高等学校电子与通信类专业“十一五”规划教材

应用密码学

张仕斌 万武南
张金全 孙宣东 编著

西安电子科技大学出版社
http://www.xduph.com

高等学校电子与通信类专业“十一五”规划教材

应用密码学

张仕斌　万武南
张金全　孙宣东　编著

西安电子科技大学出版社

2009

内 容 简 介

本书是作者在多年的教学与科研实践的基础上，按照高等院校的培养目标和基本要求，为实施教学改革，使密码学技术面向应用实践，而编写的一本应用密码学技术基础教材。本书在全面讲解密码学基本知识和阐述密码理论的同时，还介绍了大量的算法，阐述了部分算法的安全性以及密码学发展的新方向；为了强化密码算法的理解、掌握与应用，本书还介绍了一些典型密码算法的应用以及密码算法的课程设计，每章后都配有相应的习题以实现学与练的统一。

全书共 11 章，主要内容包括密码学基础知识、古典密码、对称密码、序列密码、非对称密码、Hash 函数、数字签名、身份认证技术、密钥管理技术、密码学的新方向、密码学的应用等。本书内容丰富详实、构思新颖、突出适用，既可作为普通高等院校信息安全、密码学、应用数学、通信工程、计算机、电子商务等相关专业的本科生或研究生的教学用书，也可作为相关领域技术人员的参考书。

图书在版编目(CIP)数据

应用密码学/张仕斌等编著. —西安：西安电子科技大学出版社，2009.12

高等学校电子与通信类专业“十一五”规划教材

ISBN 978-7-5606-2345-0

Ⅰ.应… Ⅱ.张… 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(2009)第 174397 号

策　　划　李惠萍

责任编辑　李惠萍

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

网　　址　www.xduph.com　　电子邮箱　xdupfxb001@163.com

经　　销　新华书店

印刷单位　西安文化彩印厂

版　　次　2009 年 12 月第 1 版　2009 年 12 月第 1 次印刷

开　　本　787 毫米×1092 毫米　1/16　印　张　17.25

字　　数　406 千字

印　　数　1～4000 册

定　　价　25.00 元

ISBN 978-7-5606-2345-0/TN·0537

XDUP 2637001-1

前　言

21世纪以来，随着信息化在全球的快速发展，信息系统及其运行的安全性与社会经济发展和公众利益的关系越来越密切；同时，传统的社会活动不断向网络空间延伸扩展，网络空间中的竞争与对抗越来越尖锐、复杂。这些因素已经构成了重要的国家安全问题，关系到一个国家的政治、经济、文化、科技和国防安全。

密码技术是信息安全技术的内核和基石，这方面的任何重大进展，都有可能改变信息安全技术的走向。同时，密码技术的技巧和方法自始至终深刻影响着整个信息安全技术界的发展和突破。密码技术作为信息安全技术的核心，在保障网络信息安全的应用中具有重要的意义，而对典型密码学算法的掌握又是快速实现信息安全的捷径。

本书是作者结合自身多年的教学和科研工作实践经验、在广泛调研和充分论证并参考众多国内外有关网络信息安全和应用密码学文献的基础上，通过教学实践，为高等院校信息安全、密码学、应用数学、通信工程、计算机、电子商务等相关专业的本科生和研究生编写的一本专业教材。在本书的编写中，始终遵循这样一个目标：为网络与信息安全领域提供一本既可以作为教学用书，也可以作为专业技术人员参考书的实用教材。

作者力求本书能体现以下特色：

★ 先进性：本书给出一些具有代表性而且比较重要的例子，描述了当前及未来具有很强应用前景的对称密码体制与非对称密码体制在密码芯片、移动通信、电子商务和工业等领域中的应用，以及典型的密码算法的应用(如数字签名、身份识别和电子货币等)。

★ 易学性：在内容安排上力求深入浅出、条理清晰，尽量使各章内容相互独立，以便读者学习时可以跳过自己不需要的章节，而不影响其它章节的理解。

★ 实用性：在讲述应用密码学基本概念、基本理论之前，介绍了与密码学基本理论、基本概念相关的数论知识，弥补了其它密码学专著忽略密码学相关数学知识的不足。通过阅读本书，读者可以对密码学涉及到的所有数学知识有一个比较全面的了解，有助于加深读者对密码学的理解。

