高·等·院·校·信·息·安·全·专·业·系·列·教·材

中国计算机学会教育专业委员会与清华大学出版社联合组织编写

名誉主编：何德全　编委会主任：肖国镇

Modern Cryptography

现代密码学

杨波 编著

http://www.tup.tsinghua.edu.cn

清华大学出版社

高·等·院·校·信·息·安·全·专·业·系·列·教·材

Modern Cryptography

现代密码学

杨波 编著

清华大学出版社
北京

内 容 简 介

本书旨在介绍现代密码学的基本原理及方法。全书共分 8 章，第 1 章介绍现代密码学的基本概念，其余各章分别介绍流密码、分组密码、公钥密码、密钥分配与密钥管理、消息认证和杂凑算法、数字签字和密码协议、网络加密与认证。

本书内容翔实，概念表述严谨，语言精练，例题丰富，切合教学之用。

本书可作为高等院校信息安全、计算机、通信工程、密码学及相关专业大学本科生和研究生的教材，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. —北京：清华大学出版社，2003

(高等院校信息安全专业系列教材)

ISBN 7-302-06814-3

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

中国版本图书馆 CIP 数据核字(2003)第 050134 号

出 版 者：清华大学出版社

http://www.tup.tsinghua.edu.cn

社 总 机：010-62770175

地　　址：北京清华大学学研大厦

邮　　编：100084

客户服务：010-62776969

责任编辑：张　民

封面设计：孟繁聪

版式设计：刘祎淼

印 刷 者：北京四季青印刷厂

发 行 者：新华书店总店北京发行所

开　　本：185×230　**印张**：15　**字数**：295 千字

版　　次：2003 年 8 月第 1 版　2003 年 8 月第 1 次印刷

书　　号：ISBN 7-302-06814-3/TP・5065

印　　数：1～5000

定　　价：24.00 元

高等院校信息安全专业系列教材

编审委员会

序

在社会信息化的进程中，信息已成为社会发展的重要资源，信息安全也成为21世纪国际竞争的重要战场。为了保护国家的政治利益和经济利益，各国政府都非常重视信息和网络安全，信息安全已成为一个世纪性、全球性的研究课题。

我国的信息安全事业正在蓬勃发展，国家领导高度重视，各部门通力合作、统筹规划，大大加快了我国信息安全产业发展的步伐。随着信息安全产业的快速发展，社会对信息安全人才的需求在不断增加，在高等教育领域大力推进信息安全的专业化教育，将是国家在信息安全领域掌握自主权、占领先机的重要举措。

目前，许多大学和科研院所已创办了信息安全专业或是开设了相关课程。很高兴中国计算机学会教育专业委员会和清华大学出版社在近期联合组织了一系列信息安全专业的研讨活动。他们以严谨负责的态度，认真组织全国各高校和科研院所的专家、学者，共同研讨信息安全专业的教育方法和课程体系，并在进行大量前瞻性研究工作的基础上，启动了“高等院校信息安全专业系列教材”的编写工作。这套教材将是我国信息安全专业的第一套完整、权威的教材，相信可以对全国的高等院校信息安全专业的建设起到很好的促进作用。

希望中国计算机学会教育专业委员会和清华大学出版社能够将这个研究课题一直做下去，也希望这套教材能够取得成功并不断完善，以促进各高等院校培养出更多、更好的信息安全专门人才，为我国的信息安全事业做出更大的贡献。

何德全

中国工程院院士

高等院校信息安全专业系列教材编审委员会名誉主编

2003年7月于北京

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，国家对信息安全人才的需求量不断增加，但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、通信工程、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何德全院士担任名誉主编，著名学者肖国镇教授担任编委会主任，共同指导“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。经过编委会全体委员及相关专家的推荐和审定，确定了编写教材的作者，这些作者绝大多数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。

本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。

为了保证出版质量，我们坚持宁缺毋滥的原则，成熟一本，出版一本，并保持不断更新，力求将我国信息安全领域教育、科研的最新成果和成熟经验反映到教材中来。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本系列教材中，以进一步满足大家对外版书的需求。热切期望广大教师和科研工作者加入我们的队伍，同时也欢迎广大读者提出宝贵意见，以便我们对本系列教材的组织、编写与出版工作不断改进，为我国信息安全专业的教材建设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。

中国计算机学会教育专业委员会

清华大学出版社

2003 年 7 月

前言

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，信息安全的主要内容是信息的保密性。

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，如何处理好这一复杂而又巨大的系统的安全，成为信息安全的主要问题。由于因特网的全球性、开放性、无缝连通性、共享性和动态性发展，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可能会来自独立的犯罪者、有组织的犯罪集团和国家情报机构。

信息安全可分为系统安全（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，它涉及安全体系结构、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 章介绍了现代密码学的基本概念后，第 2、3、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、时间性和不可否认性，本书以两章的篇幅（第6章消息认证和杂凑算法、第7章数字签字和认证协议）介绍这部分内容。最后一章（第8章网络加密与认证）介绍了加密技术和认证技术在网络中的具体应用。

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；二是在内容的取舍、安排等方面充分体现了教材的特点，便于教师在教学过程中实施。

本书在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、朱文余等教授的著作。

最后要特别感谢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，肖教授认真审阅了全书并提出了许多宝贵的指导意见。清华大学出版社也为本书的出版做了大量的工作，作者在此对他们表示衷心的感谢。

作　者

2003年7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，信息安全的主要内容是信息的保密性。

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，如何处理好这一复杂而又巨大的系统的安全，成为信息安全的主要问题。由于因特网的全球性、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可能会来自独立的犯罪者、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。因此要了解信息安全，首先应该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。这些事件有时会直接威胁信息的安全，影响信息的存储媒质。

本节主要讨论人为威胁，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。

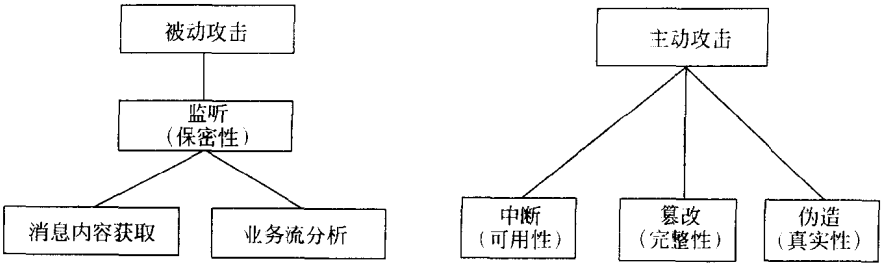

图 1-1 攻击类型分类

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；另一类是进行业务流分析，假如通过某种手段，比如加密，使得敌手无法从截获的消息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，这些信息对通信双方来说可能是敏感的，例如公司间的合作关系可能是保密的、电子函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

主动攻击包括对数据流的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　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　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　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。