高等院校信息技术规划教材

密码学及安全应用

唐四薪　李浪　谢海波　编著

清华大学出版社

高等院校信息技术规划教材

密码学及安全应用

唐四薪　李浪　谢海波　编著

清华大学出版社
北京

内 容 简 介

本书按照概述、原理和应用的知识结构，全面介绍密码学的基本原理、算法和最新的应用，对密码学的原理和应用做了详细、通俗且符合认知逻辑的阐述。本书分为11章，内容包括信息安全概述、密码学基础、数字签名、密钥管理与密钥分配、认证技术、数字证书和PKI、电子商务安全协议、电子支付的安全、移动电子商务的安全、物联网的安全和信息安全管理。

本书可作为高等院校计算机科学与技术、电子商务、信息安全、信息系统与信息管理等专业本科生的教材，也可供从事密码学教学、科研和管理工作的相关人员参考。

图书在版编目(CIP)数据

密码学及安全应用/唐四薪，李浪，谢海波编著. --北京：清华大学出版社，2016
高等院校信息技术规划教材
ISBN 978-7-302-42330-0

Ⅰ. ①密…　Ⅱ. ①唐…　②李…　③谢…　Ⅲ. ①密码－高等学校－教材　Ⅳ. ①TN918.1

中国版本图书馆CIP数据核字(2015)第287093号

责任编辑：张　民　战晓雷
封面设计：傅瑞学
责任校对：时翠兰
责任印制：杨　艳

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 装 者：北京鑫海金澳胶印有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：21　　**字　　数**：484千字
版　　次：2016年4月第1版　　**印　　次**：2016年4月第1次印刷
印　　数：1～2000
定　　价：45.00元

产品编号：065132-01

前言 foreword

密码学原本是一门古老的学科，在过去很多年里和人们的生产生活关系也不大。但随着 Internet 和电子商务的出现和普及，密码学正逐渐走入人们生活的方方面面，为人们的信息安全起着保驾护航的作用。

从宏观上来看，密码学对电子商务的发展起到了毋庸置疑的促进作用，因此，密码技术的进步间接地促进了我国经济的发展，同时，密码学还被广泛应用到电子政务、物联网等各个领域，带来了巨大的社会效益和经济效益。

为了培养掌握密码学原理及技术的专门人才，很多高等院校的计算机科学与技术、信息安全、网络工程、信息管理等专业都开设有密码学方面的课程，但密码学原理只有与具体的应用技术结合才能产生实用价值。作者在多年的教学实践中发现，密码学教学在讲授基本原理的同时，还应侧重于讲授密码学在电子商务、物联网等领域的应用，以提高学生的实际应用能力和学习这门课程的兴趣。

同时，学习密码学的不同应用还能使学生了解密码学的发展趋势，例如，由于计算和存储能力的差别，密码学在电子商务安全和物联网安全中的应用是显著不同的，在电子商务安全中，公钥密码算法被大量使用，以实现身份认证、签名等需求，而在物联网安全协议中，即使是身份认证，也一般采用对称密码和散列函数来实现，特别是轻量级分组加密算法。因此，密码算法具有向重量级和轻量级两头发展的趋势。

本书在编写过程中力求体现以下特色：

(1) 新颖性。本书介绍了一些具有代表性且具有很强应用前景的技术。如散列链、前向安全数字签名、盲签名、电子现金、量子密码等，以及典型密码技术的应用，包括电子商务安全协议、电子支付安全、物联网安全等领域。

(2) 全面性。密码学的用途早已不再局限于加密和解密方面，还包括数字签名、身份认证、数字证书和 PKI 等应用。本书对密码学的各种用途作了全面的介绍。

(3) 实用性。本书对密码学原理的介绍力求做到详细、通俗且符合认知逻辑，在讲述有关密码学基本理论之前，介绍了相关的数论知识，并在每个知识点后都给出了例题，以方便教师授课和学生自学。

