信息安全与密码学

信息安全与密码学_下载链接1_

著者:徐茂智

出版者:清华大学

出版时间:2007-1

装帧:

isbn:9787302139584

本书介绍信息安全与密码学的基础理论与基本应用。信息安全的核心是密码学，所以密码学也是本书的重点。全书由绪论、信息安全初步、信息安全技术、传统密码学、公钥密码算法、Hash函数、计算复杂性理论、零知识证明与比特承诺、基于身份的公钥密码学、数字签名、密钥管理和密码学中的基本数学知识(附录)组成，共11章及一个附录。所涉及的内容基本上涵盖了现代密码学的基本概念、基本算法．以及信息安全的基本知识。附录是刘数论基本知识，以及群、环、域等一些基本代数概念的简单介绍。本书每章均配有习题，便于检验和加深学生对所学内容的理解和掌握。

本书可作为数学、计算机科学、通信、电子工程等相关专业的本科高年级学生或研究生一个学期课程的教材或参考书。

作者介绍:

目录: 第1章 绪论第2章 信息安全初步第3章 信息安全技术第4章 传统密码学第5章 公钥密码算法第6章 Hash函数第7章 计算复杂性理论第8章 零知识证明与比特承诺第9章 基于身份的公钥密码学第10章 数字签名第11章 密钥管理附录A 密码学中的基本数学知识参考文献
・・・・・・(收起)

信息安全与密码学_下载链接1_

标签

信息安全与密码学

信息安全

破解

密码学

加密

评论

我们老师选的书都是小众～～～

信息安全与密码学_下载链接1_

书评

当时非常痛恨 老师上这么课，全班能听懂的没几个 现在工作了 拐回来重新学习
这本书还是不错的 想学好信息安全 必须有足够的数学基础
我们上这课之前老师足足给我们补了半个月的数学，算法。

信息安全与密码学_下载链接1_