

《刘氏高强度公开加密算法设计原稿

图书基本信息

书名：《刘氏高强度公开加密算法设计原理与装置（第二版）》

13位ISBN编号：9787302030676

10位ISBN编号：7302030677

出版时间：1998-08

出版社：清华大学出版社

作者：刘尊全

页数：201

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

《刘氏高强度公开加密算法设计原稿

内容概要

内容简介

这是一部计算机密码学的专著。全书分为两部分：背景和作者的发明。第一部分阐述了数据加密算法的基本方法和原理，详细剖析了数据加密标准DES和公钥密码体制RSA算法，指出了它们的脆弱性及其存在的问题，其中一些重要论点首次公布于世；第二部分阐述了作者创立的刘氏高强度公开加密算法体制，详细论述了设计原理、数学描述、加密解密装置、数值实验、可实际应用的具体实现方法和算法特性。书中理论清晰，内容新颖，并附有程序实例与数值结果，可供读者分析比较和实际应用，具有重要的实用价值和学术价值。书末附有刘氏加密算法的应用程序光盘，可供读者实际使用。可供计算机密码学的研究人员、数据加密的开发人员、应用人员阅读，也可供大专院校有关专业的师生参考。

书籍目录

目录

第1章 数据加密算法的基本方法和原理

1.1 基本概念

1.2 数据加密标准DES的算法分析

1.2.1 背景

1.2.2 DES概述

1.2.3 DES算法的剖析

1.2.4 加密变换

1.2.5 解密变换

1.2.6 DES算法的设计原理

1.2.7 DES算法的C++源代码

1.2.8 DES算法的公开性与脆弱性

1.2.9 DES算法存在的问题及其面临的挑战

1.3 公钥密码体制RSA的算法分析

1.3.1 背景

1.3.2 RSA概述

1.3.3 关于素数的分布

1.3.4 产生和测试素数的数值实验

1.3.5 RSA算法的C++源代码

1.3.6 RSA算法的加密强度问题

1.3.7 RSA算法的脆弱性及其问题

1.4 小结

第2章 刘氏高强度公开加密算法设计原理与装置

2.1 概述

2.2 基本方法和设计原理

2.2.1 随机映象

2.2.2 随机格式

2.2.3 随机函数

2.2.4 变长密钥及其自动生成

2.2.5 关于算法的加密强度

2.2.6 关于算法的计算开销

2.3 刘氏公开加密算法

2.3.1 算法的数学描述

2.3.2 形式化描述

2.3.3 运算机制及解的唯一性

2.3.4 加密和解密装置设计

2.3.5 专利内容

2.4 数值实验

2.4.1 刘氏算法的C++源代码

2.4.2 加密解密实例

2.5 刘氏公开加密算法分析

2.5.1 关于映射参数的选择

2.5.2 刘氏算法的密钥分析

2.5.3 刘氏算法与DES算法的存储空间分析

2.5.4 刘氏算法中基数M的取值对加密强度的影响

2.5.5 刘氏算法与DES算法的加密强度及计算时间比较

2.5.6 加密强度为242200的实例

2.6 密码体制的设计策略与理论分析

2.6.1 刘氏算法的设计策略

2.6.2 刘氏算法的两个重要特性

2.6.3 刘氏算法的理论剖析

2.6.4 刘氏算法的实现技术

2.7 小结

结束语

参考文献

后记

附录 “刘氏高强度公开加密算法应用程序” 光盘使用说明

《刘氏高强度公开加密算法设计原稿

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:www.tushu000.com