高等学校计算机网络工程专业规划教材

网络信息安全

徐明 刘端阳 张海平 丁宏 编著

西安电子科技大学出版社
http://www.xduph.com

高等学校计算机网络工程专业规划教材

网络信息安全

徐　明　刘端阳
张海平　丁　宏　编著

西安电子科技大学出版社

2006

内 容 简 介

本书围绕网络信息安全中的基本问题，比较全面地介绍了网络信息安全的基础理论和应用实践知识。本书的内容包括：网络信息安全概论，密码技术，PKI，安全技术应用，防火墙技术，病毒原理，网络黑客攻击技术，入侵检测技术，计算机取证技术以及信息隐藏等技术。

本书可作为高等学校网络工程、计算机、信息安全专业本科生、研究生的教材，也可作为相关领域专业科研人员的参考书。

图书在版编目（CIP）数据

网络信息安全 / 徐明等编著. —西安：西安电子科技大学出版社，2006.5

ISBN 7-5606-1660-7

Ⅰ. 网… Ⅱ. 徐… Ⅲ. 计算机网络—安全技术 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2006）第 025300 号

策　　划　臧延新　云立实

责任编辑　杨宗周

出版发行　西安电子科技大学出版社(西安市太白南路 2 号)

电　　话　(029)88242885　88201467　　邮　　编　710071

http: //www.xduph.com　　E-mail: xdupfxb@pub.xaonline.com

经　　销　新华书店

印刷单位　陕西光大印务有限责任公司

版　　次　2006 年 5 月第 1 版　2006 年 5 月第 1 次印刷

开　　本　787 毫米×1092 毫米　1/16　印张　9

字　　数　199 千字

印　　数　1～4000 册

定　　价　11.00 元

ISBN 7 - 5606 - 1660 - 7/TP • 0402

XDUP 1952001-1

*****如有印装问题可调换*****

本社图书封面为激光防伪覆膜，谨防盗版。

出 版 说 明

计算机技术和通信技术的结合形成的全球互联网络已经把人类社会带入了以互联网为中心的信息化时代。目前网络技术日新月异，网络已成为承载信息经济运转的高效平台，但是我国的网络工程专业人才还很缺乏，与 IT 产业的飞速发展很不适应，不能满足社会各行各业对网络专业人才的需求。因此，培养具有计算机技术和网络技术方面的理论基础，具备系统工程经验和综合能力，能够从事网络规划、网络工程设计、网络维护和管理、网络安全防护等工作的专业技术人才成为当务之急。许多高校看到了这一趋势，纷纷开设了网络工程专业，但是缺乏能够满足当前教学要求的系列教材。为此，西安电子科技大学出版社聘请了西安交通大学、华南理工大学、西安电子科技大学、西安理工大学、山东科技大学、空军工程大学、杭州电子科技大学、西安邮电学院、成都信息工程学院等九所高校长期在教学科研第一线的专家教授，组成了高等院校计算机网络工程专业教材编审专家委员会，对网络工程专业的教学计划和课程大纲进行了反复研究、充分讨论，通过招标方式筛选并确定了系列书的主编院校及作者，争取在一年的时间里出版并推出整套教材。

由于网络工程专业是各高校新开办的专业，各高校的课程设置和教学要求不尽相同，因此这套教材尽可能系统地覆盖了网络工程专业的主要课程和相关知识，反映网络技术的最新进展和研究成果，在介绍基本理论和基本方法的基础上，特别突出工程实践的重要性和内容的新颖性，重点培养学生从事实际工程的研发能力。在写作风格上，本套教材力求逻辑严谨，语言明快，形式活泼，可读性强。本套教材的作者都是长期从事网络教学的骨干教师，他们较高的学术水平和丰富的教材编写经验是这套丛书顺利出版的保障，在此向他们表示衷心的感谢。

这套经过精心策划和组织的系列教材的出版，不仅是对网络工程专业教学改革的有益探索，而且也积极推动了该专业的教材建设，我们将听取来自各方面的建议，通过不断的改进，使这套教材能够得到各院校的认可并更趋完善。