本书的知识结构可分为概述、原理、应用三大块，内容如下：第1章为概述，第2～6章为密码学的基本内容，第7～10章为密码学的各种具体应用，第11章为安全管理的内容。

本书的理论教学课时以54课时为宜。对于目录中带*号的部分，可以根据需要选择性讲解。本书注重教材立体化建设，每章后都提供了具有丰富题型的习题，并为教师提供如下配套资料：PPT课件、习题答案、考试试卷、教学大纲等，可登录清华大学出版社网站免费下载，也可和作者联系(tangsix@163.com)。

本书由唐四薪、李浪、谢海波编著，唐四薪编写了第3～9章和第10章的部分内容，李浪编写了第1、2章，谢海波编写了第11章的内容。参加编写的还有唐琼、肖望喜、喻缘、邹飞、谭晓兰、何青、刘艳波、戴小新、尹军、刘燕群、陆彩琴、唐金娟等，他们编写了第10章的部分内容。衡阳师范学院李浪教授对本书进行了审定。

本书的写作得到了国家自然科学基金资助项目(61572174)的资助，并得到了湖南省教育厅科学研究课题(15C0204、15A029、15C0202)的资助。

本书在编写过程中参考了大量专家学者的图书和论文资料，作者已尽可能地在参考文献中列出，谨在此向有关作者表示感谢，若有疏漏，也在此表示歉意。由于本人水平和教学经验有限，加之书中部分内容比较前沿，书中错误和不当之处在所难免，敬请广大读者和同行批评指正。

作　者

目录 Contents

第1章 chapter 1

信息安全

由于Internet的广泛普及与使用，其应用已深入渗透到商业、金融、政府、文教等诸多领域。Internet信息和服务在给合法用户带来方便的同时，也让非法用户变得有机可乘。

密码学是一门古老的学科，大概自人类社会产生战争便产生了密码。在古代，由于密码技术长期仅用于军事、政治和外交等领域的保密通信，因此与人们的日常生活没有多大关系。但是，随着计算机网络越来越深入地应用到人们的生活和工作中，出现了诸如电子商务、电子政务、网络金融、证券交易这些对信息安全要求很高的网络应用，使得密码学受到人们的广泛关注。

一般来说，信息安全保障需要依赖各种安全机制来实现，而许多安全机制则依赖于密码技术。使用密码技术不仅可以保障信息的机密性，而且还可以保护信息的完整性和真实性，防止信息被篡改、伪造和假冒。因此，密码学是信息安全的技术基础，其应用贯穿于网络信息安全的整个过程，在解决信息的机密性保护、完整性保护、可鉴别性和信息抗抵赖性等方面发挥着重要的作用，并已渗透到信息系统安全工程的各个领域和大部分安全机制的实现中。

1.1 信息安全概况

“安全”一词并没有统一的定义，对安全的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。

信息作为一种资源由于其普遍性、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。信息安全的实质就是要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。

信息安全是指信息系统(包括硬件、软件、数据、人、物理环境及其基础设施)受到保护，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，系统能够连续、可靠、正常地运行，信息服务不被中断，最终实现业务连续性。信息安全主要包括以下5方面的内容，即需保证信息的保密性、真实性、完整性、可用性和所寄生系统的安全性。

信息安全可分为狭义安全与广义安全两个层次，狭义的安全是建立在以密码学为基础的计算机安全技术领域；广义的信息安全是一门综合性学科，安全不再是单纯的技术

问题，而是将管理、技术、法律等问题相结合的产物。

1.1.1 信息安全对电子商务发展的影响

信息安全的重要性在电子商务发展中体现得最为明显。电子商务已经逐渐成为人们进行商务活动的新模式，作为一种新的经济形式正改变着社会生活的方方面面，也为人们带来了无限商机。但安全问题一直成为电子商务发展的制约因素，这表现在：一些个人和商业机构对是否采用电子商务仍持观望态度，因为他们担心自己的银行卡是否会被盗用，或担心自己的客户信息会被窃取。

