<<现代密码学>>

图书基本信息

书名：<<现代密码学>>

13位ISBN编号：9787302146094

10位ISBN编号：7302146098

出版时间：2007-4

出版时间：清华大学出版社

作者：杨波

页数：212

<<现代密码学>>

内容概要

本书全面而详细地介绍现代密码学的理论和相关算法。
可帮助读者将所学知识应用于信息安全的实践中。
全书共分8章，第1章引言介绍现代密码学的基本概念，其余各章包括流密码、分组密码体制、公钥密码、密钥分配与密钥管理、消息认证和杂凑算法、数字签字和密码协议、网络加密与认证。
本书从教材使用的角度考虑，概念清晰、结构合理、通俗易懂、内容深入浅出，并充分考虑方便教师在教学过程中的实施，同时还注意与其他专业课教学的衔接。
本书取材新颖，不仅介绍现代密码学所涉及的基础理论和实用算法，同时也涵盖了现代密码学的最新研究成果，力求使读者通过本书的学习而了解本学科最新的发展方向。
本书可作为高等学校有关专业大学生和研究生的教材，也可作为通信工程师和计算机网络工程师的参考读物。

<<现代密码学>>

书籍目录

版权说明