系列教材编委会

2005 年 2 月

高等学校计算机网络工程专业
教材编审专家委员会

前　言

随着计算机和网络技术日新月异的发展，网络信息安全问题已成为信息数字时代人类共同面临的挑战。伴随着信息技术的发展与应用，信息安全的内涵也在不断地延伸，从最初的信息保密性发展到信息的完整性、可用性、可控性和不可否认性，进而又发展为“攻(攻击)、防(防范)、测(检测)、控(控制)、管(管理)、评(评估)”等多方面的基础理论和实施技术。网络信息安全是一个综合、交叉学科领域，涉及数学、物理、通信和计算机等诸多学科。目前，网络安全问题的具体表现为：计算机系统受病毒感染和破坏的情况相当严重；电脑黑客活动已形成重要威胁；信息基础设施面临网络安全的挑战；信息系统在预测、反应、防范和恢复能力方面存在许多薄弱环节；网络政治颠覆活动频繁等。

面对越来越严重的网络信息安全威胁，加速培养网络信息安全方面的人才是构建并完善我国网络信息安全保障体系的关键环节。网络信息安全方面的知识已经成为计算机、网络和通信等相关专业必备的基本知识。

本书共分 10 章。主要内容安排如下：第 1 章为网络信息安全概论；第 2、3、4 章分别为密码技术、公钥基础设施和密码技术应用；第 5 章为黑客入侵技术；第 6 章为病毒原理；第 7 章为防火墙技术；第 8 章是入侵检测技术；第 9 章介绍了信息隐藏与隐写分析技术；第 10 章介绍了计算机与网络取证技术。本书力求紧跟国内外网络信息安全技术的前沿领域，全面、通俗、系统地反映网络信息安全的理论和实践知识。

在本书的编写过程中，参考了国内外有关作者的大量文献资料，参考了互联网上的众多资料，在此表示衷心的感谢。本书的第 2、7 章由张海平编写；第 4、6 章由丁宏编写；第 3 章由刘端阳博士(浙江工业大学)编写；第 1、5、8、9、10 章的编写和全书的统稿由徐明完成。

本书的部分研究工作得到了浙江省自然科学基金(Y104426)和浙江省高校青年教师资助计划的资助。

由于网络信息安全技术发展快、涉及面广，加上笔者学识水平有限，书中难免存在不足之处，敬请广大读者批评指正。

编　者

2006 年 1 月

目　录

第 1 章　网络信息安全概论

1.1　网络信息安全问题的根源

现代计算机系统功能日渐复杂，网络体系日渐强大，对社会产生了巨大深远的影响，但同时由于计算机网络具有开放性、互联性、多样性、终端分布不均匀性等特征，致使网络易受黑客、恶意软件和其他不轨的攻击。对于军队、政府和金融系统而言，其网上信息的安全和保密尤为重要。因此，要提高计算机网络的防御能力，加强网络的安全措施非常迫切而且必要，否则该网络将是个无用的，甚至会危及国家安全的网络。由于网络和计算机系统本身具有的一些特性，使得网络信息安全问题面临着越来越多的威胁。影响计算机网络安全的因素很多，有些因素可能是有意的，也可能是无意的；可能是人为的，也可能是非人为的。归结起来，导致网络安全问题日益严重的根源主要有以下几个方面。

1．网络协议的开放性、共享性和协议自身的缺陷

覆盖全球的因特网，以其 TCP/IP 协议开放性与共享性方便了各种计算机网络的入网互联，极大地拓宽了资源共享的可能性。但由于早期网络协议以开放性和共享性为主要目标而对安全问题的忽视，以及 Internet 在使用和管理上的相对无序状态，导致目前网络安全受到了严重威胁，安全事故屡有发生。

网络协议自身的安全缺陷主要是指协议和业务的不安全。导致协议不安全的主要原因，一方面是 Internet 从建立开始就缺乏安全的总体构想和设计。因为 Internet 起源的初衷是方便学术交流和信息沟通，并非商业目的。Internet 所使用的 TCP/IP 协议是在假定的可信环境下，为网络互联而专门设计的，本身缺乏安全措施。TCP/IP 协议的 IP 层没有安全认证和保密机制(只基于 IP 地址进行数据包的寻址，无认证和保密机制)；在传输层，TCP 连接能被欺骗、截取和操纵，而 UDP 易受 IP 源路由和拒绝服务的攻击。另一方面，协议本身可能会泄露口令，连接可能成为被盗用的目标。

业务的不安全主要表现为：业务内部可能隐藏着一些错误的信息；有些业务本身尚未完善，难于区分出错原因；有些业务设置复杂，一般非专业人士很难对其完成完善的设置。

2．操作系统和应用程序的复杂性

由于网络和终端硬件设备的不断升级换代以及计算机功能的不断增强，现代操作系统和应用程序变得越来越庞大而复杂，导致的一个不良后果就是操作系统和应用程序本身存在许多安全漏洞和隐患。另外，操作系统和应用系统的复杂性也为对它们的配置不当而引发安全问题埋下了伏笔，甚至它们的默认安装和配置也成为安全的一大隐患。

