第一图书网, tushu007.com

<<密码学导引>>

图书基本信息

书名：<<密码学导引>>

13位ISBN编号：9787030072955

10位ISBN编号：7030072952

出版时间：2001-10-01

出版时间：科学出版社

作者：冯登国,裴定一

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

第一图书网, tushu007.com

内容概要

全书包括十一章和一个附录，系统地介绍了现代密码学的基本理论和技术，主要内容包括密码学的基本概念、倍息理论基础、复杂性理论基础，流密码，分组密码的设计原则、工作模式和一些有代表性的分组密码算法及攻击分组密码的一些典型方法，公钥密码算法，各种数字签名方案和各种签名的应用环境，Hash函数的分类、攻击方法和一些有代表性的Hash算法，时戳技术，大量的身份识别协议和基于身份的密码方案，一些赛钥管理技术，电

第一图书网, tushu007.com

书籍目录

前言
第1章引论
1.1密码滨基本概念
1.2古典密码学
1.2.1古典密码体制
1.2.2古典密码体制分析
1.3注记和文献
第2章密码学的信息理论基础
2.1Shannon的保密系统的信息理论
2.1.1保密系统的数学模型
2.1.2熵及其基本性质
2.1.3完善保密性
2.1.4伪密钥和唯一解距离
2.2Simmons的认证系统的信息理论
2.2.1认证系统的数学

第一图书网, tushu007.com

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