据中国互联网络信息中心(CNNIC)2015 年 7 月发布的《第 36 次中国互联网络发展状况统计报告》显示，中国网民规模已达 6.68 亿，网购用户规模达到了 3.73 亿，这意味着有近三分之一的中国人在进行网络购物。从这个意义上讲，电子商务与人们的生活已越来越密切，并已经渗透到各行各业。电子商务作为一种新的经济形势已经成为不争的事实，这使得越来越多的企业开始重视电子商务的作用，搭建自己的电子商务网站和交易平台。

报告还指出，2011 年上半年有 85.7%的网民在网上查询过商品信息，但只有 29%的网民实现了网上购物。这表明，网上购物的人群占网民总人数的比例还处于较低的水平，目前大多数网民对电子商务还是持观望或不信任的态度。

许多网民不愿意网上购物固然与他们的购物习惯和上网熟练程度有关，但对于安全问题的担心也是一个不可忽视的重要因素。而且对于那些参与电子商务交易的网民来说，其购物也多是集中在书籍、服饰、数码产品等价值较低的领域。这表明我国电子商务发展的广度和深度均未达到其应有的水平，而解决安全问题是将电子商务向纵深推进的必要条件。

相对于传统商务，电子商务对管理水平、信息传输技术等都提出了更高的要求，其中安全体系的构建尤为重要，电子商务迫切需要有效的安全保障机制和措施。总的来看，在运用电子商务模式进行交易的过程中，信息安全问题成为了电子商务最核心的问题，也是电子商务得以顺利推行的保障。信息安全的重要性表现在以下两方面。

1. 安全问题是实施电子商务的关键因素

人类传统的交易是面对面进行的，可以当面识别对方身份，当面清点钱物，因而比较容易保障交易双方的信任关系和交易过程的安全性。而电子商务活动中的交易行为是通过网络进行的，买卖双方互不见面，因而缺乏传统交易中的信任感和安全感。

根据 CNNIC 发布的《中国互联网络发展状况统计报告》，在电子商务方面，52.26%的用户最关心的是交易的安全可靠性。由此可见，电子商务中的网络安全和交易安全问题是实现电子商务的关键之所在。

Internet 所具有的开放性是电子商务方便快捷、被广泛接受的基础，而开放性本身又会使网上交易面临种种危险。比如，在开放的网络上处理交易，如何保证传输数据的安全成为电子商务能否普及的最重要的因素之一。

2. 信息安全涉及国家经济安全

从宏观上看，电子商务在我国各行各业逐步普及，应用不断深入，电子商务安全对国家安全的影响也在不断加深，这主要表现在两个方面：一是危及经济安全。随着电子商务活动的普及，越来越多的资金流在网络中流动，极大地诱惑着不法分子犯罪。以网络为基础构建的银行、证券等金融系统成为现代社会运行的核心，一旦这些系统遭受攻击或者破坏出现故障，便直接危及国家经济安全。例如，采用网络攻击手段进行商业欺诈和勒索，窃取、篡改和盗用信息，销售假货等类型的网络经济犯罪活动正急剧增加，这会对我国经济发展和金融秩序造成严重危害。二是影响社会稳定。银行、保险、税务、证券、民航、医疗等行业都开始实施电子商务，这些领域一旦出现比较严重的信息安全问题，则有可能会严重影响人民的生活，进而影响社会稳定。例如，铁道部的购票网站由于访问速度缓慢而饱受人们诟病，一度使春节购票成为广大人民群众关注的焦点问题。因此，安全建设工作必须贯穿电子商务建设的整个过程。

根据调查显示，目前电子商务安全主要存在的问题包括计算机网络安全、商品的品质、商家的诚信、货款的支付、商品的递送、买卖纠纷的处理、网站售后服务7个方面。这7个方面的问题可以归结为两大部分：计算机网络安全和电子交易安全。

