对网络上的保密信息和受保护的资源的访问权。

2）在用户的设备上发动 DoS 攻击，导致其网络中断和过载，使用户无法正常使用。

针对以上问题，目前重要的安全防护工作主要包括：

1）明确安全防范工作的重点和对象。

2）防止外部的非法访问，防止黑客的入侵，保证整个企业内部网络的安全，保证企业网络通信的畅通。

3）公司内部可能有一些员工对公司有不满情绪，对企业的网络直接发起攻击。因为他们的计算机在企业防火墙的内部，对企业网络内部发起攻击会比外部的黑客入侵有更大的危险性，而且防火墙无法阻止这些攻击，因此内部网络的安全防范必须给予高度的重视。

4）企业内部一些重点部门（如财务部）存放有公司的一些重要资料，因此必须重点保护。

1.3　信息安全与园区网安全维护

常见的病毒防治方案有如下几种。

1. 安装防护工具软件

安装杀毒软件来防范用户的电脑被病毒入侵，建议例如病毒防火墙软件 McAfee，具有病毒库更新迅速、可查杀范围广等特点。

2．定期扫描电脑病毒

至少每星期进行一次电脑病毒扫描，建议设定扫描时间在非工作时间，例如假期或午休时间。

切记要选择“扫描所有固定磁盘”（以 McAfee 为例）。不要只选择性地扫描应用文件，因为很多流行的电脑病毒和蠕虫会依附在 eml、vbs 和 shs 等格式的文件中。

3．设置员工的使用权限

尽量避免其他人使用自己的电脑，因为他们有可能引入恶意软件或病毒，感染电脑。如果必须和他人共用你的电脑，必须设置第三者对文件夹或硬盘的存取权限。

避免使用共享文件夹（Shared Folder），必须使用时可以为共享文件夹设定访问者的用户名称和密码，以限制已被感染的电脑通过共享文件夹感染自己的电脑。

4．处理电子邮件的附件时要特别小心

不要随便打开来历不明的电子邮件附件。一些病毒或蠕虫会伪装为节日的祝贺或庆祝语、求职信等，除非了解这个文件的内容，否则请不要执行任何附件。

不要散播恶作剧电子邮件，恶作剧电子邮件通常散布虚假的信息，它们通常以连锁信形式散播病毒。

5．检查外来文件，方可使用

软盘、光盘或从 Internet 下载（尤其在不知名的网站下载）的外来文件，需先用防毒软件检查后才能打开或者使用。

6．及时安装补丁程序

常用的软件包括操作系统、浏览器和办公室应用程序需经常安装补丁程序。

留意最新的补丁程序的资讯，关心微软最新推出的补丁程序，启动“Windows Update”。

7．过滤一切传播病毒或蠕虫的渠道

电子邮件并非传播病毒或者蠕虫的唯一渠道，对于其他传播途径例如浏览网站或者文件传送（FTP）也要建立过滤机制阻截病毒或蠕虫。

8．为系统及资料备份还原做好准备

预先准备一套以上的还原光盘放置在安全的地方，这套备份光盘能帮助用户的电脑重新启动及清除在硬盘上的病毒（现在市面上大部分系统安装光盘都带有 DOS 杀毒工具）。此外，准备一套防毒软件的应急盘，可以在还原时做病毒清除。

将硬盘上的资料（重要数据）备份于另一个存储器中，例如光盘或者服务器，最好一个月更新一次最新的资料。切勿存放在同一个系统中，即使电脑系统被完全破坏也有办法恢复数据。

9．其他保护方法

确保服务器和个人电脑不会从软驱或光驱启动（BOOT UP），将 BIOS 或者 CMOS 的启动设置更改为从硬盘启动，这样可以有效地防范引导区类型的病毒。

安装防火墙（Firewall），利用防火墙来防范病毒入侵。在没有硬件防火墙的前提下，设定防火墙的对外访问通信的限制，一般防火墙只限制了进入信息。这样才能阻止木马程序建立对外通信而导致数据丢失。

10. 网络知识的培训

通过对员工进行基本的网络知识培训，让员工了解网络中常见的使用操作。

1.4　加密与身份认证技术概述

1.4.1　加密技术简介

密码学（Cryptography）一词来源于古希腊的 Crypto 和 Graphein，意思是密写。它是以认识密码变换的本质、研究密码保密与破译的基本规律为对象的学科。

经典密码学主要包括两个既对立又统一的分支：密码编码学和密码分析学。研究密码变化的规律并用之于编制密码以保护秘密信息的科学，称为密码编码学。研究密码变化的规律并用之于密文以获取信息情报的科学，称为密码分析学，也叫密码破译学。前者是实现对信息保密的，后者是实现对信息反保密的。密码编码学与密码分析学相辅相成，共处于密码学的统一体中。

