

<<数据保密与安全>>

图书基本信息

书名：<<数据保密与安全>>

13位ISBN编号：9787302104445

10位ISBN编号：7302104441

出版时间：2005-6-1

出版时间：清华大学出版社

作者：David Salomon,蔡建,梁志敏

页数：344

字数：602000

译者：蔡建,梁志敏

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>

<<数据保密与安全>>

内容概要

新式的密码方法可以打乱数字排列顺序，使其变得不可读，从而为专业技术人员和安全人员提供了保密性。

提供保密和安全通信的另一种方式是将信息嵌入数字文件中以实现信息的隐藏，这种方式被称为隐写术。

本书重点讨论了数据安全与保密，包括古典密码术、现代密码术以及隐写术的内容。

通过讲述不同的方法、技术和算法，作者诠释了所有主题。

此外，本书还提供了一些非常有用的示例，以帮助读者加深理解，并且对各种技术和方法作出了专业性分析。

本书主要内容：数据加密；AES-Rijndael；量子密码术；椭圆曲线密码术；文本与图像中的隐写术；随机数；无损数据隐藏；公钥密码术；音频水印。

<<数据保密与安全>>

作者简介

David Salomon是加州州立大学Northridge分校计算机科学专业的知名教授，拥有多本优秀著作，包括Data Compression:the Complete Reference,Second Edition和Guide to Data Compression Methods。

<<数据保密与安全>>

书籍目录

第 部分 数据加密 第1章 单一字母替代密码 1.1 字母分布 1.2 单一字母密码的破译 1.3 Pigpen密码 1.4 Polybius单一字母密码 1.5 扩展单一字母密码 1.6 Playfair密码 1.7 同音替代密码 第2章 换位密码 2.1 一些简单示例 2.2 循环表示法和密钥 2.3 旋转模板的换位 2.4 柱状换位密码 2.5 双重换位密码 2.6 两步骤的“ADFGVX”密码 2.7 一种破译换位密码的方法 2.8 小结 第3章 多字母替代密码 3.1 自反密码 3.2 Porta多字母密码 3.3 Beaufort密码 3.4 Trithemius密码 3.5 Vigen è re密码 3.6 Vigen è re密码的破译方法 3.7 长密钥 3.8 Vigen è re密码的一种变化 3.9 Gronsfeld密码 3.10 置换的产生 3.11 Eyraud密码 3.12 Hill密码 3.13 Jefferson多元密码 3.14 条纹密码 3.15 多音密码与不定性 3.16 Polybius多字母密码 3.17 符合指数 第4章 随机数 4.1 人工产生随机数 4.2 真正的随机数 4.3 伪随机数发生器 4.4 随机性的统计测试 第5章 Enigma机 5.1 转子机 5.2 Enigma机的历史 5.3 Enigma机的操作原理 5.4 Enigma编码的破译 第6章 流密码 6.1 对称密钥和公钥 6.2 流密码 6.3 线性移位寄存器 6.4 元胞自动机 6.5 非线性移位寄存器 6.6 其他流密码 6.7 动态替代 6.8 Latin方块组合器 6.9 SEAL流密码 6.10 RC4流密码 第7章 分组密码 7.1 分组密码 7.2 Lucifer算法 7.3 数据加密标准 7.4 Blowfish密码 7.5 国际数据加密算法(IDEA) 7.6 RC5算法 7.7 Rijndael算法 第8章 公钥密码术 8.1 Diffie-Hellman-Merkle密钥 8.2 公钥密码术 8.3 RSA密码术 8.4 Rabin公钥方法 8.5 El Gamal公钥方法 8.6 PGP技术 8.7 共享秘密的门限方案 8.8 四个要素 8.9 身份验证 8.10 椭圆曲线密码术 第9章 量子密码术 第 部分 数据隐藏 第10章 文本中的数据隐藏 10.1 基本特性 10.2 数据隐藏的应用 10.3 水印 10.4 直观的方法 10.5 简单的数字方法 10.6 文本中的数据隐藏 10.7 无害文本 10.8 Mimic函数 第11章 图像中的数据隐藏 11.1 LSB编码 11.2 BPCS隐写术 11.3 无损数据隐藏 11.4 扩频隐写术 11.5 量化数据的隐藏 11.6 Patchwork方法 11.7 图像中的签名查找 11.8 变换域方法 11.9 JPEG图像中的鲁棒数据隐藏 11.10 鲁棒的频域水印方法 11.11 检测恶意的干扰 11.12 小波方法 11.13 Kundur-Hatzinakos水印法一 11.14 Kundur-Hatzinakos水印法二 11.15 二值图像中的数据隐藏 11.16 Zhao-Koch方法 11.17 Wu-Lee方法 11.18 CPT方法 11.19 TP方法 11.20 传真图像中的数据隐藏 第12章 数据隐藏的其他方法 12.1 乐谱的保护 12.2 MPEG-2视频文件中的数据隐藏 12.3 数字音频 12.4 人类的听觉系统 12.5 时域中的音频水印 12.6 回波隐藏 12.7 隐写文件系统 12.8 也许达到极限的隐写术 12.9 公钥隐写术 12.10 目前的隐写术软件 第 部分 基本的资源 附录A 卷积 附录B 散列法 附录C 循环冗余码 附录D Galois域 附录E 练习答案 密码术时间表 术语表 参考文献

<<数据保密与安全>>

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>