★ 典型性：通过必要的实例和典型密码算法的基本工作原理及其应用方法对密码学进行较系统、深入的介绍，密码算法的选取和例题设置等方面都体现出广泛的代表性和典型性，为读者快速掌握和应用密码学的核心概念、方法与技术提供了便利。

★ 实践性：本书的附录部分是密码学算法应用的课程设计，通过课程设计的实践既增强了学生对密码算法的理解与掌握，同时也锻炼了他们将实践与理论相结合的能力。

本书的编排从教学适用性出发，特别重视读者对应用密码学知识的系统理解和有针对性地重点掌握关键内容；在体系结构、语言表达、内容选取和应用举例等方面都做了特别的考虑，因此本书也适于自学。

在本书的编写过程中，作者除了介绍自身的研究内容以外，还参考了国内外大量的书

籍及 Internet 上公布的相关资料，对此作者都尽量在参考文献中列出。但由于网上资料数量众多且杂乱，可能无法对所有文献一一注明出处。这些资料大多来源于众多大学、研究机构、商业公司及一些研究网络安全技术的个人，他们为推动网络安全技术的发展做出了贡献，在此表示衷心的感谢。作者写作过程中参考的这些资料，其原文版权属于原作者，特此声明。

本书由张仕斌教授组织编写并进行统稿，其中第 1 章、第 8 章、第 9 章和第 10 章由张仕斌老师编写，第 2 章和第 4 章由孙宣东老师编写，第 3 章和第 6 章由万武南老师编写，第 5 章、第 7 章和附录由张金全老师编写，第 11 章由张仕斌和万武南老师共同编写。

为了便于多媒体教学，本书配有电子教案(PPT)，订购本教材的教师可到出版社网站上下载(http://www.xduph.com)。

由于现代密码技术及应用发展迅速，作者水平有限，加上时间仓促，书中难免有不足之处，敬请斧正。

作　者

2009 年 7 月于成都

目　录

第1章 绪 论

知识点

◇ 信息安全的基本概念
◇ 信息安全机制与信息安全服务
◇ 密码学在信息安全中的作用
◇ 信息安全模型
◇ 密码学的基本知识
◇ 密码体制的安全性

本章导读

本章首先介绍信息安全的基本概念及基本属性、信息安全问题的根源、信息安全服务与信息安全机制和信息安全攻击的主要形式；接着介绍信息安全模型、密码学在信息安全中的作用；然后再介绍密码学的发展简史、密码学的基本概念和密码体制的构成及其分类；最后介绍密码分析及方法和密码体制的安全性。通过对本章的学习，可使读者对信息安全和密码学的基本知识及它们之间的关系有一个初步了解，对读者按计划学好本书后续知识具有重要的指导作用。

1.1 信息安全概述

信息是信息化社会发展的重要战略资源，也是衡量一个国家综合国力的重要指标之一。信息的普遍性、共享性、增值性、可处理性和多效用性，使其对于人类具有特别重要的意义。在信息时代，任何一个国家的政治、军事和外交等都离不开信息，经济建设、科学的发展和技术的进步也离不开信息。对信息的开发、控制和利用已成为国家间利益争夺的重要内容。当前，随着网络信息技术的迅猛发展，信息的地位与作用仍然在急剧上升，信息安全问题因此而日益突出。未来的军事斗争将首先在信息领域展开，并全程贯穿着信息战，信息安全将成为赢得战争胜利的重要保障。特别是在当前我国信息化建设已进入高速发展的阶段，电子政务、电子商务、网络金融、网络媒体等蓬勃发展，这些与国民经济、社会稳定发展息息相关的领域急需信息安全保障。因此，加强信息安全技术的研究，提高信息安全的应用水平，在信息系统应用领域营造信息安全氛围，既是时代发展的客观要求，

也是未来信息技术发展的迫切需要。

1. 信息安全的基本概念

1) 信息安全的定义

到目前为止，“安全”并没有统一的定义，但其基本含义可以理解为：客观上不存在威胁，主观上不存在恐惧。“信息安全”同样也没有公认和统一的定义，但国内外对信息安全的论述大致可分为两大类：一是指具体的信息系统的安全；而另一类则是指某一特定信息体系结构的安全，比如一个国家的金融系统、军事指挥系统。但一些专家认为这两种定义均很片面，所涉及的内容过窄。我们认为，信息安全是指一个国家社会信息化状态不受外来的威胁与侵害，一个国家的信息技术体系不受外来的威胁与侵害。这是因为“信息安全”应该首先是一个国家宏观的社会信息化状态是否处于自主控制之下，是否稳定的问题，其次才是信息技术安全的问题。