现代密码学除了包括密码编码学和密码破译学两个主要学科外，还包括近几年才形成的新分支——密码密钥学，它是以密码的核心部分——密钥作为研究对象的学科。密钥管理是一种规程，它包括密钥的产生、分配、存储、保护、销毁等环节，在保密系统中至关重要。上述三个分支学科构成现代密码学的主要学科体系。

密码技术是保护信息安全的主要手段之一。密码技术自古有之，到目前为止，已经从外交和军事领域走向公开。它是一门结合数学、计算机科学、电子与通信等诸多学科于一身的交叉学科，不仅具有保证信息机密性的信息加密功能，而且具有数字签名、身份验证、秘密分存、系统安全等功能。所以，使用密码技术不仅可以保证信息的机密性，而且可以保证信息的完整性和确定性，防止信息被篡改、伪造和假冒。

在信息时代，信息安全问题越来越重要。我们经常需要一种措施来保护我们的数据，防止被一些怀有不良用心的人看到或者破坏。因此，在客观上就需要一种强有力的安全措施来保护机密数据不被窃取或篡改。解决这个问题的方式就是数据加密。一个加密网络，不但可以防止非授权用户的搭线窃听和入网，而且也是对付恶意软件的有效方法之一。

有些时候用户可能需要对一些机密文件进行加密，不一定因为要在网络上传输该文件，而是担心有人窃取计算机密码而获得该机密文件。身份认证是基于加密技术的，用来确定用户是否是真实的。在传输过程中对数据进行加密，可以保障数据在传输过程中安全。网络安全所要求的保密性、完整性、可用性都可以利用密码技术来实现。可以说，密码技术是保护大型通信网络上传输信息的实用手段之一。

随着我国社会经济活动信息化的飞速发展，信息的安全问题日益突出。采用密码技术对信息进行加密保护和安全认证是保护信息安全的有效手段。商用密码技术属于国家秘密，国家对商用密码产品的科研、生产、销售和使用实行专控管理。国家规定“不得使用自行研制的或者境外生产的密码产品”。

密码技术是网络与信息安全的核心技术，其基本的设计思想是把欲发送消息（明文）进行各种变换（称为加密算法）后的载体形式（称为密文）进行存储和传输，授权的接收

者用相应的变换（称为解密算法）恢复明文，不合法的截收者对明文不可见或不理解，从而达到信息安全的目的。

现代密码技术发展至今 20 余年，出现了许多高强度的密码算法和密钥管理技术。数据安全技术也已由传统的只注重保密性转移到了保密性、真实性、完整性和可控性的完美结合，并且相继发展了身份认证、消息确认和数字签名技术。

所谓加密（Encryption）是指将一个信息（或称明文——Plaintext）经过加密钥匙（Encryption Key）及加密函数转换变成无意义的密文（Ciphertext），而接收方则将此密文经过解密函数、解密钥匙（Decrypt on Key）还原成明文。这一概念是密码学的基础。

数据加密技术要求只有在指定的用户或网络下才能解除密码而获得原来的数据，这就需要给数据发送方和接收方一些特殊的信息用于加、解密，这就是所谓的密钥。需要保护的原始信息称为明文，用密钥编码操作后得到的看上去没有意义的结果称为密文。

加密的优点是即使其他的控制机制（如密码、文件权限等）受到了攻击，入侵者窃取的数据仍是无用的。

密码技术的基本任务是使通常称为 Alice 和 Bob 的两个人在不安全的信道上进行通信，而他们的敌人 Oscar 不能理解他们正在通信的内容。

Alice 打算发送给 Bob 的消息，我们称为明文。明文的形式可以是任意的，在计算机领域里通常是二进制数据。Alice 用预先确定的密钥处理（加密）明文，得到密文，通过信道发送给 Bob。在信道上通过截听而能看到密文的 Oscar 由于不知道解密密钥，所以不能确定明文是什么，而知道解密密钥的 Bob 却能解密密文得到明文。

信息加密过程是由形形色色的加密算法具体实施的，密码设计的基本公理和前提是算法公开，系统的安全性仅依赖于密钥的保密性。按照密钥使用方式不同来区分，可以将这些加密算法分为对称密钥密码算法（又称私有密钥算法）和非对称密钥密码算法（又称公钥密码算法）。两种密码体制各有优缺点，适用于不同的加密需求和应用场合。

