<<现代密码学理论与实践>>

图书基本信息

书名：<<现代密码学理论与实践>>

13位ISBN编号：9787505398160

10位ISBN编号：7505398164

出版时间：2004-5

出版时间：电子工业

作者：[英]WenboMao著

页数：706

字数：1180000

<<现代密码学理论与实践>>

内容概要

第Ⅰ部分是密码学与信息安全的入门性介绍。
第Ⅱ部分介绍学习本书必备的数学背景知识，也可作为学习现代密码学理论基础的系统背景知识。
第Ⅲ部分介绍提供保密和数据完整性保护最基本的密码算法和技术。
第Ⅳ部分介绍应用密码学和信息安全中一个重要的概念——认证。
第Ⅴ部分对公钥密码技术（加密、签名和签密）的强（实用）安全性概念进行严格的形式化处理，并给出认证协议的形式化分析方法。
第Ⅵ部分包括两个技术章节和一个简短的评述。

本书适合大学本科生、在高科技公司从事信息安全系统设计和开发的安全工程师、企业信息安全系统管理人员或者生产安全产品的软/硬件开发商以及刚开始从事密码学或计算机安全方面研究的博士生等使用。

作者简介

Wenbo Mao：计算机科学博士。
在英国Manchester大学做博士后研究期间，与C.Boyd博士对密码协议和协议形式的分析进行了深入研究并做出贡献。
后加入HP公司做高级技术成员，在英国的Bristol研究实验室的可信赖系统实验室，参加了多项重要的电子商务系统和信息安全系统的设计

<<现代密码学理论与实践>>

书籍目录

A SHORT DESCRIPTION OF THE BOOKPREFACELIST OF FIGURESLIST OF ALGORITHMS,PROTOCOLS AND ATTACKS I INTRODUCTION 1 BEGINNING WITH A SIMPLE COMMUNICATION GAME 2 WRESTLING BETWEEN SAFEGUARD AND ATTACK II MATHEMATICAL FOUNDATIONS STANDARD NOTATION 3 PROBABILITY AND INFORMATION THEORY 4 COMPUTATIONAL COMPLEXITY 5 ALGEBRAIC FOUNDATIONS 6 NUMBER THEORYIII BASIC CRYPTOGRAPHIC TECHNIQUES 7 ENCRYPTION—SYMMETRIC TECHNIQUES 8 ENCRYPTION--ASYMMETRIC TECHNOQUES 9 IN AN IDEAL WORLD:BIT SECURITY OF THE BASIC PUBLIC-KEY CRYPTOGRAPHIC FUNCTIONS 10 DATA INTEGRITY TECHNOQUESIV AUTHENTICATION 11 AUTHENTICATION PROTOCOLS—PRINCIPLES 12 AUTHENTICATION PROTOCOLS——THE REAL WORLD 13 AUTHENTICATION FRAMEWORK FOR PUBLIC-KEY CRYPTOGRAPHY V FORMAL APPROACHES TO SECURITY ESTABLISHMENT 14 FORMAL AND STRONG SECURITY DEFINITIONS FOR PUBLIC-KEY CRYPTOSYSTEMS 15 PROVABLY SECURE AND EFFICIENT PUBLIC-KEY CRYPTOSYSTEMS 16 STRONG AND PROVABLE SECURITY FOR DIGITAL SIGNATURES 17 FORMAL METHODS FOR AUTHENTICATION PROTOCOLS ANALYSISVI CRYPTOGRAPHIC PROTOCOLS 18 ZERO-KNOWLEDGE PROTOCOLS 19 RETURNING TO "COIN FLIPPING OVER TELEPHONE" 20 AFTERREMARK

<<现代密码学理论与实践>>

版权说明