2) 信息安全的基本属性

不管攻击者采用什么样的手段，他们都要通过攻击信息的基本属性来达到攻击的目的。在技术层次上，信息安全应是保证在客观上杜绝对信息的安全威胁，使得信息的拥有者在主观上对其信息的本源性放心。信息安全根据其本质的界定，应具有以下所述基本属性：

(1) 保密性(Confidentiality)：指信息不泄漏给非授权的个人、实体和过程，或供其使用的特性。

(2) 完整性(Integrity)：指信息未经授权不能被修改、不被破坏、不被插入、不延迟、不乱序和不丢失的特性。对网络信息安全进行攻击其最终目的就是破坏信息的完整性。

(3) 可用性(Avaliability)：指合法用户访问并能按要求顺序使用信息的特性，即保证合法用户在需要时可以访问到所需信息及相关资料。对可用性的攻击就是阻断信息的可用性，如破坏网络和有关系统的正常运行就属于这类攻击。

(4) 可控性(Controlability)：指授权机构对信息的内容及传播具有控制能力的特性，可以控制授权范围内的信息流向以及信息传播方式。

(5) 可审查性(Auditability)：指在信息交流过程结束后，通信双方不能抵赖曾经做出的行为，也不能否认曾经接收到对方的信息。

(6) 可靠性(Reliability)：指信息以用户认可的质量连续服务于用户的特性(包括信息的准确、迅速和连续地传输、转移等)，但也有一些专家认为可靠性是人们对信息系统而不是对信息本身的要求。

信息安全其实质就是指采用一切可能的方法和手段，保护信息系统或信息网络中的信息资源免受各种类型的威胁、干扰和破坏，即保证信息的安全性，确保信息的上述“六性”的安全。

2. 信息安全问题的根源

现在讲信息安全问题，已经不再像以前那样仅简单地谈计算机病毒，信息安全的防御也不再是仅安装了病毒软件和防火墙就能达到目的，这是因为信息系统所面临的安全威胁正随着信息技术的广泛应用在不断地增加。产生信息安全问题的根源可以从以下两个方面来进行分析：一是我们使用的计算机所面临的安全威胁；二是网络系统所面临的威胁。

1）计算机所面临的主要安全威胁

随着个人计算机的普及，个人计算机也已成为黑客攻击的目标之一，就其安全威胁而言，主要涉及以下几个方面。

（1）计算机病毒：是当前最常见、最主要的威胁，几乎每天都有计算机病毒产生。计算机病毒的主要危害体现在破坏计算机文件和数据，导致文件无法使用，系统无法启动；消耗计算机CPU、内存和磁盘资源，导致一些正常服务无法进行，出现死机、占用大量的磁盘空间；有的还会破坏计算机硬件，导致计算机彻底瘫痪。

（2）木马：是一种基于远程控制的黑客工具，也称为“后门程序”。木马作为一种远程控制的黑客工具，主要危害包括窃取用户信息（比如计算机或网络账户和密码、网络银行账户和密码、QQ账户和密码、E-mail账户和密码等），携带计算机病毒（造成计算机或网络不能正常运行，甚至完全瘫痪），或被黑客控制，攻击用户计算机或网络。

（3）恶意软件：是指一类特殊的程序，是介于计算机病毒与黑客软件之间的软件的统称。它通常在用户不知晓也未授权的情况下潜入系统，具有用户不知道（一般也不许可）的特性，激活后将影响系统或应用的正常功能，甚至危害或破坏系统。其主要危害体现在非授权安装（也被称为“流氓软件”）、自动拨号、自动弹出各种广告界面、恶意共享和浏览器窃持等。当前，恶意软件的出现、发展和变化给计算机及网络系统带来了巨大的危害。

2）网络所面临的主要安全威胁

相对于个人计算机而言，网络所面临的安全威胁除具有计算机所面临的三种常见的威胁之外，主要是由于网络的开放性、网络自身固有的安全缺陷和网络黑客的入侵与攻击（人为的因素）等三个方面带来的安全威胁。

