普通高等教育“十一五”国家级规划教材

首届中国大学出版社图书奖

中央网信办暨教育部评选的国家网络安全优秀教材奖

教育部高等学校信息安全专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

网络空间安全重点规划丛书

顾问委员会主任：沈昌祥 编委会主任：封化民

现代密码学
(第4版)

杨 波 编著

Cyberspace Security

根据教育部高等学校信息安全专业教学指导委员会编制的
《高等学校信息安全专业指导性专业规范》组织编写

清华大学出版社

普通高等教育“十一五”国家级规划教材

首届中国大学出版社**图书奖**

中央网信办暨教育部评选的**国家网络安全优秀教材奖**

教育部高等学校信息安全专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

网络空间安全重点规划丛书

现代密码学

(第4版)

杨　波　编著

清华大学出版社
北京

内 容 简 介

本书全面而详细地介绍现代密码学的理论和相关算法，可帮助读者将所学知识应用于信息安全实践。全书共分10章，内容包括现代密码学的基本概念、流密码、分组密码、公钥密码、密钥分配与密钥管理、消息认证和哈希函数、数字签名和认证协议、密码协议、可证明安全、网络加密与认证。

本书从教材使用的角度考虑，概念清晰、结构合理、讲解通俗易懂、内容深入浅出，并充分考虑方便教师在教学过程中的实施，同时还注意与其他专业课教学的衔接。本书取材新颖，不仅介绍现代密码学所涉及的基础理论和实用算法，而且涵盖了现代密码学的最新研究成果，力求使读者通过本书的学习而了解本学科最新的发展方向。

本书可作为高等学校相关专业大学生和研究生的教材，也可作为通信工程师和计算机网络工程师的参考读物。

图书在版编目(CIP)数据

现代密码学/杨波编著. —4版. —北京：清华大学出版社，2017
(网络空间安全重点规划丛书)
ISBN 978-7-302-46555-3

Ⅰ. ①现… Ⅱ. ①杨… Ⅲ. ①密码学—高等学校—教材 Ⅳ. ①TN918.1

中国版本图书馆CIP数据核字(2017)第030107号

责任编辑：张　民　李　晔
封面设计：常雪影
责任校对：李建庄
责任印制：刘海龙

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 刷 者：三河市君旺印务有限公司
装 订 者：三河市新茂装订有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：20　　**字　　数**：485千字
版　　次：2003年8月第1版　2017年7月第4版　　**印　　次**：2017年7月第1次印刷
印　　数：1～2000
定　　价：49.50元

产品编号：073430-01

网络空间安全重点规划丛书

编审委员会

出版说明

21世纪是信息时代，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世界发展的潮流和核心，而信息安全在信息社会中将扮演极为重要的角色，它会直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展，全球对信息安全人才的需求量不断增加，但我国目前信息安全人才极度匮乏，远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾，必须加快信息安全人才的培养，以满足社会对信息安全人才的需求。为此，教育部继2001年批准在武汉大学开设信息安全本科专业之后，又批准了多所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信、物理、数学等领域的交叉学科，对于这一新兴学科的培养模式和课程设置，各高校普遍缺乏经验，因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动，并成立了“高等院校信息安全专业系列教材”编审委员会，由我国信息安全领域著名专家肖国镇教授担任编委会主任，指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则，认真研讨国内外高等院校信息安全专业的教学体系和课程设置，进行了大量前瞻性的研究工作，而且这种研究工作将随着我国信息安全专业的发展不断深入。系列教材的作者都是既在本专业领域有深厚的学术造诣、又在教学第一线有丰富的教学经验的学者、专家。

该系列教材是我国第一套专门针对信息安全专业的教材，其特点是：

① 体系完整、结构合理、内容先进。

② 适应面广：能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。

③ 立体配套：除主教材外，还配有多媒体电子教案、习题与实验指导等。

④ 版本更新及时，紧跟科学技术的新发展。

在全力做好本版教材，满足学生用书的基础上，还经由专家的推荐和审定，遴选了一批国外信息安全领域优秀的教材加入到系列教材中，以进一步满足大家对外版书的需求。“高等院校信息安全专业系列教材”已于2006年年初正式列入普通高等教育“十一五”国家级教材规划。

