<<密码学引论>>

图书基本信息

书名：<<密码学引论>>

13位ISBN编号：9787307067042

10位ISBN编号：7307067048

出版时间：2009-3

出版时间：武汉大学出版社

作者：张焕国，王张宜 著

页数：284

前言

二十一世纪是信息的时代，信息成为一种重要的战略资源。
信息科学成为最活跃的学科领域之一，信息技术改变着人们的生活和工作方式，信息产业成为世界第一大产业。
信息的安全保障能力成为一个国家综合国力的重要组成部分。
当前，以Internet为代表的计算机网络的迅速发展和“电子政务”、“电子商务”等信息系统的广泛应用，正引起社会和经济的深刻变革，为网络安全和信息安全开拓了新的服务空间。
世界主要工业化国家中每年因利用计算机犯罪所造成的经济损失远远超过普通经济犯罪。
内外不法分子互相勾结侵害计算机系统，已成为危害计算机信息安全的普遍性、多发性事件。
计算机病毒已对计算机系统的安全构成极大的威胁。
社会的信息化导致新的军事革命，信息战、网络战成为新的作战形式。
总之，随着计算机在军事、政治、金融、商业等部门的广泛应用，社会对计算机的依赖越来越大，如果计算机系统的安全受到破坏将导致社会的混乱并造成巨大损失。
因此，确保计算机系统的安全已成为世人关注的社会问题和计算机科学的热点研究课题。
信息安全事关国家安全，事关经济发展，必须采取措施确保我国的信息安全。
发展信息安全技术与产业，人才是关键。
培养信息安全领域的专业人才，成为当务之急。
2001年经教育部批准，武汉大学创建了全国第一个信息安全本科专业。
2003年经国务院学位办批准武汉大学建立信息安全博士点。
现在，全国设立信息安全本科专业的高等院校已增加到70多所，设立信息安全博士点的高等院校和科研院所也增加了很多。
2007年“教育部高等学校信息安全类专业教学指导委员会”正式成立，并在武汉大学成功地召开了“第一届中国信息安全学科建设与人才培养研讨会”。
我国信息安全学科建设与人才培养进入蓬勃发展阶段。

<<密码学引论>>

内容概要

《密码学引论（第2版）》以信息安全专业指导性专业规范中对密码学知识和实践能力的要求为依据，从理论与实际相结合的角度介绍密码学的基本理论、基本技术和实际应用。
全书共分为九章。
第一章，概论。
第二章，密码学的基本概念。
第三章，分组密码。
第四章，序列密码。
第五章，公开密钥密码。
第六章，数字签名。
第七章，HASH函数。
第八章，认证。
第九章，密钥管理。

《密码学引论（第2版）》与第一版相比，主要进行了以下调整和改写：其一是修正了一版书中已发现的一些错误；其二是增加了一些新内容，以反映密码学的新发展；其三是为了方便教学使用，对一部分内容的叙述方法进行了调整和改写，增加了密码算法的实现示例和习题。

《密码学引论（第2版）》是普通高等教育“十一五”国家级规划教材，适合用作信息安全专业和其他相关专业的本科生教材，也可用作信息安全和其他相关领域研究生和工程技术人员的技术参考书。

<<密码学引论>>

书籍目录

<<密码学引论>>

章节摘录

第1章 概论　　随着计算机和网络在军事、政治、金融、工业、商业等部门的广泛应用，社会对计算机和网络的依赖越来越大，如果计算机和网络系统的信息安全受到破坏将导致社会的混乱并造成巨大损失。
因此，确保计算机和网络系统的信息安全已成为世人关注的社会问题和计算机科学与技术领域的研究热点。
当前，以Internet为代表的计算机网络的迅速发展和广泛应用，正引起社会和经济的深刻变革，极大地改变着人们的生活和工作方式。
Internet已经成为我们生活和工作中的一个不可缺少的组成部分。
基于计算机网络的“电子政务”、“电子商务”和“电子金融”等应用正在兴起，它们的兴起在政务、商务和金融领域引起了一场革命。
对此，发展我国的电子政务、电子商务和电子金融已成为建设具有中国特色社会主义强国的不可回避的选择。
然而，目前影响电子政务、电子商务、电子金融应用的主要技术障碍是信息安全问题。
由于Internet原来缺少安全设计，再加上Internet的开放性和无政府状态，使Internet成为一个不安全的网络。
这就使得Internet不能适应电子政务、电子商务和电子金融等系统对信息安全的要求。
世界主要工业国家中每年因利用计算机犯罪所造成的经济损失令人吃惊，据美国FBI的调查报告，美国每年因利用计算机犯罪所造成的经济损失就高达1700多亿美元，远远超过普通经济犯罪所造成的经济损失。
据美国的一项调查报告，有40%的被调查者承认在他们的机构中曾发生过利用计算机犯罪的事件。
在我国利用计算机犯罪的案例也在迅速上升。
例如，最近几年我国的网络银行屡屡发生金融欺诈事件。

<<密码学引论>>

编辑推荐

为了增进信息安全领域的学术交流、为信息安全专业的大学生提供一套适用的教材，2003年武汉大学组织编写了一套《信息安全技术与教材系列丛书》。
这套丛书涵盖了信息安全的主要专业领域，既可用做本科生的教材，又可作为工程技术人员的技术参考书。
这套丛书出版后得到了广泛的应用，深受广大读者的厚爱，为传播信息安全知识发挥了重要作用。
现在，为了能够反映信息安全技术的新进展、更加适合信息安全教学的使用和符合信息安全类专业指导性专业规范的要求，武汉大学对原有丛书进行了升版。

版权说明