（1）网络的开放性：主要表现为由于网络业务都是基于公开的协议、连接的建立是基于主机上彼此信任的原则和远程访问，因而使得各种攻击无需到现场就能成功。正是由于网络的开放性，使得在虚幻的计算机网络中网络犯罪往往十分隐蔽，虽然有时会留下一些蛛丝马迹，但更多的时候是无迹可寻。

（2）网络自身固有的安全缺陷：这是网络安全领域首要关注的问题，发现系统漏洞（安全缺陷）也是黑客进行入侵和攻击的主要步骤。据调查，国内80%以上的网站存在明显的漏洞。漏洞的存在给网络上的不法分子的非法入侵提供了可乘之机，也给网络安全带来了巨大的风险。据美国CERT/CC统计，2006年总共收到系统漏洞报告8064个，平均每天超过22个（自1995年以来，漏洞报告总数已经达到30 780个）。这些漏洞的存在对广大互联网用户的系统造成了严重的威胁。

当前，操作系统的漏洞是我们面临的最大风险。比如，Windows操作系统是目前使用最为广泛的系统，但经常发现存在漏洞。过去Windows操作系统的漏洞主要被黑客用来攻击网站，对普通用户没有多大影响，但近年来一些新出现的网络病毒利用Windows操作系统的漏洞进行攻击，能够自动运行、繁衍、无休止地扫描网络和个人计算机，然后进行有目的的破坏。比如“红色代码”、“尼姆达”、“蠕虫王”以及“冲击波”等。随着Windows操作系统越来越复杂和庞大，出现的漏洞也越来越多，利用Windows操作系统漏洞进行攻击造成的危害越来越大，甚至有可能给整个互联网带来不可估量的损失。

（3）人为因素的威胁：虽然人为因素和非人为因素都对计算机及网络系统构成威胁，但精心设计的人为攻击（因素）威胁更大。人为因素的威胁是指人为造成的威胁，包括偶发

性和故意性威胁。具体来说主要包括网络攻击、蓄意入侵和计算机病毒等。一般来说，人为因素威胁可以分为人为失误、恶意攻击和管理不善。

◆ 人为失误：一是配置和使用中的失误，比如系统操作人员安全配置不当造成的安全漏洞，用户安全意识不强，用户口令选择不恰当，用户将自己的账号随意转借给他人或信息共享等都会对网络安全带来威胁；二是管理中的失误，比如用户安全意识薄弱，对网络安全不重视，安全措施不落实，导致安全事故发生。据调查表明，在发生安全事故的原因中，居前两位的分别是“未修补软件安全漏洞”和“登录密码过于简单或未修改”，这表明了大多数用户缺乏基本的安全防范意识和防范常识。

◆ 恶意攻击：是当前计算机及网络系统面临的最大威胁，主要分为两大类：一是主动攻击，它使用各种攻击方式有选择地破坏信息的完整性、有效性和可用性等；二是被动攻击，它是在不影响计算机及网络系统正常工作的情况下，进行信息的窃取、截获、破译等，以获取重要的机密信息。这两类攻击均能对计算机及网络系统造成极大的破坏，并导致机密信息泄露。

◆ 管理不善：一般来说，网络安全不能单靠网络安全技术来满足，还需要有完善的法律法规、管理制度才能达到期望的目标。目前，系统管理的不善也为一些不法分子造成可乘之机。据统计，80％以上的机密泄露都是由于系统内部人员管理不善造成的。同时，对网络系统的严格管理也是避免网络受到攻击的重要措施。

3. 信息安全服务与信息安全机制

当前，为了保证网络系统中信息安全的实现，人们通常在基于某些安全机制的基础上，向用户提供一定的安全服务，以保障各种资源合法地使用和稳定可靠地运行及传输。

1）安全服务

安全服务就是加强信息系统数据处理和信息传输安全性的一类服务，采用安全服务也能在一定程度上弥补和完善现有操作系统和信息系统的安全漏洞，其目的在于采用一种或多种安全机制阻止安全攻击。在 ISO 7498－2 标准中定义了 6 类可选的安全服务：鉴别(Authentication)、数据机密性(Data Confidentiality)、数据完整性(Data Integrity)、访问控制(Access Control)、可用性(Availability)、不可否认性(Non-repudiation)服务。

