<<应用编码与计算机密码学>>

图书基本信息

书名：<<应用编码与计算机密码学>>

13位ISBN编号：9787302112181

10位ISBN编号：7302112185

出版时间：2005-11

出版时间：清华大学

作者：龙冬阳

页数：284

字数：427000

<<应用编码与计算机密码学>>

内容概要

本书从编码理论与信息论的角度系统地阐述了计算机密码学研究的核心内容，首先介绍了变长编码理论的若干基本概念，讨论信息熵、信源编码和数据压缩方法等问题，然后详细描述了传统的古典密码体制、迭代码全制、数据加密标准DES、高级加密标准AES、公钥密码体制、Hash函数、数字签字、密钥管理及安全协议等内容，最后简单介绍了量子密码学的基本概念。

为了便于选用本书作为教材或教学参考书的读者进行自学，随同本书提供了相关的素材文件，读者可以通过访问http://www.tupwk.com.cn/downpage或http://infosec.sysu.edu.cn下载。其中包括了我们教学过程中许多本科生或研究生所做的课程设计内容，如用Visual C++或Java等语言工具实现的DES，AES，RSA，MD5，SHA1等典型密码算法等。

本书可用作计算机科学与工程、信息系统管理、数字与通信等相关专业本科生或低年级研究生计算机密码学课程的教材或教学参考书，同时也可供从事信息处理、计算机网络与信息安全等专业的工程技术人员参考使用。

<<应用编码与计算机密码学>>

书籍目录

<<应用编码与计算机密码学>>

版权说明