3. 程序设计带来的问题

一方面由于商业和非商业的原因，程序员总是期望能在最短的时间内完成程序并实现尽可能多的功能，这就容易导致程序存在安全问题；另一方面，目前流行的开发程序的语言本身会带来安全问题(如C、C++中的边界问题)。

4. 设备物理安全问题

网络设备和计算机系统本身的物理安全隐患，如灰尘、潮湿、雷击和电磁泄露等，也是网络信息安全出现问题的重要根源之一。

5. 人员的安全意识与技术问题

人是信息活动的主体，是引起网络信息安全问题最主要的因素之一，这可以从以下三个方面来理解。第一，人为的无意失误主要是指用户安全配置不当造成的安全漏洞，包括用户安全意识不强、用户口令选择不当、用户将自己的账号信息与别人共享和用户在使用软件时未按要求进行正确的设置等。第二，人为的恶意黑客攻击，是网络信息安全面临的最大威胁。在英文中，黑客有两个概念：Hacker 和 Cracker。一般来说，Hacker 是这样一类人，他们对钱财和权利蔑视，而对网络技术本身非常专注，他们在网上进行探测性的行动，帮助人们找到网络的漏洞，可以说他们是这个领域的绅士。但是 Cracker 不一样，他们要么为了满足自己的私欲，要么受雇于一些商业机构，具有攻击性和破坏性。他们修改网页，窃取机密数据，甚至破坏整个网络系统。因其危害性较大，Cracker 已成为网络安全真正的，也是主要的防范对象。这类人闯入计算机网络系统盗取信息，故意破坏他人财产，使服务器中断。他们对电脑非常着迷，自认为比他人聪明，因此，随心所欲地闯入某些信息禁区，开玩笑或恶作剧，甚至干出违法的事。他们把此看作一种智力挑战，好玩，但当有利可图时，很多人往往抵制不住诱惑而走上犯罪的道路。信息战也是黑客开展攻击的一个非常重要的缘由。第三，管理不善也是一个重要因素之一。对网络信息系统的严格管理是避免受到攻击的重要措施。据统计，在美国，90%以上的 IT 企业对黑客攻击准备不足，75%～85%的网站都抵挡不住黑客的攻击。管理的缺陷也可能导致系统内部人员泄露机密，被一些不法分子获取可乘之机。

6. 相关的法律问题

由于网络环境是一种虚拟社会，现实社会和生活中的诸多问题在这个虚拟社会中都有所表现。现实社会中政府各行政主管部门多年来已经形成的管理职能必然向这个虚拟社会延伸。为了调整这个虚拟社会中的各种矛盾，规范秩序，制定相应的法规、规章和法律就成为了各部门的必然选择。但由于与网络相关的法律的不完善性、滞后性以及由于网络虚拟社会的无国界性和法律效力的国界性矛盾，也是导致目前网络信息安全问题的根源之一。实际上，网络环境下的信息安全不仅涉及到技术问题，而且涉及到法律政策问题和管理问题。技术问题虽然是最直接的保证信息安全的手段，但离开了法律政策和管理的基础，纵有最先进的技术，网络信息安全也得不到保障。

1.2 网络信息安全体系架构

信息是资源的抽象，用以表达资源，并可以被用来进行处理、存储和传输。例如，学生档案信息是对学生的抽象，它由专门人员进行登记，用电子数据文件对这些资源进行存储，并通过网络系统进行传输。

1. 网络信息系统中的资源

我们将网络信息系统中的资源分为三种：

(1) 人：信息系统的决策者、使用者和管理者。

(2) 应用：由一些业务逻辑组件及界面组件组成。

(3) 支撑：为开发应用组件而提供技术上支撑的资源，包括网络设施、操作系统软件等。

人类资源主要提供智力的服务以及体力的服务。虽然每个人都是由一些生理组织系统组成的，结构上差别不大，但他们所能提供的智力和体力服务却大不相同，这是由于他们各自的知识体系不同造成的。同时由于人类是高智能的系统，他们具有更为复杂的社会关系，这些都将是社会工程所要研究的内容。在目前以技术为主的网络信息系统中，将人按角色和权限进行划分，其实也暗中提出了对相应人类资源的知识和社会职责的要求。