2007年6月，教育部高等学校信息安全类专业教学指导委员会成立大会

暨第一次会议在北京胜利召开。本次会议由教育部高等学校信息安全类专业教学指导委员会主任单位北京工业大学和北京电子科技学院主办,清华大学出版社协办。教育部高等学校信息安全类专业教学指导委员会的成立对我国信息安全专业的发展起到重要的指导和推动作用。2006年教育部给武汉大学下达了"信息安全专业指导性专业规范研制"的教学科研项目。2007年起该项目由教育部高等学校信息安全类专业教学指导委员会组织实施。在高教司和教指委的指导下,项目组团结一致,努力工作,克服困难,历时5年,制定出我国第一个信息安全专业指导性专业规范,于2012年年底通过经教育部高等教育司理工科教育处授权组织的专家组评审,并且已经得到武汉大学等许多高校的实际使用。2013年,新一届"教育部高等学校信息安全专业教学指导委员会"成立。经组织审查和研究决定,2014年以"教育部高等学校信息安全专业教学指导委员会"的名义正式发布《高等学校信息安全专业指导性专业规范》(由清华大学出版社正式出版)。

2015年6月,国务院学位委员会、教育部出台增设"网络空间安全"为一级学科的决定,将高校培养网络空间安全人才提到新的高度。2016年6月,中央网络安全和信息化领导小组办公室(下文简称中央网信办)、国家发展和改革委员会、教育部、科学技术部、工业和信息化部及人力资源和社会保障部六大部门联合发布《关于加强网络安全学科建设和人才培养的意见》(中网办发文[2016]4号)。为贯彻落实《关于加强网络安全学科建设和人才培养的意见》,进一步深化高等教育教学改革,促进网络安全学科专业建设和人才培养,促进网络空间安全相关核心课程和教材建设,在教育部高等学校信息安全专业教学指导委员会和中央网信办资助的网络空间安全教材建设课题组的指导下,启动了"网络空间安全重点规划丛书"的工作,由教育部高等学校信息安全专业教学指导委员会秘书长封化民校长担任编委会主任。本规划丛书基于"高等院校信息安全专业系列教材"坚实的工作基础和成果、阵容强大的编审委员会和优秀的作者队伍,目前已经有多本图书获得教育部和中央网信办等机构评选的"普通高等教育本科国家级规划教材"、"普通高等教育精品教材"、"中国大学出版社图书奖"和"国家网络安全优秀教材奖"等多个奖项。

"网络空间安全重点规划丛书"将根据《高等学校信息安全专业指导性专业规范》(及后续版本)和相关教材建设课题组的研究成果不断更新和扩展,进一步体现科学性、系统性和新颖性,及时反映教学改革和课程建设的新成果,并随着我国网络空间安全学科的发展不断完善,力争为我国网络空间安全相关学科专业的本科和研究生教材建设、学术出版与人才培养做出更大的贡献。

我们的E-mail地址是:zhangm@tup.tsinghua.edu.cn,联系人:张民。

"网络空间安全重点规划丛书"编审委员会

前言

当今世界，互联网深刻改变了人们的生产和生活方式，但我们在网络安全方面却面临着严峻挑战。从宏观上说，网络安全是事关国家安全的重大战略问题——没有网络安全就没有国家安全；从微观上看，网络安全关乎我们每个人的信息安全。网络安全指网络系统中硬件、软件及其系统中的数据安全。从本质上说，网络安全就是网络上的信息安全。

信息安全又分为系统安全（包括操作系统的安全、数据库系统的安全等）、数据安全（包括数据的安全存储、安全传输）和内容安全（包括病毒的防护、不良内容的过滤等）3 个层次，是一个综合、交叉的学科领域，要利用数学、电子、信息、通信、计算机等诸多学科的长期知识积累和最新发展成果。信息安全研究的内容很多，涉及安全体系结构、安全协议、密码理论、信息分析、安全监控、应急处理等，其中密码技术是保障数据安全的关键技术。