*1.1.2 威胁网络信息安全的案例

针对网络信息安全的威胁主要有利用网络进行盗窃、诈骗，利用Internet虚假宣传欺骗消费者，窃取企业或政府部门的机密，侵犯消费者的个人隐私等。

1. 利用网络进行盗窃

在电子商务交易中，人们需要网上银行和第三方支付平台进行网上支付。目前，对网上银行或支付平台账户的保护措施一般是设置密码或安装数字证书等手段，但这些保护措施常会由于人们的疏忽或犯罪分子精心设计的圈套而被破解，使得账户里的资金被盗。目前，网络盗窃犯罪主要有两种方式：

(1) 利用网络向受害人电脑植入木马，通过各种方式引诱用户访问含有木马的网站或安装木马程序，以便盗取账号、密码，再盗窃账户资金。2006—2009年间，长沙人李某将“网银大盗”和“灰鸽子”两种木马病毒放在租用的服务器上，通过这两种木马窃取受感染网民的网银存款，他用这种手段先后窃取受害者银行资金40余万元。

(2) 利用钓鱼网站诱骗用户输入账号、密码信息，从而盗取资金。“网络钓鱼”是指犯罪分子通过伪造的假网站或网页等手法，盗取用户的银行账号、证券账号、密码信息和其他个人资料，然后以转账、网上购物或制作假卡等方式获取利益。2008年8月域名为www.taobaof.net的网站从域名到网页布局都模仿淘宝网，骗取用户的网上银行账号、密码，从而盗取用户银行资金。

2. 利用网络进行诈骗

网络诈骗犯罪本质就是伪造身份，骗取对方信任。目前，网络诈骗的主要手段有

两种：

(1) 在购物网站上发布各类虚假信息，实施诈骗。这类诈骗活动又分为两种。

一种是商家欺骗客户。如商家在交易平台上开设商铺，发布超低价商品信息，哄骗客户将货款直接转账到其银行账户下(即不通过支付平台支付的场外交易)，商家收到货款后，不发货或者发一些明显与质量不符的货物。

另一种是客户欺骗商家，比如向商户购买商品，通过聊天工具给商户发送伪造的支付凭证，诱使商户银讫发货，类似这样的案子有很多。

(2) 在互联网上开设虚假网站行骗。

犯罪分子开设虚假网站，发布虚假供货信息或高额回报的集资信息，得手后，往往"网间蒸发"，人去网空，这类诈骗案件的犯罪分子利用在互联网上开设网站手续简便、快捷和隐蔽的特点，有恃无恐。

如 2007 年，一个自称"美国科技基金网"的网站打着专门从事高收益投资项目的幌子，鼓励投资者投入 8800 元人民币，就可在网上获取 ID 号，从第二天每天返利 440 元人民币，一共返利 50 天。如果发展了"下线"还可获得下线投资额的 10%作为奖励。该网站最初几个星期还可以兑现返利，但 3 个月后突然消失，在这期间，受害者达 1400 余人，被骗金额 880 多万元。

3. 侵犯消费者的隐私

消费者的个人隐私包括消费者的电话号码、银行账号、购物记录、姓名、住址、身份证号码等。不法分子可以通过在网上发布在线调查、抽奖、注册或者免费赠送礼品等活动要求用户输入个人资料，以窃取消费者的身份证号、银行卡密码等敏感信息。另一种方法是通过攻破一些大型的网站，再获取这些网站数据库中保存的用户资料信息。不法分子窃取到消费者的隐私信息后，可能利用这些信息向消费者发送垃圾信息，根据隐私信息破解用户的账号、密码，甚至以将隐私信息公开相威胁，向用户或网站敲诈勒索。

4. 窃取企业或政府部门的机密

企业的商业机密是指不为公众知悉，能为权利人带来经济利益，具有实用性并已被权利人采取保密措施的技术或经营信息。一些企业为了经营管理方便，将一些商业机密信息存储于计算机系统中。黑客通过网络攻击侵入这些计算机系统，获得商业机密信息的行为时有发生，黑客可以将获取到的机密信息出售，或者向企业进行敲诈等。