所谓应用，是指面向业务的技术资源。这些技术组成一个处理与人类业务相关的信息。应用虽然也表现为软件或硬件组件，但我们通常更看中的是它能为人类解决什么样的问题。甚至可以说，应用是将一部分人类执行业务的逻辑或智能用技术的形式进行了实现，而随着人工智能技术的发展，这些技术中所体现的智能将越来越高，面向的业务范围也越来越广。计算机和网络技术最早是由一些科学家所使用的，那时的业务更像是一些技术领域的业务，后来将业务扩展到商务等实际应用领域。目前，我们的业务应用还处于相对初级的阶段，但它的扩展是未来发展的主要方向，并且将会更个性、更智能。

支撑类资源更多的是一些具体的技术，为应用类资源的实现提供服务。这类资源也有它们自己要处理的信息，例如路由技术就需要处理路由资源等。支撑类资源往往种类繁多，但在信息系统中，它们一般包括一系列的物理设施、电子设施、网络技术、操作系统等。

应用和支撑之间的区别：应用资源是以逻辑驱动技术，而支撑资源是以技术驱动逻辑。

2. 网络与信息安全的任务

网络安全的任务是保障各种网络资源(局域网资源、边界资源和网络基础设施)的稳定、可靠地运行和受控、合法地使用。

信息安全的任务是保障信息在存储、传输、处理等过程中的安全。具体的有：

(1) 机密性(confidentiality)：指防止非授权用户获得有用的信息的特性。

(2) 完整性(integrity)：指数据没有遭到非授权的更改和破坏。

(3) 不可抵赖性(non-repudiation)：指实体不能抵赖其发送、接受某信息或参与某活动事实的特性。

(4) 可用性(availability)：指保证授权用户对资源合法使用的特性。

3. 网络信息安全机制

网络信息安全通常是由一系列安全机制来实现的。所谓安全机制，是指将安全技术实现逻辑抽象而成的一系列的模式。

在网络信息安全领域，人们提出的高层机制主要有六种：预警、防护、检测、响应、恢复、反击。它们的关系如图 1-1 所示。

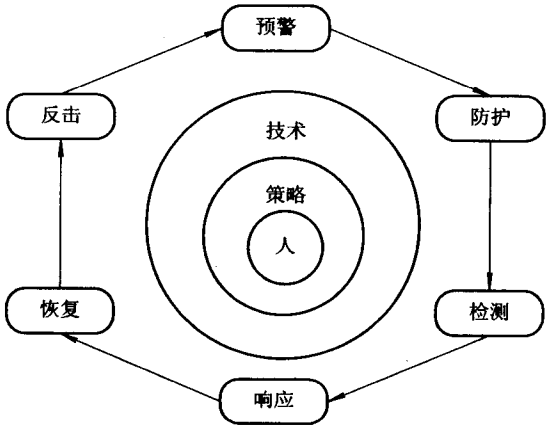

图 1-1　安全机制之间的关系

网络信息安全中层机制有：身份认证、授权、加密、网络隔离、高可用性、内容分析等。

网络信息安全基础应用域包括：网络基础设施安全、边界安全和局域网安全。网络信息安全具体应用域有：防火墙应用、入侵检测、反病毒软件、文件共享安全应用等。

安全服务(安全任务)、安全机制和安全应用域是网络信息安全系统的三要素，它们的关系可以用一个三维坐标进行表述，如图 1-2 所示。

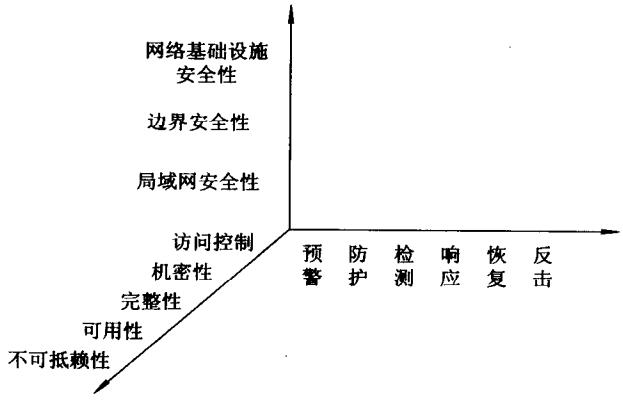

图 1-2　安全服务、安全机制和安全应用域之间的关系

4. 网络安全防范体系框架结构

为了能够有效地了解用户的安全需求，选择各种安全产品和策略，有必要建立一些系统的方法来进行网络安全防范。网络安全防范体系的科学性、可行性是其可顺利实施的保

障。图 1-3 给出了基于 DISSP 扩展的一个三维安全防范技术体系框架结构。第一维是安全服务，给出了八种安全属性(ITU-T REC-X.800-199103-I)。第二维是系统单元，给出了信息网络系统的组成。第三维是结构层次，给出并扩展了国际标准化组织 ISO 的开放系统互联(OSI)模型。