密码技术中的加密方法包括单钥密码体制（又称为对称密码体制）和公钥密码体制，而单钥密码体制又包括流密码和分组密码。本书在第 1 章介绍现代密码学的基本概念后，在第 2～4 章分别介绍流密码、分组密码、公钥密码。不管哪种密码体制都需要用到密钥，因此密钥分配与密钥管理也是密码技术的重要内容，这部分内容在第 5 章介绍。信息的安全性除要考虑保密性外，还需考虑信息的真实性、完整性、顺序性、时间性以及不可否认性。本书以 3 章的篇幅（第 6 章消息认证和哈希算法、第 7 章数字签字和认证协议、第 8 章密码协议）介绍这部分内容。第 9 章可证明安全介绍如何刻画公钥密码体制的语义安全性。第 10 章网络加密与认证介绍加密技术和认证技术在网络中的具体应用。书中 4.1.5 节的卡米歇尔定理、4.1.11 节循环群、4.1.12 节循环群的选取、8.3 节安全多方计算协议、第 9 章可证明安全供研究生使用。

本书自 2003 年 8 月第 1 版以来，已被 150 余所学校作为教材，曾获批普通高等教育“十一五”国家级规划教材，2016 年获得首届国家网络安全优秀教材奖。第 4 版在第 3 版的基础上进行修订，因为内容陈旧而去掉了原 5.3 节，重新编写了第 9 章，增加了 3.7 节、3.8 节、6.1.4 节、6.6 节和 7.4 节。

本书的特点：一是内容新颖、深入、全面，涵盖了现代密码学的最新成果；二是内容的安排充分考虑到作为教材，如何方便地在教学中使用。

在本书的编写过程中,参考了国内外的有关著作和文献,特别是Stallings、王育民、卢开澄、朱文余等人的著作。

西安电子科技大学通信工程学院的肖国镇教授作为本书的责任编委,认真审阅了全书并提出了许多宝贵的指导意见,对此表示特别的感谢。清华大学出版社张民编辑为本书的出版做了大量的工作,在此表示衷心的感谢。

由于作者水平有限,书中不足在所难免,恳请读者批评指正。

作　者

2017年4月

目录

第1章 引 言

1.1 信息安全面临的威胁

1.1.1 安全威胁

信息在社会中的地位和作用越来越重要，已成为社会发展的重要战略资源，信息技术改变着人们的生活和工作方式，信息产业已成为新的经济增长点，社会的信息化已成为当今世界发展的潮流和核心。与此同时信息的安全问题也已成为世人关注的社会问题。人们对信息安全的认识随着网络的发展经历了以下一个由简单到复杂的过程。

20世纪70年代，主机时代的信息安全是面向单机的，由于早期的用户主要是军方，因此在安全性方面主要考虑的是信息的保密性。

20世纪80年代，微机和局域网的兴起带来了信息在微机间的传输和用户间的共享问题，丰富了信息安全的内涵，使人们认识到数据完整性、可用性的重要性。安全服务、安全机制等基本框架，成为信息安全的重要内容。

20世纪90年代，因特网爆炸性的发展把人类带进了一个新的生存空间。因特网具有高度分布、边界模糊、层次欠清、动态演化，而用户又在其中扮演主角的特点，如何保证这一复杂而巨大系统的安全，成为信息安全的主要问题。由于网的全球性、开放性、无缝连通性、共享性、动态性发展，使得任何人都可以自由地接入，其中有善者，也有恶者。恶者会采用各种攻击手段进行破坏活动。信息安全面临的攻击有独立的犯罪者、有组织的犯罪集团和国家情报机构。对信息的攻击具有以下新特点：无边界性、突发性、蔓延性和隐蔽性。因此考虑信息安全，就要首先知道信息安全面临哪些威胁。

