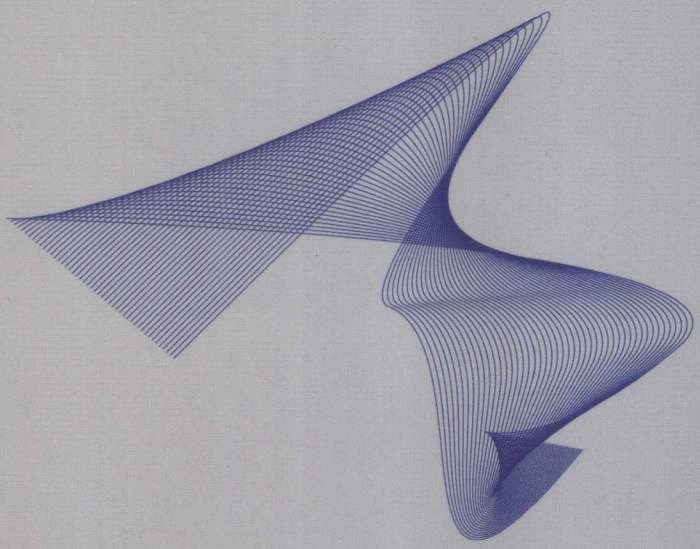
普通高等教育“十一五”国家级规划教材

“信息化与信息社会”系列丛书之
高等学校信息安全专业系列教材

密码学
——密码算法与协议



郑 东 李祥学 黄 征 编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY http://www.phei.com.cn

普通高等教育“十一五”国家级规划教材

“信息化与信息社会”系列丛书之

高等学校信息安全专业系列教材

密码学——密码算法与协议

郑　东　李祥学　黄　征　编著

電子工業出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 简 介

在过去的三十余年里，现代密码学的研究获得了突飞猛进的发展，是当今通信与计算机界的热门课题。本书主要介绍密码学的基本原理与设计方法，其中包括对称密码算法与非对称密码算法、数字签名算法及哈希函数的设计原理、密钥管理体制设计方法、高级数字签名协议设计模型等，最后给出了一些密码技术在网络应用中的实际例子。

本书既可作为高等学校计算机、通信及信息安全专业高年级本科生的教材，也可作为电子信息与通信和信息管理等专业研究生的教材，同时还可以作为相关工程技术人员学习密码学知识的入门读物。

图书在版编目（CIP）数据

密码学：密码算法与协议 / 郑东，李祥学，黄征编著. —北京：电子工业出版社，2009.6

（信息化与信息社会系列丛书. 高等学校信息安全专业系列教材）

普通高等教育“十一五”国家级规划教材

ISBN 978-7-121-08704-2

I. 密… II. ①郑… ②李… ③黄… 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 063548 号

策划编辑：刘宪兰

责任编辑：张 京

印 刷：北京智力达印刷有限公司

装 订：北京中新伟业印刷有限公司

出版发行：电子工业出版社

北京市海淀区万寿路 173 信箱 邮编 100036

开 本：787×1092 1/16 印张：13.75 字数：352 千字

印 次：2009 年 6 月第 1 次印刷

印 数：4000 册 定价：26.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

总　序

信息化是世界经济和社会发展的必然趋势。近年来，在党中央、国务院的高度重视和正确领导下，我国信息化建设取得了积极进展，信息技术对提升工业技术水平、创新产业形态、推动经济社会发展发挥了重要作用。信息技术已成为经济增长的“倍增器”、发展方式的“转换器”、产业升级的“助推器”。

作为国家信息化领导小组的决策咨询机构，国家信息化专家咨询委员会一直在按照党中央、国务院领导同志的要求就信息化前瞻性、全局性和战略性的问题进行调查研究，提出政策建议和咨询意见。在做这些工作的过程中，我们愈发认识到，信息技术和信息化所具有的知识密集的特点，决定了人力资本将成为国家在信息时代的核心竞争力，大量培养符合中国信息化发展需要的人才已成为国家信息化发展的一个紧迫需求，成为我国应对当前严峻经济形势，推动经济发展方式转变，提高在信息时代参与国际竞争比较优势的关键。2006 年 5 月，我国《2006—2010 年国家信息化发展战略》公布，提出“提高国民信息技术应用能力，造就信息化人才队伍”是国家信息化推进的重点任务之一，并要求构建以学校教育为基础的信息化人才培养体系。

