

<<现代密码学原理与应用>>

图书基本信息

书名：<<现代密码学原理与应用>>

13位ISBN编号：9787111372851

10位ISBN编号：7111372859

出版时间：2012-4

出版时间：机械工业出版社

作者：宋秀丽

页数：296

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>

<<现代密码学原理与应用>>

内容概要

《现代密码学原理与应用(普通高等院校信息安全专业规划教材)》(作者宋秀丽)全面介绍了现代密码学的基本概念、理论及应用,在体系构架和内容编排上以提高读者的密码实际应用能力为目标,简化或忽略了部分密码学的数学基础理论分析,增加了密码学的应用技术和发展。

全书共12

章,内容包括信息安全与密码学、古典密码体制、流密码、分组密码体制、公钥密码体制、Hash函数与数字签名、密钥管理、认证理论及应用、密码技术综合应用、现代密码学发展前沿及应用、密码学相关数学知识,以及上机实验。

《现代密码学原理与应用(普通高等院校信息安全专业规划教材)》可作为高等院校信息安全、计算机科学、通信工程、应用数学、信息管理、电子商务等相关专业的教材。

也可作为信息处理、通信保密、计算机应用等领域科研人员和工程技术人员的自学参考书。

<<现代密码学原理与应用>>

书籍目录

前言

第1章 信息安全与密码学

1.1 信息安全

1.1.1 信息安全的概念

1.1.2 信息安全的基本属性

1.1.3 信息安全面临的威胁

1.1.4 信息安全基本模型

1.2 密码学理论与发展

1.2.1 密码体制及分类

1.2.2 密码攻击类型

1.2.3 密码学的发展历程

1.2.4 密码学在信息安全中的重要地位

1.3 小结

1.4 习题

第2章 古典密码体制

第3章 流密码

第4章 分组密码体制

第5章 公钥密码体制

第6章 Hash函数与数字签名

第7章 密钥管理

第8章 认证理论及应用

第9章 密码技术综合应用

第10章 现代密码学发展前沿及应用

第11章 密码学相关数学知识

第12章 上机实验

参考文献

<<现代密码学原理与应用>>

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>