<<现代密码学>>

图书基本信息

书名：<<现代密码学>>

13位ISBN编号：9787560622347

10位ISBN编号：7560622348

出版时间：2009-2

出版时间：西安电子科技大学出版社

作者：杨晓元 编

页数：219

<<现代密码学>>

前言

自20世纪Shannon发表“保密系统的信息理论”以来，密码学一直是一个活跃的研究领域。随着计算技术与网络的发展，现代密码学被广泛地应用于军事、政治、外交和商业等领域。

本书主要讲述现代密码学的基础理论及一些重要的研究内容，要求读者有一定的数学基础，包括近世代数、数论和概率论等知识。

全书共分8章。

第一章讲述计算复杂性理论的基本内容，使读者对算法的复杂性、问题的难度、P与NP的区别以及多项式归约的思想有一定的认识。

第二章介绍Shannon保密理论的主要内容，并简要介绍Simmons认证理论。

第一章和　　第二章为后面各章的学习奠定基础。

第三章讲述密码函数及其性质，从频谱理论的角度出发，研究密码函数的相关免疫性、扩散特性、非线性性、雪崩效应、稳定性、差分特性等性能。

第四章讲述序列密码，包括序列密码的基础理论、密钥序列的产生方法、序列密码的安全性及应用等内容。

第五章讲述分组密码，除了介绍数据加密标准I）ES和高级加密标准AES这两种加密体制之外，还重点讨论了差分分析和线性分析的基本思想及方法，对于其它一些攻击分组密码的手段，如截段差分分析、高阶差分分析及非线性攻击等也作了简要介绍。

第六章讲述近年来公钥密码研究中的热点问题，包括椭圆曲线及超椭圆曲线密码体制以及基于身份的公钥体制等。

第七章较全面地介绍了数字签名的思想及方法，包括几种经典的数字签名算法和体制以及国内外在签密方面的最新研究成果。

第八章讨论多方密码协议，包括秘密共享与门限密码体制、零知识证明协议和安全多方计算等。

本书是在多年教学实践和研究的基础上形成的，编写者一直从事密码学和信息安全方面的研究，并多次讲授过研究生的现代密码学课程。

<<现代密码学>>

内容概要

《现代密码学》内容涉及现代密码学的基础理论和重要协议，包括计算复杂性理论、信息论基础、密码函数、序列密码变换理论、分组密码及其安全性、公钥密码体制、数字签名与签密和多方密码协议。

《现代密码学》可供高等院校密码学和信息安全等专业的研究生和高年级本科生使用，也可供信息安全领域的技术人员参考。

<<现代密码学>>

书籍目录

章节摘录

第一章　计算复杂性理论　　计算复杂性理论的核心内容是NP完全性理论，而NP完全问题是否难解是当代数学和计算机科学中尚未解决的最重要的问题之一。
众所周知，公钥密码的理论基石是NP完全问题的难解性，如果对NP完全问题能找到有效解法，则绝大多数公钥密码体制将面临着被攻破的威胁。
本章主要介绍计算复杂性理论中最基本的内容，使读者对算法的复杂性、问题的难度、P与NP的区别以及多项式归约的思想有一定的认识，从而更深入地理解密码体制的安全性，为后面的学习打下良好的基础。
1.1　计算复杂性理论概述　　计算复杂性理论是理论计算机科学中有关可计算理论的分支，它使用数学方法对计算中所需的各种资源的耗费作定量的分析，并研究各类问题之间在计算复杂程度上的相互关系和基本性质，是算法分析的理论基础。
为了计算一类问题，总要耗费一定的时间和存储空间等资源。
资源的耗费量是问题大小的函数，称为问题对该资源需求的复杂度。
计算复杂性理论主要研究和分析复杂度函数随问题大小而增长的阶，探讨它们对于不同的计算模型在一定意义下的无关性；根据复杂度的阶对被计算的问题分类；研究各种不同资源耗费之间的关系；估计一些基本问题的资源耗费情况的上、下界，等等。
计算复杂性理论中常常用到计算模型、问题、算法、时间复杂性等概念，下面一一介绍。
……

<<现代密码学>>

编辑推荐

《现代密码学》是在多年教学实践和研究的基础上形成的，编写者一直从事密码学和信息安全方面的研究，并多次讲授过研究生的现代密码学课程。

版权说明