为了促进上述目标的实现，国家信息化专家咨询委员会一直致力于通过讲座、论坛、出版物等各种方式推动信息化知识的宣传、教育和培训工作。2007 年，国家信息化专家咨询委员会联合教育部、原国务院信息化工作办公室成立了“信息化与信息社会”系列丛书编委会，共同推动“信息化与信息社会”系列丛书的组织编写工作。编写该系列丛书的目的，是力图结合我国信息化发展的实际和需求，针对国家信息化人才教育和培养工作，有效梳理信息化的基本概念和知识体系，通过高校教师、信息化专家、学者与政府官员之间的相互交流和借鉴，充实我国信息化实践中的成功案例，进一步完善我国信息化教学的框架体系，提高我国信息化图书的理论和实践水平。毫无疑问，从国家信息化长远发展的角度来看，这是一项带有全局性、前瞻性和基础性的工作，是贯彻落实国家信息化发展战略的一个重要举措，对于推动国家的信息化人才教育和培养工作，加强我国信息化人才队伍的建设具有重要意义。

考虑当前国家信息化人才培养的需求、各个专业和不同教育层次（博士生、硕士生、本科生）的需要，以及教材开发的难度和编写进度时间等问题，“信息化与信息社会”系列丛书编委会采取了集中全国优秀学者和教师、分期分批出版高质量的信息化教育丛书

的方式，根据当前高校专业课程设置情况，先开发“信息管理与信息系统”、“电子商务”、“信息安全”三个本科专业高等学校系列教材，随后再根据我国信息化和高等学校相关专业发展的情况陆续开发其他专业和类别的图书。

对于新编的三套系列教材（以下简称系列教材），我们寄予了很大希望，也提出了基本要求，包括信息化的基本概念一定要准确、清晰，既要符合中国国情，又要与国际接轨；教材内容既要符合本科生课程设置的要求，又要紧跟技术发展的前沿，及时地把新技术、新趋势、新成果反映在教材中；教材还必须体现理论与实践的结合，要注意选取具有中国特色的成功案例和信息技术产品的应用实例，突出案例教学，力求生动活泼，达到帮助学生学以致用的目的，等等。

为力争出版一批精品教材，“信息化与信息社会”系列丛书编委会采用了多种手段和措施保证系列教材的质量。首先，在确定每本教材的第一作者的过程中引入了竞争机制，通过广泛征集、自我推荐和网上公示等形式，吸收优秀教师、企业人才和知名专家参与写作；其次，将国家信息化专家咨询委员会有关专家纳入到各个专业编委会中，通过召开研讨会和广泛征求意见等多种方式，吸纳国家信息化一线专家、工作者的意见和建议；再次，要求各专业编委会对教材大纲、内容等进行严格的审核，并对每一本教材配有一至两位审稿专家。

如今，我们很高兴地看到，在教育部和原国务院信息化工作办公室的支持下，通过许多高校教师、专家学者及电子工业出版社的辛勤努力和付出，“信息化与信息社会”系列丛书中的三套系列教材即将陆续和读者见面。

我们衷心期望，系列教材的出版和使用能对我国信息化相应专业领域的教育发展和教学水平的提高有所裨益，对推动我国信息化的人才培养有所贡献。同时，我们也借系列教材开始陆续出版的机会，向所有为系列教材的组织、构思、写作、审核、编辑、出版等做出贡献的专家学者、老师和工作人员表达我们最真诚的谢意！

应该看到，组织高校教师、专家学者、政府官员以及出版部门共同合作，编写尚处于发展动态之中的新兴学科的高等学校教材，还是一个初步的尝试。其中，固然有许多的经验可以总结，也难免会出现这样那样的缺点和问题。我们衷心地希望使用系列教材的教师和学生能够不吝赐教，帮助我们不断地提高系列教材的质量。

