

<<公钥密码学>>

图书基本信息

书名：<<公钥密码学>>

13位ISBN编号：9787118017779

10位ISBN编号：7118017779

出版时间：1998-1

出版时间：国防工业出版社

作者：Arto Salomaa

页数：281

字数：237000

译者：丁存生

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<公钥密码学>>

内容概要

众所周知，在今天的信息安全领域，特别是在保密通信、数字签名、指令认证和密钥管理中，公钥密码学是必不可少的。

本书正是欧洲科学院院士，计算机界、数学界和密码学界著名的学者Arto Salomaa教授关于公钥密码学的一本系统而有创新的专著。

内容包括：经典双向密码学，公钥思想，背包系统，RSA系统，密码系统的其他基础，密码方案：通信中的惊人应用。

本书既可作为国防及民用信息安全、密码技术人员的参考读物，又可作为培养高级密码技术人才的教科书。

<<公钥密码学>>

书籍目录

第一章 经典双向密码学 1.1 密码体制与密码分析 1.2 单表系统 1.3 多表和其他系统 1.4 Rotors 和 DES
第二章 公钥思想 2.1 某些街道是单向的 2.2 如何认识这一思想 2.3 公钥的明显优点
第三章 背包系统 3.1 建立陷门 3.2 如何找到陷门 3.3 可达性理论 3.4 设法再次隐藏陷门 3.5 高密度背包
第四章 RSA 系统 4.1 合法世界 4.2 攻击和防卫 4.3 素性 4.4 密码分析和因子分解 4.5 RSA 的部分信息 4.6 离散对数和密钥交换
第五章 密码系统的其他基础 5.1 二次域中的乘幂 5.2 同态的迭代 5.3 自动机与语言理论 5.4 编码理论
第六章 密码方案：通信中的惊人应用 6.1 不仅仅是行为规范 6.2 电话掷硬币：修订的扑克 6.3 如何共享秘密 6.4 秘密的部分泄露 6.5 盲传送 6.6 银行业和秘密投票中的应用 6.7 使人相信证明而无需细节 6.8 零知识证明 6.9 身份的零知识证明
附录A 复杂度理论讲座
附录B 数论讲座习题历史和文献
注记
名词索引
参考文献

<<公钥密码学>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>