<<应用密码学>>

图书基本信息

书名：<<应用密码学>>

13位ISBN编号：9787563510658

10位ISBN编号：7563510656

出版时间：2005-6

出版时间：北京邮电大学出版社

作者：杨义先/钮心忻编

页数：288

<<应用密码学>>

内容概要

信息安全的核心是密码，而应用密码学则是信息安全应用领域所有人员必须了解的基础知识。
作为相关专业的研究生教材，本书对密码学基础、数据加密标准（DES）、高级数据加密标准（AES）、典型分组加密算法、RSA密码的软硬件实现、高速加密卡、序列密码乱源、序列密码设计、序列密码强度评估等加密知识和数字签名基础、代理签名、PKI、WPKI系统口令认证、身份认证、访问控制、密钥管理等认证知识以及电子支付概论、电子支票系统、公平的电子支付、VPN、IPSec协议等应用知识进入了深入而系统地描述，并通过多个实用系统全面剖析了相关的密码应用。
本研究生教材内容全面，既有密码学的基本理论，又有应用密码的关键技术，还有当前热门的实用案例介绍。
全书图文并茂，文字流畅，表述严谨，包含了应用密码方面的许多国际最新进展和发展趋势。
本书的初衷虽然是通信、计算机、信息安全、密码学等相关专业的研究生教材，但是，本书也可以广泛适用于从事信息处理、通信保密、计算机等领域的科研人员和工程技术人员等。

<<应用密码学>>

书籍目录

<<应用密码学>>

版权说明