5. 对信息系统的单纯性攻击行为

单纯性攻击行为可造成信息系统无法访问，或访问速度很慢。例如，2010 年初，黑客攻破解析百度域名的域名服务器，替换了百度的域名解析记录，使用户无法访问百度网站。此次攻击持续时间长达数小时，造成的损失无法估量。

能造成"阻断用户访问"效果的攻击手段，除了"域名劫持"之外，更普遍的手段是分布式拒绝服务攻击(DDoS)。黑客利用木马程序控制成千上万台计算机，同时向攻击目

标发起连接请求，这些请求在瞬间超过了服务器能够处理的极限，导致其他用户无法访问这些网站。如2007年，知名网站鞭牛士遭受DDoS攻击，该攻击持续16个小时，造成网站不能被正常访问。

1.1.3 网络信息安全的组成

网络安全从其本质上来说就是网络上的信息安全。信息系统是通过计算机和网络实现的，需要利用Internet的各种基础设施和标准，因此构成信息安全系统结构的底层是计算机网络服务层。网络服务层是各种网络应用系统的基础，它能提供信息传输功能、用户接入方式和安全通信服务，并保证网络运行安全。

所谓网络信息安全是指保障承载信息系统的计算机设备、系统软件平台和网络环境能够无故障运行，并且不受外部入侵和破坏。

一般来说，网络信息安全主要包括系统实体安全、系统运行安全和系统软件安全，如图1.1所示。其特点是针对计算机网络本身可能存在的安全问题，实施强大的网络安全监控方案，以保证计算机网络自身的安全性。

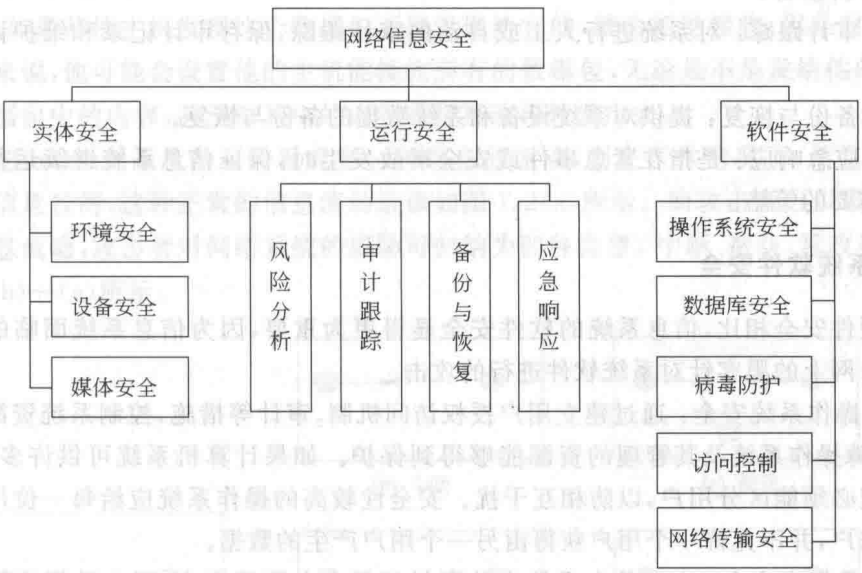

图1.1 网络信息安全的组成要素

1. 系统实体安全

所谓系统实体安全(又称物理安全)，是指保护计算机设备、设施(含网络)以及其他媒体免遭自然灾害、人为破坏和环境威胁的措施或过程。实体安全是整个信息系统安全的前提，它是由环境安全、设备安全和媒体安全3部分组成。

(1) 环境安全：是指保护信息系统免受水、火、有害气体、地震、雷击、高温、潮湿和静电等灾害的危害。这要求在建设机房和架设线路时全面考虑有可能对系统造成破坏的各种因素，并设计可行的防范措施。