

<<深入浅出密码学>>

图书基本信息

书名：<<深入浅出密码学>>

13位ISBN编号：9787302296096

10位ISBN编号：730229609X

出版时间：2012-9

出版时间：清华大学出版社

作者：Christof Paar,Jan Pelzl

页数：351

字数：468000

译者：马小婷

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>

<<深入浅出密码学>>

内容概要

密码学的应用范围日益扩大，它不仅用于政府通信和银行系统等传统领域，还用于Web浏览器、电子邮件程序、手机、制造系统、嵌入式软件、智能建筑、汽车甚至人体器官移植等领域。今天的设计人员必须全面系统地了解应用密码学。

《深入浅出密码学——常用加密技术原理与应用》作者帕尔和佩尔茨尔长期执教于计算机科学与工程系，拥有十分丰富的应用密码学教学经验。本书可作为研究生和高年级本科生的教科书，也可供工程师自学之用。

《深入浅出密码学——常用加密技术原理与应用》拥有的诸多特征使得它成为密码学从业者和学生独一无二的资源——本书介绍了绝大多数实际应用中使用的加密算法，并重点突出了它们的实用性。

<<深入浅出密码学>>

作者简介

帕尔(Christof

Paar)任波鸿大学嵌入式安全系教授，并兼任马萨诸塞大学教授。

Christof讲授密码学课程的时间已有15年之久，并曾为摩托罗拉、飞利浦和NASA等多家机构的从业人员授课。

迄今已发表100多篇学术论文。

佩尔茨(Jan

Pelzl)是安全咨询公司的管理总监。

Jan拥有应用密码学博士学位，他对基于椭圆曲线的密码学的研究可谓苦心孤诣，对该领域具有非常独到和深邃的理解，已在重要刊物上发表了多篇论文。

<<深入浅出密码学>>

书籍目录

第1章 密码学和数据安全导论

1.1 密码学及本书内容概述

1.2 对称密码学

1.2.1 基础知识

1.2.2 简单对称加密：替换密码

1.3 密码分析

1.3.1 破译密码体制的一般思路

1.3.2 合适的密钥长度

1.4 模运算与多种古典密码

1.4.1 模运算

1.4.2 整数环

1.4.3 移位密码(凯撒密码)

1.4.4 仿射密码

1.5 讨论及扩展阅读

1.6 要点回顾

1.7 习题

第2章 序列密码

2.1 引言

2.1.1 序列密码与分组密码

2.1.2 序列密码的加密与解密

2.2 随机数与牢不可破的分组密码

2.2.1 随机数生成器

2.2.2 一次一密

2.2.3 关于实际序列密码

2.3 基于移位寄存器的序列密码

2.3.1 线性反馈移位寄存器(LFSR)

2.3.2 针对单个LFSR的已知明文攻击

2.3.3 Trivium

2.4 讨论及扩展阅读

2.5 要点回顾

2.6 习题

第3章 数据加密标准与替换算法

3.1 DES简介

3.2 DES算法概述

3.3 DES的内部结构

3.3.1 初始置换与逆初始置换

3.3.2 f函数

3.3.3 密钥编排

3.4 解密

3.5 DES的安全性

3.5.1 穷尽密钥搜索

3.5.2 分析攻击

3.6 软件实现与硬件实现

3.6.1 软件

3.6.2 硬件

<<深入浅出密码学>>

3.7 DES替换算法

.....

第4章 高级加密标准

第5章 分组密码的更多内容

第6章 公钥密码学简介

第7章 RSA密码体制

第8章 基于离散对数问题的公钥密码体制

第9章 椭圆曲线密码体制

第10章 数字签名

第11章 哈希函数

第12章 消息验证码

第13章 密钥建立

参考文献

<<深入浅出密码学>>

媒体关注与评论

《深入浅出密码学——常用加密技术原理与应用》一书价值非凡，将帮助从业者构建固若金汤的系统，并引导未来研究人员进一步探索奥妙无穷的密码学知识。

——Bart Preneel, K.U.Leuven

<<深入浅出密码学>>

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>