信息安全所面临的威胁来自很多方面，并且随着时间的变化而变化。这些威胁可以宏观地分为人为威胁和自然威胁。

自然威胁可能来自于各种自然灾害、恶劣的场地环境、电磁辐射和电磁干扰、网络设备自然老化等。这些无目的的事件，有时会直接威胁信息的安全，影响信息的存储介质。

我们主要讨论人为威胁，也就是对信息的人为攻击。这些攻击手段都是通过寻找系统的弱点，以便达到破坏、欺骗、窃取数据等目的，造成经济上和政治上不可估量的损失。人为攻击可分为被动攻击和主动攻击，如图1-1所示。

1. 被动攻击

被动攻击即窃听，是对系统的保密性进行攻击，如搭线窃听、对文件或程序的非法复

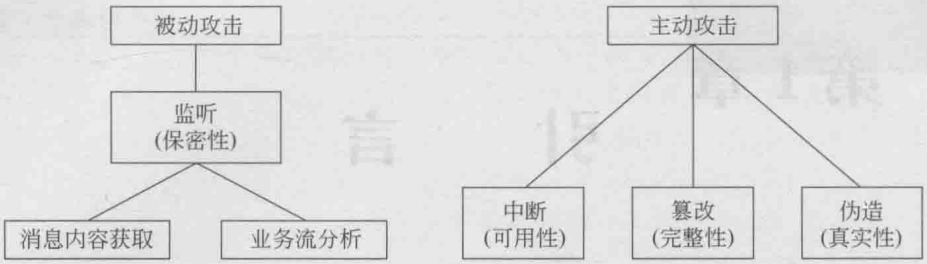

图 1-1 攻击类型分类

制等,以获取他人的信息。被动攻击又分为两类:一类是获取消息的内容,很容易理解;第二类是进行业务流分析,假如我们通过某种手段,例如加密,使得敌手从截获的消息无法得到消息的真实内容,然而敌手却有可能获得消息的格式、确定通信双方的位置和身份以及通信的次数和消息的长度,这些信息可能对通信双方来说是敏感的,例如公司间的合作关系可能是保密的、电子邮件用户可能不想让他人知道自己正在和谁通信、电子现金的支付者可能不想让别人知道自己正在消费、Web 浏览器用户也可能不愿意让别人知道自己正在浏览哪一个站点。

被动攻击因不对消息做任何修改,因而是难以检测的,所以抗击这种攻击的重点在于预防而非检测。

2. 主动攻击

这种攻击包括对数据流的某些篡改或产生某些假的数据流。主动攻击又可分为以下3类:

(1) 中断。中断是对系统的可用性进行攻击,如破坏计算机硬件、网络或文件管理系统。

(2) 篡改。篡改是对系统的完整性进行攻击,如修改数据文件中的数据、替换某一程序使其执行不同的功能、修改网络中传送的消息内容等。

(3) 伪造。伪造是对系统的真实性进行攻击,如在网络中插入伪造的消息或在文件中插入伪造的记录。

绝对防止主动攻击是十分困难的,因为需要随时随地对通信设备和通信线路进行物理保护,因此抗击主动攻击的主要途径是检测,以及对此攻击造成的破坏进行恢复。

1.1.2 入侵者和病毒

信息安全的人为威胁主要来自用户(恶意的或无恶意的)和恶意软件的非法侵入,入侵信息系统的用户也称为黑客,黑客可能是某个无恶意的人,其目的仅仅是破译和进入一个计算机系统;或者是某个心怀不满的雇员,其目的是对计算机系统实施破坏;也可能是一个犯罪分子,其目的是非法窃取系统资源(如窃取信用卡号或非法资金传送),对数据进行未授权的修改或破坏计算机系统。

恶意软件指病毒、蠕虫等恶意程序,分为两类(如图 1-2 所示):一类需要主程序,另一类不需要。前者是某个程序中的一段,不能独立于实际的应用程序或系统程序;后者是