<<现代密码学原理与实践>>

图书基本信息

书名：<<现代密码学原理与实践>>

13位ISBN编号：9787560621302

10位ISBN编号：7560621309

出版时间：2009-1

出版时间：西安电子科技大学出版社

作者：于工　等编著

页数：223

字数：339000

前言

21世纪是一个高度信息化的时代，信息安全问题引起了全世界的密切关注。
为适应人才培养的需求，很多理工类大学都开设了信息安全及密码学方面的课程，因而广大学生和教师迫切需要一本密码学方面的简明教程，以满足教学的需要。

现代密码学涉及的知识面较宽，包括信息理论、通信技术、检错纠错编码、计算机网络等，它用到许多数学知识，如数论、群论等。
没有系统学习过这些数学理论的人往往会望而生畏，就此止步。
实际上，作为初学者，只需要对有关数学知识有一些初步了解，就能理解现代密码学的大多数基本观点和基本算法，能够从中受到新思想的启迪。
在本书中，作者从不同角度对相关课题作了精辟的论述，这对于教师、科研人员及研究生的学习起到了积极的作用。

本书定位于本科生教材（也可作为相关专业研究生教材），计划课时48学时左右。
书中内容覆盖面比较广，且篇幅适中，论述浅显易懂，不苛求数学理论的严密性，偏重编码方法与应用，适合于初学者学习；概念和思路的讲述力求准确清晰，语言力求简练清楚，以达到教师好教、学生好用的目的。
为了帮助初学者入门，书中将密码理论中所必需的初等数论与有限域的相关知识精练而通俗地集中于附录A，供缺乏这方面基础的读者预先学习，为后续学习扫清障碍。
为了加深学生对内容的理解，每章都安排有与理论教学相应的实践练习，通过程序设计与计算机演练，使学生能够理论联系实际，更好地掌握所学知识。
另外，每章后均有习题，以便课后练习。

<<现代密码学原理与实践>>

内容概要

《现代密码学原理与实践》全面、系统地论述了现代密码学的基本原理与方法，强调现代密码学在保密与认证两方面的功能，特别是在通信与网络安全中的重要作用。
全书共七章，包括传统密码、序列密码、分组密码、公钥密码、签名与认证、密钥管理和密码协议、密码学在网络安全中的应用等内容。
作为本科教材，《现代密码学原理与实践》理论深度适中，强调概念和思路，偏重编码方法与应用，书中所列的程序可使学生加深对知识的理解。
另外，实验的程序代码与习题答案均在附录中提供，以方便教学与自学。

<<现代密码学原理与实践>>

书籍目录

章节摘录

1.1　基本概念1.1.1　密码与密码学密码是为解决信息安全而进行的编码。
安全指通信系统抗御外来攻击的能力。
外来攻击主要有两大类：一类是以截获或窃听通信内容为目标的被动攻击，攻击者截获他人信息、窃取密码、打探隐私、偷盗机密、危害民众；另一类是以篡改或伪造信息为手段的主动攻击，攻击者冒充合法发信人，发布信息，安置黑客，散布病毒，甚至破坏通信系统。
针对被动攻击，密码可以使所传输信息具有保密功能，窃听者即使截获了一些信息，也会因不懂密文而不知所云。
针对主动进攻，密码应具备“认证”功能，对发信人身份、消息来源以及消息完整性等加以认证，使非法发信人不得进入系统，使虚假消息能被识别，使篡改行为得以被发现。
保密和认证是密码的两大基本功能。
为了军事、政治、司法等方面的需求，有时也需要破译对方的密码或者赚取对方的认证，由此便出现了与“密码编码学”原理相同但目的相反的另一分支，叫做“密码分析学”。
这种保密与破译的斗争如同矛与盾的关系一样，魔高一尺，道高一丈，相依相存，相克相长，促进了二者共同的发展。
近年来曾多次听到某种保密系统悬赏破译，某个防火墙产品欢迎投诉，其目的就是通过不断发现问题与解决问题，增强自己的抗攻击性能。
为了设计出更加安全可靠的密码系统，设计者不仅要研究出更新更强的密码技术，还要研究对手有哪些可能的攻击手段。
设计以分解大数复杂性为基础的RSA密码体制时，必定要讨论分解大数的技巧；设计以离散对数复杂性为基础的密码体制时，难免要讨论离散对数的计算方法，因此，聪明的密码设计者同时也应该是高明的密码分析者，二者统一于同一个目标。
“密码学”则是“密码编码学”与“密码分析学”的总称。

<<现代密码学原理与实践>>

编辑推荐

《现代密码学原理与实践》可作为高等院校信息工程、通信工程、计算机科学与技术以及电气工程与自动化等专业“信息安全”类课程的教材，也可供相关专业科技工作人员参考。

<<现代密码学原理与实践>>

版权说明