曲作枝

2008 年 12 月 15 日

序　言

人类走过了农业社会、工业社会，如今正处于信息社会的伟大时代，“信息社会”这个词语无疑已经家喻户晓，信息化的大潮正席卷着世界的每一个角落。地球两端，万里之隔，人们能通过互联网与亲朋畅快交流，音容笑貌犹如就在眼前，真正是天涯变咫尺；分支机构遍布全球的庞大企业运转有条不紊，各机构协作顺畅，其功能强大的信息系统功勋卓著；分析复杂神秘的生物基因，预测瞬息万变的天气趋势，有了容量惊人的数据库系统和“聪明绝顶”的高性能计算系统，科学家们如虎添翼。总之，人类处处受益于信息化成果并正在信息化这条大道上加速前进，决不会放慢脚步。

然而，阳光之下总会有阴影，人类越依赖于信息系统，信息安全问题就越发凸显。关于信息安全的形形色色的新闻日益频繁地见诸于媒体：某银行数据库数据被窃取导致客户信息泄露，使客户惶惶不安，银行面临信任危机；某计算机病毒大肆泛滥，无数用户系统瘫痪，让相关企业损失惨重；某国军方网络被黑客侵入，军事机密竟被人如探囊取物般轻易窃取……这样的事件一再提示我们，信息安全问题是社会信息化发展进程中无法回避的客观产物，只有主动积极地面对和解决这一问题才能保障信息化的顺利推进，确保经济、社会的稳定乃至国家的安全。

目前，世界各国政府在信息安全领域的重视程度正在不断加大，并纷纷推出了本国的相关标准、规范或法律，大力扶持高校和其他科研机构对信息安全问题的研究，同时采取各种措施促进信息安全领域的人才培养以满足本国信息化建设的需要，为本国的信息产业发展提供中坚力量。特别是一些信息化进程起步较早，水平较高的发达国家，其信息安全领域的研究水平和产业化程度已相当令人瞩目。

我国正处于信息化建设的关键阶段，2006 年发布的《2006—2010 年国家信息化发展战略》更是从战略的高度指出了推进信息化对我国经济建设和国家发展的重要作用，规划出了新时期我国信息化发展的宏伟蓝图。由此可见，我国的信息化建设和信息产业正面临前所未有的机遇和挑战。

正是在这样的时代背景下，信息安全问题越来越引起全社会上下的广泛关注。信息安全领域必须不断提高研究水平以满足经济建设和国家安全的需要，为我国信息化建设的大踏步前进保驾护航，为创建和谐社会，实现可持续发展贡献力量。因此，大量高素质的信息安全人才成为了最急需、最宝贵的资源。

康有为曾经说过："欲任天下之事，开中国之新世界，莫亟于教育"。我们的国家要想不断发展科技，增强国力，开创出我们自己富强文明的"新世界"，必须加大力度进行信息化建设。而要使我国的信息化水平走在世界前列，全面提高信息安全领域教育水平，特别是促进高等学校信息安全专业对相关人才的培养和教育，就成为了成败的关键。高等学校信息安全系列教材的编撰就是希望能够为我国的信息安全领域专业人才的培养、为我国信息化水平的腾飞助一臂之力。

信息安全专业教育有其自身的特点，要求学习该专业的学生能够将系统知识与专业知识有机结合，在注重提升理论高度的同时还要能够把理论知识与工程实践紧密联系起来。本系列教材针对高等学校信息安全专业教育的这些特点，同时根据其知识体系、教育层次和课程设置，规划了教材的内容，增加了实际案例，力争做到既紧跟前沿技术的发展，又不失扎实的基本理论和生动活泼的形式，使学生能够学以致用。本系列教材从不同角度论述和总结了信息安全领域的科学问题，有着较强的适用性，既可作为高等学校信息安全专业和相关专业本科生的教材，也可以作为非信息安全专业的公共教科书，同时还可以作为从事信息安全工作的科研技术人员和管理人员的培训教材或参考书，使其了解信息安全相关关键技术和发展态势。