2）安全机制

所谓安全机制就是实现安全服务的技术手段，也是保护信息系统免受攻击及确保系统安全运行的重要手段。信息系统的安全是一个系统的概念，为了保障信息系统的安全可以采用多种安全机制。在 ISO 7498－2(我国称为 GB/T9387－2)标准中，将安全机制定义为特殊安全机制和通用安全机制两大类。特殊安全机制包括加密(Encryption)、数字签名(Digital Signature)、访问控制(Access Control)、数据完整性(Data Integrity)、鉴别(Authentication)、业务流量填充(Traffic Padding)、路由控制(Routing Control)和公正机制(Notarization Mechanisms)；通用安全机制包括可信功能、安全标签、事件检测、安全审计跟踪和安全恢复机制。在以上安全机制中，除了业务填充、路由控制和事件检测之外，其余安全机制都与密码算法有关，因此说密码算法是信息安全的核心技术。通常，一种安全机制可以提供多种安全服务，而一种安全服务也可采用多种安全机制。

4. 信息安全攻击的主要形式

当前，对信息系统的攻击是来自多方面的，这些攻击可以宏观地分为人为(或主观因

素)攻击和自然灾害(或客观因素)攻击。它们都会对信息安全构成威胁，但是精心设计的人为攻击的威胁是最大的，也是最难防御的。这里主要介绍人为攻击。

一般而言，人为攻击都是通过寻找系统的弱点，以非授权的方式达到破坏、欺骗和窃取数据信息等目的的。当前，如果采用不同的分类标准(如攻击手段、攻击目标等)，信息安全攻击的形式可以有不同的分类结果。美国国家标准局在2000年9月发布的"信息保障技术框架(IATF)3.0"版本中将攻击形式分为被动攻击、主动攻击、物理临近攻击、内部人员攻击和软硬件配装攻击等5类。

(1) 被动攻击：指未经用户同意和认可的情况下将信息或数据文件泄露给系统攻击者，但不对数据信息进行任何修改。被动攻击通常包括监听未受保护的通信信息，进行流量分析；破解弱加密的数据流，获得认证信息(如密码等)。其中，流量分析的情况比较微妙。例如通过某种手段，如加密屏蔽了信息内容或其他通信量，使得攻击者从截获的信息中无法得到信息的真实内容，但攻击者还能通过观察这些数据包的格式或模式，分析通信双方的位置、通信的次数及信息长度等，而这些信息可能对通信双方来说是非常敏感的，不希望被攻击者得知。这就是所谓的流量分析。

被动攻击常采用搭线监听、无线截获和其他方式的截获(如通过木马、病毒等程序)。被动攻击一般不易被发现，是主动攻击的前期阶段。此外，由于被动攻击不会对被攻击对象做任何修改，留下的痕迹较少或根本没有留下痕迹，因而非常难以检测。抗击被动攻击的重点在于预防，具体措施包括使用VPN(虚拟专用网络)、采用加密技术保护网络及使用加密保护的分布式网络等。

(2) 主动攻击：主要涉及某些数据流的篡改或虚假数据流的产生。主动攻击常分为假冒(或伪造)、重放、篡改信息和拒绝服务四类。

主动攻击的特点与被动攻击恰好相反。被动攻击虽然难以检测，但可以采用有效的防止策略，而要绝对防止主动攻击是十分困难的，因为需要随时随地地对所有的通信设备和通信活动进行物理和逻辑保护。因而主动攻击的主要途径是检测，以及能从此攻击造成的破坏中及时地恢复，同时检测还具有某种威慑效应，在一定程度上也能起到防止攻击的作用。具体措施包括入侵检测、安全审计和完整性恢复等。

(3) 物理临近攻击：指未授权人以更改、收集或拒绝访问为目的而物理接近网络系统或设备。这种接近可以是秘密进入或公开接近，或两种方式同时使用。

(4) 内部人员攻击：可以是恶意的也可以是非恶意的。恶意攻击是指内部人员有计划地窃听或损坏信息或拒绝其他授权用户的访问。据美国FBI的评估显示，80%以上的攻击和入侵都来自组织内部。由于内部人员知道系统的布局、有价值的数据存放在什么地方及何种防御工具在运行，因此这种攻击手段难以防止。非恶意攻击则通常是由于粗心、缺乏技术知识或为了"完成工作"等无意间绕过安全策略但对系统产生了破坏的行为造成的。

