<<密码学与通信安全基础>>

图书基本信息

书名：<<密码学与通信安全基础>>

13位ISBN编号：9787560945682

10位ISBN编号：7560945686

出版时间：2008-11

出版时间：华中科技大学出版社

作者：祝跃飞，王磊　编著

页数：152

前言

鉴于安全机制和通信系统早已紧密结合甚至融合，通信专业的硕士研究生学习必要的密码理论和技术已经成为现实的需要。
本书正是专门针对这一需要而编写的。
当前，密码学的内容非常丰富，通信专业的研究生应该掌握哪些基本的密码理论和技术是编写本书首先需要考虑的问题。
基于通信专业研究生学习密码学的目的和一般所具备的知识基础考虑，我们在下述思想指导下进行了内容的选取和体系设计。
第一，通信专业研究生学习密码学的主要目的是理解和掌握基本的密码技术，进而理解其在通信系统中应用的基本思想和方法。
因此，本书的重点在于应用密码学和掌握典型密码算法，而未包括难度较大的密码安全性理论和密码分析方面的内容。
第二，考虑到读者学习过大学工科数学和信息论与编码课程，书中就不再涉及相关的数学原理。由于目前国内信息安全数学基础课程已经成熟，因此教材中没有包含相关数学基础的详细内容，仅在附录中给出主要的概念和结论。
另外，考虑到一般通信专业学生没有系统学习计算复杂性理论，在附录中简要介绍了相关的基本知识供读者参考。
第三，读者学习密码学的最终目的是在理解和掌握现有的核心密码技术及其应用的基础上，深入理解密码学的思想和应用方法，从而能够较好地适应密码学和通信安全技术快速发展的需要，因此本书建立了一个密码学的体系结构，重点揭示了密码设计思想及密码应用模式和方法。
第四，在密码应用方面，选取因特网应用作为重点介绍，既取决于目前通信现实，更利于深入系统地理解密码技术的应用思想，同时介绍各种无线通信网的安全体系，从而使读者较为全面地了解目前密码学在通信中的应用。
在这些内容的介绍中，采用了先阐述原理再展开对细节做必要介绍的模式，而不是以技术手册的方式进行全面细节介绍，这样更符合教材的特点。
第五，为了适应读者不同层次学习的需求，本书分为4个层次。
第1个层次为1－4章，其内容为应用密码学基础，其中，第1章概要介绍密码学学科体系，第2－4章分别介绍加密体制、认证系统和基本密码协议。
第2个层次包括第5－9章，内容为应用密码学，较为系统地介绍了密码技术在因特网中的综合应用，同时简单介绍了各种无线通信网和密码相关的安全机制。
第3个层次包括第10－12章，内容为密码算法，重点介绍各种典型算法的细节和数学原理，供需要深入了解算法进而实现算法的读者学习。
最后1个层次是第13章，介绍了密码学的其他典型内容，供读者全面地了解密码学。
前2个层次为基本内容，而后2个层次为深入学习的内容。
这种分层次的体系结构非常便于读者由浅入深的学习。
由于本书定位于通信安全的密码学基础，对密码学的介绍还是比较基本的，如果需要进一步深入学习，请参考有关的专业书籍（如参考文献[2]、[5]等）。
感谢国家自然科学基金项目和国家“863”项目的支持。
作者　　2008年2月

<<密码学与通信安全基础>>

内容概要

本书主要面向通信专业的硕士研究生，是基于这类读者的一般知识基础和学习密码学的目的而专门设计编写的。

本书内容按照4个层次编写：第1层次为应用密码学基础，在概要中介绍密码学学科体系，介绍各种基本密码技术；第2层次为应用密码学，较为系统地介绍密码技术在因特网中的应用，同时简单地介绍密码技术在各种无线通信网中的应用；第3层次为密码算法，重点介绍各种典型算法及其数学原理；第4层次简单介绍现代密码学的一些其他问题。

另外，在附录中简要给出必要的数学基础和计算复杂性的理论基础知识。

本书的分层体系便于读者由浅人深逐步学习密码学，因内容不包括层次较深的密码安全理论和密码分析内容，故可供以应用为主而非研究为目的学习密码学的读者作为参考书籍。

<<密码学与通信安全基础>>

书籍目录

章节摘录

历史上，密码在军事、外交上的许多重大事件中起过重要甚至决定性的作用，事例不胜枚举。

第二次世界大战的历史更是集中体现了密码的意义：“月光之夜”的故事可谓密码价值的经典事例。

德国制订了代号为“月光之夜”的行动计划，计划夜间毁灭性地空袭英国工业重镇考文垂，英国通过破译德军密码及时获悉了这一计划，但如果采取措施来减轻对其重要工业基地的损失，将暴露已破译德军密码，进而导致德军很快更换密码，为了通过已破译密码获得更有价值的情报，英国首相丘吉尔艰难地选择了牺牲考文垂。

中途岛海战是太平洋战场的转折点，美国胜利的根本原因在于及时破译了日本偷袭中途岛的情报，从而设伏使日本海军遭到致命的打击。

由于行动计划被完全破译，日本战争核心人物山本五十六大将在视察途中被美国空军拦截击落座机而亡。

有专家估计，盟军密码专家的破译工作，至少使第二次世界大战缩短了8年。

由于密码的特殊作用，世界大多数国家的军政部门始终都有庞大的、秘密的密码研究机构。

当今，世界范围内的政治、军事、外交、经济等斗争更加尖锐与复杂，特别是社会信息化导致了国家安全战略的变化，各国都在不断加强对密码学研究。

编辑推荐

本书主要讲述应用密码学基础、应用密码学、密码算法、现代密码学的一些其他问题。本书可供各类以密码学应用为主而非研究为目的的学习的读者作为参考书籍。

<<密码学与通信安全基础>>

版权说明