<<现代密码学教程>>

图书基本信息

书名：<<现代密码学教程>>

13位ISBN编号：9787563520190

10位ISBN编号：7563520198

出版时间：2009-8

出版时间：北京邮电大学出版社

作者：谷利泽，郑世慧，杨义先　编著

页数：368

前言

发展21世纪中国信息安全要靠教育，而搞好信息安全教育就需要好的教材。
2004年，灵创团队北京邮电大学信息安全中心完成了第一套信息安全专业本科系列教材，该套教材被教育部列入了“普通高等教育‘十五’国家级规划教材”。
至今，三年多的时间过去了，这套教材在信息安全专业的教学中发挥了重要的作用，起到了较好的教学效果，受到教师和学生的好评。

在这三年中，我们始终致力于包括专业建设、课程建设、师资建设、教材建设、实训基地建设、实验室建设和校企就业（创业）平台建设等在内的信息安全本科专业的全面建设。
2005年，作为组长单位我们完成了教育部“信息安全专业规范研究”和“信息安全学科专业发展战略研究”课题；召开了“全国高校本科‘信息安全专业规范与发展战略研究’成果发布与研讨会”。
我们完成的国内第一次制定的信息安全专业规范，从知识领域、知识单元和知识点三个层次构建学科专业教学的知识体系；由通识教育内容、专业教育内容和综合教育内容三大部分，构建课程参考体系；采用顶层设计的方法构建了带有实践性环节的教学体系。
我们在国内第一次较全面地提出信息安全学科专业教学改革与创新的研究以及发展思路和政策建议；这些成果已提交教育部相关教学指导委员会，对于引导高等学校信息安全学科专业教学改革与建设，指导信息安全学科专业评估，促进信息安全学科专业教学规范建设与管理，提高专业教育质量和水平起到了重要的作用。
多所举办信息安全专业的高校都参照该课题成果调整了自己的教学计划、课程体系和实验方案。

我们积极搭建信息安全专业校际交流平台，组织成立了“全国信息安全本科教材编写委员会”和“全国信息安全本科专业师资交流与培训互助组”。
主持召开了“全国信息安全专业教学经验交流和师资培训研讨会”和“全国信息安全专业实验室建设和实验课程教学经验交流研讨会”。
在四川绵阳建设了占地40亩的全国信息安全专业本科生实习实训基地，接受了来自全国近30所高校的本科生进入该基地参加丰富多彩的实训。

我们努力建设精品课程，主办了“全国高校信息安全专业精品课程建设经验交流会议”，来自全国各地高校的专家齐聚北京邮电大学，介绍了精品课程建设的经验。
我们组织建设了全国第一批信息安全实验室，并且编写出版了实验教材《信息安全实验指导》，我们的《现代密码学》课程已经被评为北京市精品课程，并在2007年度被评为“国家精品课程”。

<<现代密码学教程>>

内容概要

本书是一本关于现代密码学的基础教材。
全书共分11章和1个附录（参考文献），主要分成4部分。
第1部分（第1～3章）主要介绍现代密码学的基础知识，包括密码学的基本概念、基本体制、基本思想以及所用到的理论知识等。
第2部分（第4～7章）主要介绍现代密码学的基本技术，包括对称密码技术（分组密码、序列密码）、Hash函数、公钥密码技术等。
第3部分（第8～10章）主要介绍现代密码学的基本应用，包括数字签名技术、密钥管理、密码协议等。
第4部分（第11章）对现代密码学的今后发展进行了展望。
本书重点突出、抓住核心；通俗易懂、容易入门；例证丰富、快速理解；习题多样、牢固掌握。
本书是信息安全专业的专业基础课教材，适合作为高等院校信息科学专业或其他相关专业本科生和研究生的教材，也可作为相关领域的教师、科研人员以及工程技术人员的参考书。

<<现代密码学教程>>

书籍目录

章节摘录

第1章　密码学概论　　密码学（Cryptology）是结合数学、计算机科学、电子与通信等诸多学科于一体的交叉学科，是研究信息系统安全保密的一门科学，它分为密码编码学和密码分析学两类。本章首先介绍密码学与信息安全的关系，然后简述密码学发展史，最后介绍密码学中的一些基本知识。

1.1　信息安全与密码学　　因特网的飞速发展和普及应用加速了信息社会的节奏与步伐，信息作为一种无形的资源，已经成为促进经济增长和社会进步的重要力量。

现在，信息系统已被广泛地应用于政治、军事、经济和科研等诸多领域，并逐渐成为一种很重要的工具和手段。

但事物都具有两重性，当我们尽情享受信息社会带来的诸多便利和高效的同时，也需要防范它带来的负面影响。

信息网络的社会性、开放性和共享性等特点使其蒙上了不安全因素的阴影。

由于信息的存储、传递、处理等过程往往是在开放的通信网络中进行的，使信息容易受到窃听、截取、篡改、伪造、假冒、重放等多种攻击手段的威胁。

如果信息安全问题不解决，信息社会就不能稳步有序地发展，电子商务、电子政务、网络银行等应用都将无法开展起来。

因此，信息安全已经成为信息社会亟须解决的最重要问题之一。

信息安全是一门综合的学科，它涉及信息论、计算机科学和密码学等多方面知识，其主要任务是研究计算机系统和通信网络中信息的保护方法，以及实现系统内信息的机密性、完整性、可用性、不可否认性和认证性等，其中密码学正是实现这些功能的核心技术。

……

<<现代密码学教程>>

版权说明