(5) 软硬件配装攻击：指在软硬件生产的工厂内或在产品分发过程中恶意修改硬件或软件。这种攻击可能给一个产品引入后门程序等恶意代码，以便日后在未授权的情况下可以访问所需的信息或系统。

当然，在现实生活中一次成功的攻击过程可能会综合若干种攻击手段，通常是采用被动攻击手段来收集信息，制定攻击步骤和策略，然后通过主动攻击来达到目的。此外，人为攻击所造成的危害程度取决于被攻击的对象，与所采用的攻击手段无关。

1.2 信息安全模型

为了更好地分析信息系统的安全问题，找出问题的关键，需要建立一个信息系统安全的基本模型。从网络通信的角度看，网络信息系统可分为通信服务提供者(系统)和通信服务使用者(系统)两个系统。两个系统的侧重点不一样，其安全的基本模型也不一样。

1. 通信服务提供者的信息安全模型

通信服务提供者的目标是安全可靠地跨越网络传输信息。当通信双方欲传递某个消息时，首先需要在网络中确定从发送方到接收方的一个路由，然后在该路由上共同采用通信协议协商建立一个逻辑上的信息通道。实现安全通信主要包括以下两个方面：

(1) 对消息进行安全相关的变换：如对消息进行加密和鉴别。加密的目的是对消息进行重新编码(组合)，以使非授权用户无法读懂消息的内容；鉴别的目的是确保发送者身份的真实性。

(2) 通信双方共享某些秘密信息：这些信息是不希望对手获知的，比如加密密钥。

为了使得消息安全传输，有时还需一个可信的第三方，其作用是负责向通信双方发布秘密信息或者在通信双方有争议时进行仲裁。图 1-1 就是通信服务提供者的信息安全模型。

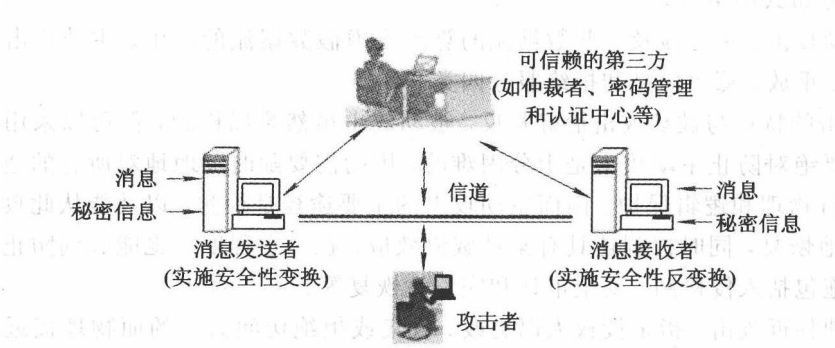

图 1-1　通信服务提供者的信息安全模型图

按照图 1-1 所示，设计一个安全的网络通信必须考虑以下四个方面的内容：

① 选择一个密码算法来执行安全性变换，即通常所说的应用于信道的加密和鉴别的算法，该算法应足够的健壮；

② 生成用于该算法的秘密信息，如密钥等；

③ 研制通信双方之间的秘密信息发布和信息共享的方法；

④ 确定通信双方之间使用的协议，以通过加密算法和秘密信息来获取所需的安全服务。

2. 通信服务使用者的信息安全模型

对于通信服务使用者系统，即传统意义上的信息系统，由于是存放和处理信息的场

所，其安全需求主要是防止未授权访问和保证系统的正常工作。图 1－2 就是通信服务使用者的信息模型。

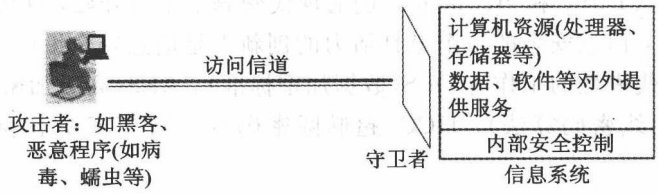

图 1－2　通信服务使用者的信息安全模型

在图 1－2 中，通信服务使用者系统(即信息系统)主要受到两种类型的威胁：

① 非授权地获取或篡改信息数据；

② 寻找系统缺陷，破坏系统以阻止合法用户使用系统提供的资源和服务。

对于这两类威胁，信息系统主要通过两道防线来加强其安全性。第一道防线是“守卫者”，它包括登录程序和屏蔽逻辑程序等访问控制机制，用于拒绝非授权用户的访问、检测和拒绝病毒等恶意程序；第二道防线是由一些内部安全控制部件组成，包括鉴别和认证子系统、审计子系统和授权系统等，主要用于管理系统内部的各项操作和分析所存储的信息，以检查是否有未授权的入侵者。