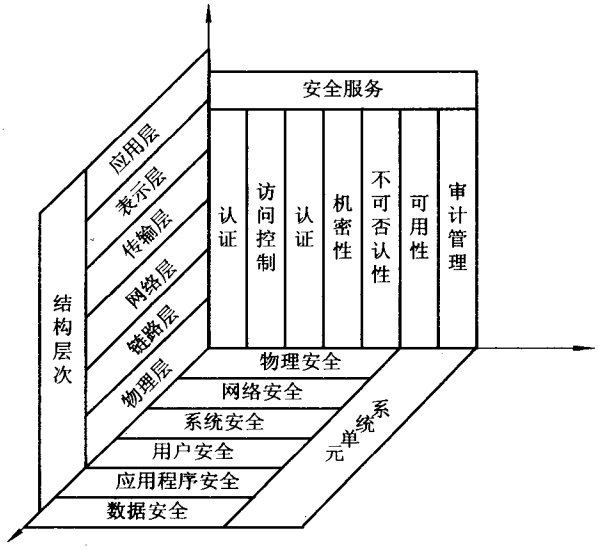

图 1-3　安全防范技术体系框架结构

1.3　网络安全防范体系层次

作为全方位的、整体的网络安全防范体系也是分层次的，不同层次反映了不同的安全问题。根据网络的应用现状和网络的结构，安全防范体系的层次可划分为物理层安全、系统层安全、网络层安全、应用层安全和安全管理，如图 1-4 所示。

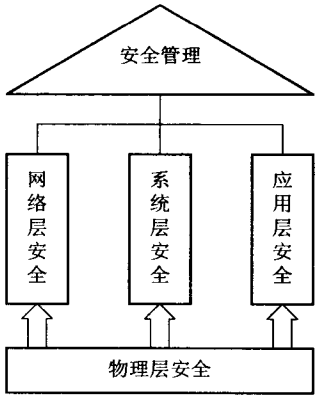

图 1-4　网络信息安全防范层次

1. 物理层安全

物理层安全包括通信线路的安全、物理设备的安全和机房的安全等。物理层的安全主要体现在通信线路的可靠性(线路备份、网管软件、传输介质)，软硬件设备安全性(替换设备、拆卸设备、增加设备)，设备的备份，防灾害能力，防干扰能力，设备的运行环境(温度、湿度、灰尘)，不间断电源保障，等等。

2. 系统层安全

系统层安全问题来自网络内使用的操作系统安全，如 Windows、UNIX 和 Linux 等。主要表现在三方面：一是操作系统本身的缺陷带来的不安全因素，主要包括身份认证、访问控制、系统漏洞等；二是对操作系统的安全配置问题；三是病毒对操作系统的威胁。

3. 网络层安全

网络层安全问题主要体现在网络方面的安全性，包括网络层身份认证、网络资源的访问控制、数据传输的保密与完整性、远程接入的安全、域名系统的安全、路由系统的安全、入侵检测的手段、网络设施防病毒等。

4. 应用层安全

应用层安全问题主要由提供服务的应用软件和数据的安全性产生，包括 Web 服务、电子邮件系统、DNS 等。此外，还包括病毒对应用系统的威胁。

5. 管理层安全

管理层安全包括安全技术和设备的管理、安全管理制度、部门与人员的组织规章等。管理的制度化极大地影响着整个网络的安全，严格的安全管理制度、明确的部门安全职责划分、合理的人员角色配置都可以在很大程度上降低各个层次的安全漏洞。

1.4 常见网络信息安全技术

1. 密码技术

数据加密就是利用密钥对原来为明文的数据信息按某种算法进行处理使其成为不可读的密文的过程。解密是加密的逆过程，利用密钥从密文信息中得到原始明文信息。现代数据加密技术主要分为两类：对称加密和公钥加密。对称加密是指加密和解密的密钥是一样的(如 DES)，而公钥加密是指加密密钥和解密密钥是相对独立的(如 RSA)。

