<<现代密码学>>

图书基本信息

书名：<<现代密码学>>

13位ISBN编号：9787030106070

10位ISBN编号：7030106075

出版时间：2002-7-1

出版时间：科学出版社

作者：沈世镒,陈鲁生

页数：156

字数：197000

<<现代密码学>>

内容概要

本书系统地介绍现代密码学的基本内容，取材具有典型性，全书共分9章，第1章介绍密码学中的一些基本概念，第2章介绍古典密码的加密方法和一些典型的古典密码体制，第3章介绍Shannon的密码学理论，第4章和第5章分别讨论分组密码和公钥密码，第6章介绍序列密码和线性移位寄存器序列。第7章和第8章分别讨论数字签名和Hash函数，第9章介绍一些重要的密码协议，本书每章末均附有习题，其中有些习题是对正文内容的补充，以供学生复习巩固书中所学内容。

本书可作为高等院校信息科学专业或其他相关专业本科生的教材。也可作为相关领域中的教学、科研人员以及工程技术人员的参考书。

<<现代密码学>>

书籍目录

版权说明