对于加密文件，一个常被讨论但又经常被误解的内容是加密强度。什么构成了加密的强度，哪种级别的加密强度是被不同的安全需要所要求的，如何确定加密的有效强度？

加密强度主要取决于 3 个因素：

1）算法的强度。除了尝试所有可能的密钥组合之外，任何数学方法都不能使信息被解密；应该使用工业标准的算法，因为它们已经被加密学专家测试过无数次；任何一个新的或个体的方法在被商业认证之前都不被信任。

2）密钥的保密性。数据的保密程度直接与密钥的保密程度相关，算法不需要保密，被加密的数据首先与密钥共同使用，然后通过加密算法加密。

3）密钥强度。根据加密和解密的应用程序，密钥的长度是由 bit 为单位。在密钥的长度加上一位则相当于把可能的密钥的总数乘以 2，简单地说构成一个任意给定长度的密钥的位的可能的密钥个数可以被表示为 2^n，因此一个 40 位密钥长度的算法将是 2^{40} 个可能的不同的密钥。

加密技术的基础为移位和置换。

移位和置换是密码技术中两种主要的编码方法，是组成最简单的密码的基础。移位很像一种字母游戏，打乱字母的排列顺序。在移位密码中，数据本身并没有改变，只是被安排成了不同的格式。置换则是不管原来的内容如何，始终按照一定的规则改变内容的排列顺序。移位

和置换都是可逆的操作，只要知道移位和置换的规则，就很容易把原来的信息恢复出来。

在香农（Shanon）的信息论理论中，认为加密就是要使数据变得杂乱无章，应该使用移位、置换等手段进行这类操作。现在绝大多数密码采纳了这种观点，因此移位和置换在各种密码算法中很常见，作为算法的某一部分发挥着打乱信息的作用。

1．对称密钥加密

对称密钥加密又称传统密码加密，私钥算法加密。它要求加密解密双方拥有相同的密钥，一方使用该密钥加密，而另一方使用该密钥解密。著名的密码算法有 DES（数据加密标准）、IDEA 等。

在此密码算法中收信方和发信方使用相同的密钥，即加密密钥和解密密钥是相同或等价的。当需要给对方发信息时，用自己的加密密钥进行加密，而在接收方收到数据后，用对方所给的密钥进行解密。这种方式在与多方通信时因为需要保存很多密钥而变得很复杂，而且密钥本身的安全就是一个问题，密钥必须通过安全的途径传送。因此，密钥管理成为系统安全的重要因素。

有许多特殊的数学算法来实现对称加密。这些算法包括数据加密标准 DES、Triple DES、IDEA、Blowfish 和 Twofish。

DES 是一种数据分组的加密算法，DES 加密算法是当今世界使用最为广泛的密码算法，它是由 IBM 公司在 20 世纪 70 年代开发的，并于 1976 年 11 月被美国国家标准局采纳为美国国家标准。DES 将数据分成长度为 64 位的数据块，使用相同的密钥来加密和解密。每 64 位又被分成两半，并利用密钥对每一半进行运算，DES 有 16 轮运算，对于每一轮的运算所使用密钥的位数是不同的。DES 的优点是快速并易于实施，但密钥的传播和管理非常困难。

三重 DES 在 DES 的基础上使用了有效的 128 位长度的密钥，信息首先被使用 56 位的密钥加密，然后用另一个 56 位的密钥译码，最后再用原始的 56 位密钥加密。Triple DES 最大的优点是可以使用已存在的软件和硬件。

IDEA（International Data Encryption Algorithm，国际数据加密算法）是 Xuejia Lai（来学嘉）和 James L. Massey 在瑞士联邦工程学院开发出来的，在 1990 年被公布并在 1991 年得到增强。IDEA 使用 128 位（16 字节）密钥进行操作。

Blowfish 是由 Bruce Schneier 开发的一种非常灵活的对称算法，在个人的加密领域里非常有效。它每轮使用不同的密文，密钥长度最大可支持到 448 位。Schneier 现在已创建了一种较新的算法 Twofish，这种算法使用 128 位的数据块，速度较快。它支持 28 位、192 位和 256 位的密钥。

对称密钥加密技术具有加解密速度快、安全强度高等优点，在军事、外交以及商业应用中的使用越来越普遍。但由于这种密码体制的密钥在分配管理和使用上有诸多局限，在大量的个人通信安全需求面前，仍然需要其他密码体制的补充。

对称密钥加密技术的一大缺点是随着网络规模的扩大，密钥的管理成为一个难点，因此密码体制的安全性从某种意义上来讲依赖于密钥的安全性。

针对对称密钥加密技术的缺点，提出了非对称密钥加密算法。

2．非对称密钥加密

加密解密双方拥有不同的密钥，在不知道特定信息的情况下，加密密钥和解密密钥在