2. 身份认证

身份认证是指验证实体与其所宣称的实体是否一致的过程。身份认证是用于保证网络信息资源被合法用户得到合理使用的基本技术手段。

3. 数字签名

数字签名是用来证明信息是由发送者签发的和信息没有被他人篡改的技术。一般数字签名是通过对源信息的 Hash 函数值进行加密来实现的。

4. 防火墙

防火墙的本义原是指古代人们房屋之间修建的那道墙，这道墙可以防止火灾发生的时候火烟蔓延到别的房屋。而这里所说的防火墙是指在本地网络与外界网络之间的一道防御系统。防火墙是在两个网络通信时执行的一种访问控制尺度，它能允许你“同意”的人和数据进入你的网络，同时将你“不同意”的人和数据拒之门外，最大限度地阻止网络中的黑客来访问你的网络。

5. 入侵检测

入侵检测是防火墙的合理补充，帮助系统对付网络攻击，扩展了系统管理员的安全管理能力(包括安全审计、监视、进攻识别和响应)，提高了信息安全基础结构的完整性。它从计算机网络系统中的若干关键点收集信息，并分析这些信息，看看网络中是否有违反安全策略的行为和遭到袭击的迹象。入侵检测被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下能对网络和系统进行监测，从而提供对内部攻击、外部攻击和误操作的实时保护。

6. 漏洞扫描

漏洞扫描就是对重要网络和计算机信息系统进行检查，发现其中可被黑客利用的漏洞。漏洞扫描的结果实际上就是系统安全性能的一个评估，它指出了哪些攻击是可能的，因此成为安全方案的一个重要组成部分。目前，漏洞扫描从技术上来划分，可以分为基于网络的扫描和基于主机的扫描两种类型。

习　题

1.1　网络信息安全的根源有哪些?
1.2　网络信息系统的资源有哪些?
1.3　网络信息安全的任务是什么?
1.4　网络安全防范体系有哪些层次?
1.5　常见的网络信息安全技术有哪些?

第2章 密码技术

2.1 密码学基本概念

密码学是研究如何实现数据加密的学科，密码学包括两方面内容，即密码编码学和密码分析学。将数据保密的技术和科学叫做密码编码学，与此对应的是破译密文的技术和科学叫做密码分析学。

假设发送者 Alice 想安全地发送消息 m 给接收者 Bob，利用加密技术的通信过程如图 2-1 所示。由于窃听者 Eve 只能看到加密后的密文信息故不能知道消息 m 的内容。其中，消息 m 被称为明文(plaintext)。对需要保密的消息进行编码的过程称为加密，编码的规则称为加密算法，被加密的消息称为密文(ciphertext)，而把密文转变为明文的过程称为解密，解密的规则称为解密算法。

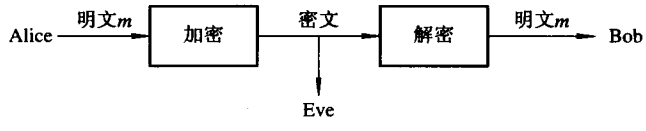

图 2-1 加密和解密

密码算法是用于加密和解密的数学函数，如果密码算法的保密性是基于算法的保密，这种算法称为受限制的算法，这种算法具有历史意义，但按照现在的安全标准，它们的保密性已远远不够，现代密码学采用密钥来解决这个问题，密钥用 K 来表示(如图 2-2 所示)。加密算法和解密算法通常在一对密钥(K)的控制下进行，分别称为加密密钥和解密密钥。

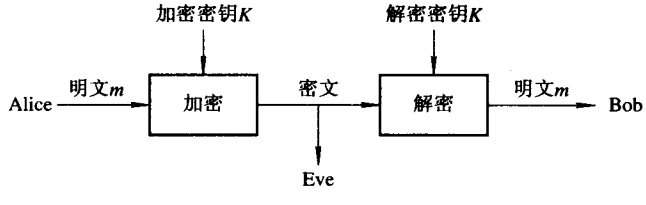

图 2-2 有密钥的加密和解密

一个现代密码系统(体制)包括所有可能的明文、密文、密钥、加密算法和解密算法，所有这些算法的安全性都基于密钥的安全性，而不是基于算法的细节的安全性。这就意味着算法可以公开，即使窃听者知道你的算法也没有关系，如果他不知道你使用的具体密钥，就不可能阅读到你的消息。

密码系统根据密钥可以分为两类，即为对称密钥系统和公钥系统。对称密钥系统就是加密密钥能够从解密密钥中推算出来，反过来也成立。在大多数对称算法中，加/解密密钥是相同的。公钥系统又称公开密钥系统或非对称密钥系统，有两个密钥，一个是公开的，