1.3　密码学在信息安全中的作用

在当前的现实生活中，安全问题随处可见。比如我们的房屋要安装防盗门以阻止盗贼的闯入；汽车安装报警器以阻止盗贼的盗窃行动；电子邮箱设置密码访问功能，以保护用户信息的安全；银行的信用卡设置密码保护功能以保证用户存取现金及交易的安全；电子商务系统中签定商品交易合同，进行电子签名以确保双方事后不能相互抵赖等等。特别是随着网络及应用技术的进一步发展，基于网络系统应用的信息安全问题日益引起人们的关注。诸如电子邮箱密码的安全使用、电子合同签署的安全问题、电子现金的安全存取和信息的安全存储等问题都需要密码技术的支撑。比如通过使用密码技术使信息加密保存，可以阻止非法用户获取你的私密信息；通过使用密码技术对信息进行认证，以确保信息完整；通过使用密码技术对用户身份进行认证和审查，可以确保授权用户的安全使用等等。这些都是密码技术在信息安全领域所起作用的具体体现。

信息安全是一门涉及计算机科学与技术、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。从广义上说，凡是涉及到网络系统中信息的保密性、完整性、可用性、可靠性、可控性和可审查性的相关技术和理论都是信息安全的研究领域。因此，密码学是信息安全的基石，是信息安全的核心技术，也是信息安全的基础性技术。密码技术是实现加密、解密、数据完整性、鉴别交换、密码存储与校验等的基础，借助于密码技术可以实现信息的保密性、完整性和鉴别服务。在保密性服务方面，加密技术将敏感信息(即受保护的信息)变换为敏感性较弱的信息；在完整性或鉴别服务方面，利用密码技术来实现信息的不可伪造。

由此看来，密码技术作为信息安全的基石、核心技术和基础性技术，是保护信息安全最重要的技术之一。当前，信息安全的主流技术和理论都是基于以算法复杂性理论为基础的现代密码技术。从 Diffie 和 Hellman 开创的现代密码学革命开始，现代密码学最近 30 多年的发展历程表明，信息安全的一个最具活力的创新点是信息安全编码理论和方法的深入研究，这方面具有代表性的工作有 DES(数据加密标准)、AES(高级加密标准)、RSA 密码算法、ECC(椭圆曲线密码算法)、HCC(超椭圆密码算法)、IDEA(国际数据加密算法)、PGP 系统等。

在信息时代飞速推进的今天，大量的信息以数字形式存放在信息系统中，信息的传输则是在开放、不安全的公共信道上。而这些信息系统和公共信道在没有设防的情况下是非常脆弱的，很容易受到入侵者的攻击和破坏。如何保护公共网络上信息的安全已成为人们关注的焦点，作为信息安全的核心技术——密码技术也引起了人们的高度重视，吸引着越来越多的科技人员投入到密码学领域的研究中。

值得注意的是，尽管密码学在信息安全领域具有举足轻重的作用，但密码学绝不是信息安全的唯一技术，它也不能解决所有的安全问题。同时，密码编码和密码分析学是一对矛和盾的关系(即所谓“道高一尺，魔高一丈”)，它们在发展中始终处于一种动态平衡状态。确保信息安全的问题，除了技术之外，管理也是非常重要的一个方面。若密码技术使用不当或攻击者绕过了密码技术的使用，密码技术就不能真正提供安全性。

