

<<实用密码学与计算机数据安全>>

图书基本信息

书名：<<实用密码学与计算机数据安全>>

13位ISBN编号：9787810546515

10位ISBN编号：7810546511

出版时间：2001-9

作者：李克洪，王大玲，董晓梅 主编

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<实用密码学与计算机数据安全>>

### 内容概要

本书介绍了实用密码技术和计算机数据安全方面的知识。

全书共分13章,包括密码学的数学基础、传统加密算法、对称密钥加密算法、公开密钥加密算法、序列密码算法、密码协议、密钥管理及算法模式、密码学的实际应用、安全操作系统、数据库安全、Internet安全以及计算机病毒方面的内容。

该书是作者在查阅了大量中、外文参考文献的基础上,结合几年来的教学、科研实践编写而成的,具有范围广、内容新的特点。

本书可做为计算机专业和通信工程专业学生、研究生的教材,也可供从事计算机安全保密研究的人员参阅。

## &lt;&lt;实用密码学与计算机数据安全&gt;&gt;

## 书籍目录

1 绪论 1.1 计算机安全及信息保密的意义 1.2 计算机安全与信息保密研究的内容 1.2.1 信息加密、解密的概念 1.2.2 算法与密钥 1.2.3 密码分析 1.2.4 算法的安全 1.2.5 算法的实现 1.2.6 计算机系统安全问题 1.3 密码学及计算机安全技术的发展 1.3.1 密码学的历史 1.3.2 国际著名安全保密机构简介 2 密码学的数学基础 2.1 信息论 2.1.1 熵(Entropy)和疑义度(Uncertainty) 2.1.2 自然语言率 2.1.3 密码系统的安全性 2.1.4 确定性距离 2.1.5 混乱与扩散 2.2 复杂性理论 2.2.1 算法复杂性 2.2.2 问题复杂性 2.3 初等数论 2.3.1 模运算 2.3.2 素数 2.3.3 最大公因数 2.3.4 乘法逆元素 2.3.5 Fermat小定理和欧拉函数 2.3.6 中国剩余定理 2.3.7 二次剩余 2.3.8 Legendre符号 2.3.9 Jacobi符号 2.3.10 生成元 2.3.11 有限域中的计算 2.4 因数分解 2.5 素数的产生 2.5.1 Solovay-strassert方法 2.5.2 Lehmann法 2.5.3 Rabin-Miller法 2.5.4 实际应用 2.5.5 强素数 2.6 有限域内的离散对数 2.7 单向哈希函数 2.7.1 概述 2.7.2 Srefru 2.7.3 N-hash 2.7.4 MD2 2.7.5 MD4 2.7.6 MD5 2.7.7 安全哈希算法SHA3 传统加密方法 3.1 换位法 3.2 简单代替密码 3.2.1 对简单代替密码的描述 3.2.2 单字母频率分析 3.3 同音代替密码 3.3.1 Beale密码 3.3.2 高阶同音代替密码 3.4 多表代替密码 3.4.1 Vigenere和Beaufort密码 3.4.2 重合度 3.4.3 Kasiski方法 3.4.4 游动密钥密码 3.4.5 转轮机和Hagelin机 3.4.6 Verham密码与一次一密密码 3.5 多字母组代替密码 3.5.1 Playfair密码 3.5.2 Hill密码 4 对称密钥算法 4.1 概述 4.1.1 分组密码 4.1.2 乘积密码 4.2 数据加密标准算法DES 4.2.1 背景 ... ..5 公开密钥算法 6 序列密码 7 密码协议 8 密码技术 9 密码学的实验应用 10 安全操作系统 11 数据库安全 12 Internet安全 13 计算机病毒概论 参考文献

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>