信息安全科学在不断发展，我们也将会努力使本系列教材适应和紧跟这种发展的节奏，使我们培养的信息安全人才能够与时俱进，用自己的所学共筑我国信息安全的万里长城。

限于作者的水平，本系列教材难免存在不足之处，敬请读者批评指正。

高等学校信息安全专业系列教材编委会

2008 年 10 月

前　言

计算机和网络的广泛应用给人们的工作与生活带来了极大便利，但同时也衍生了许多需要解决的问题，信息安全问题就是其中之一。信息安全研究在有敌方参与的网络信息系统环境下，如何确保信息的保密性（Confidentiality）、完整性（Integrity）、可用性（Availability）、可控性（Controllability）等，它是跨计算机、通信、控制、数学等不同领域，集理论、技术和工程于一体的交叉学科。密码技术是保证信息安全性的关键手段。

现代密码学形成于20世纪70年代。这一时期出现了两个在密码学史上具有里程碑意义的事件，即公用数据加密标准DES的制定和批准、公钥密码体制的诞生。通过近四十年的发展，对现代密码学的研究突飞猛进，其研究领域更加广泛和深入。在人才培养方面，国内各高校都加强了信息安全专业本科和研究生的培养力度，开设了相关的信息安全专业，进行了详细的课程设计。随之而来的是与密码学相关的书籍充斥在市面上，参差不齐。大多数密码学教学用书内容陈旧、过于简单，无法向学生提供更多的深入学习的引导，不能紧跟密码学的最新研究进展，往往不能满足其知晓最新密码技术及其应用的需求。事实上，我们需要一本涵盖最新研究进展并有一定深度的教材，使只想“知其然”的学生能够在较短的时间里对密码学的主要内容有一个基本了解，同时为那些希望以密码学及信息安全为自己未来的研究方向、想“知其所以然”的学生提供一条进一步深入学习的快速通道。

本书作者均在上海交通大学从事密码学的研究和教学达十余年，为本科生和研究生主讲“密码理论与实践”、“密码协议”、“计算机安全学”等专业课程。作者注意到了现代社会对信息安全人员需求的持续增长和现有专业人员明显短缺这一失调现象、了解学生对掌握密码学理论与技术的浓厚兴趣，本书正是基于作者的研究、教学经验并参阅相关文献编写而成的。

本书是普通高等教育“十一五”国家级规划教材，按照密码算法、密码协议、密码应用编排章节顺序，教学中也可根据需要对密码协议和密码应用部分的内容进行必要的调整。由于密码协议和密码应用种类众多，无法在一本教材中详细论述，作者只介绍了部分协议和应用。本书可作为计算机、信息安全专业高年级本科生教材，也可作为电子信息与通信和信息管理等专业的研究生教材，还可作为相关工程技术人员学习密码学知识的入门读物。

全书共分 10 章，内容包括：密码学引论、序列密码、分组密码、公钥密码、认证和哈希函数、数字签名、密钥管理技术、身份识别、高级签名、密码应用。第 1、4、6、10 章由郑东执笔，第 2、8、9 章由李祥学执笔，第 3、5、7 章由黄征执笔。本书的出版受国家自然科学基金 60703031、60803146 和中国高科技研究发展计划 2008AA01Z403 资助。本书在选题策划和撰写过程中得到了电子工业出版社刘宪兰编辑的鼓励和支持，她为本书的出版付出了辛勤的劳动，在此谨表示诚挚的感谢。

限于我们的水平和经验不足，教材中的错误和缺憾在所难免，诚恳地希望读者在使用本教材时，对发现的错误和问题能够及时指出。我们欢迎任何对于本书的批评和建设性意见，以便我们以后对本书进行修改时参考。作者 E-mail:dzheng@ sjtu.edu.cn。

编著者

2009 年 2 月

于上海交通大学信息安全工程学院

目　录