1.4 密码学的基本知识

从前面章节的介绍可以看出，信息安全的若干问题都与密码学紧密相关。密码技术是信息安全的基石、核心技术和基础性技术。本节主要介绍密码学的有关基本知识。

1.4.1 密码学的发展简史

密码学(Cryptography)是一门既古老又年轻的学科，其历史可以追溯到几千年以前。早在四千多年以前，古埃及人就开始使用密码来保密要传递的消息。此外，古代的一些行帮暗语及文字加密游戏等，实际上也是对信息的加密，这种加密通过一定的约定，把需要表达的信息限定在一定范围内流通。一直到第一次世界大战前，密码学的进展很少见诸于世，直到 1918 年，William F. Friedman 的论文“The Index of Coincidence and Its Applications in Cryptography”(重合指数及其在密码学中的应用)发表时，情况才有所好转。在这漫长的时期内，信息的保密基本上靠人工对消息加密和防破译；其应用也主要局限于军事目的，只为少数人掌握和控制。所以，它的发展受到了限制。这就是古典密码学阶段，也是密码学的起源。在这一时期密码学基本上可以说是一门技巧性很强的艺术，而不是一门科学。密码学专家常常也是凭借自己的直觉和信念来进行密码设计和分析，而对密码的分析也大多数是基于密码分析者(即破译者)的直觉和经验。

1949 年，C. E. Shannon(香农)在《贝尔系统技术》杂志上发表了一篇题为“The Communication Theory of Secrecy System(保密系统的通信理论)”的论文，为密码学奠定了坚实的理论基础，使密码学真正成为一门科学。此后，直到 1967 年，由于保密的需要，

人们基本上看不到有关密码学的文献和资料。在1967年，David Kahn(戴维·卡恩)通过收集整理了第一次世界大战和第二次世界大战的大量历史资料，出版了“The Codebreakers”(《破译者》)一书，为密码学公开化、大众化奠定了基础。当时看到本书的人们惊讶到：原来还有密码学。20世纪70年代初期，IBM等公司发表了几篇密码学的报告，从而使更多的人了解了密码学的存在。此后，密码学的文献大量涌现。

1976年，W. E. Diffie和M. E. Hellman发表了“New Direction in Cryptography(密码学新方向)”一文，提出了一种全新的密码设计思想，导致了密码学上的一场革命。他们首次证明了在发送端和接收端不需要传送密钥的保密通信是可能的，从而开创了公钥密码学的新纪元，成为现代密码学的一个里程碑。

1977年，美国国家标准局(National Bureau of Standards，NBS)即现在的国家标准与技术研究所(NIST)正式公布了数据加密标准(Data Encryption Standard，DES)，将DES算法公开，从而揭开了密码学的神秘面纱。从此，密码学的研究进入了一个崭新的时代。随后，DES被美国许多部门和机构采纳为标准，并成为事实上的国际标准。由于安全的原因，DES于1998年正式退役。

1978年，R. L. Rivest，A. Shamir和L. Adleman实现了RSA公钥密码学，此后成为了公钥密码学中杰出的代表。

1984年，Bennett. Charles H，Brassard. Gille首次提出了量子密码学(现称为BB84协议)。量子密码学与以前的密码学不同，它是一种基于量子定律的密码学，可以发现窃听等攻击行为，还可以抗击具有无限计算能力的攻击。因此，很多人认为，在量子计算机诞生之后，量子密码学有可能会成为唯一真正安全的密码学。

1985年，N. Koblitz和V. Miller把椭圆曲线理论运用到公钥密码学中，成为公钥密码学研究的新亮点。

与此同时，密码学的另一个重要方向——序列密码(也称为流密码，主要用于政府、军方等国家要害部门)理论也取得了重大的进展。1989年，R. Mathews，D. Wheeler，L. M. Pecora和Carroll等人首次把混沌理论使用到序列密码及保密通信理论中，为序列密码的研究开辟了一条新的途径。

1997年，美国国家标准与技术研究所NIST开始征集新一代数据加密标准来接任即将退役的DES。2000年10月，由比利时密码学家Joan Daemen和Vincent Rijmen发明的Rijndael密码算法成为新一代数据加密标准——AES(Advanced Encryption Standard)算法。2001年11月26日，NIST正式公布高级加密标准，并于2002年5月26日正式生效。

2000年1月，欧盟正式启动了欧洲数据加密、数字签名、数据完整性计划NESSIE，旨在提出一套强壮的包括分组密码、序列密码、散列函数、消息认证码(MAC)、数字签名和公钥加密密码标准。

当前，现代密码学的发展已经深入到信息时代的各个环节，其相应的技术也大量涌现，主要有数据加密、密码分析、信息鉴别、零知识证明、秘密分享等。另外，值得一提的是近年发展迅猛的信息隐藏技术，它是将需要保密的信息隐藏在公开信息中来保密、传输的技术，所以有人也称其为秘密的信息嵌入技术。