

## <<公开密钥密码算法及其快速实现>>

### 图书基本信息

书名：<<公开密钥密码算法及其快速实现>>

13位ISBN编号：9787118027495

10位ISBN编号：7118027499

出版时间：2002-9

出版时间：国防工业

作者：周玉洁，冯登国 编著

页数：146

字数：123000

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>

## <<公开密钥密码算法及其快速实现>>

### 内容概要

本书是根据作者多年的科研成果和教学实践，并结合国内外大量文献编著的。

本书对现有公钥密码算法（包括椭圆曲线密码算法）做了全面系统的介绍，并对它们的安全性做了分析，特别是给出了各种密码算法的快速实现方法，依照本书的算法，可以方便、快速地实现所需的公钥密码。

本书反映了当今公钥密码的研究现状，并力图使之成为一本高起点的、实用的密码学专著。

本书可供从事计算机通信、密码学和应用数学的科研人员参考，也可作为研究生教材。

# <<公开密钥密码算法及其快速实现>>

## 书籍目录

第1章 数学背景 1.1 数论 1.1.1 模运算 1.1.2 素数 1.1.3 最大公因子 1.2 域表示 1.2.1 有限域 $F_p$  1.2.2 有限域 $F_2$  1.2.3 用ONB表示的 $F_2$ 中元素的乘积 1.3 不可约多项式和本原多项式的判定 1.4 复杂性理论 1.4.1 算法与问题 1.4.2 算法复杂性 1.4.3 问题复杂性第2章 RSA公钥密码 2.1 RSA加密算法 2.2 RSA签名算法 2.3 RSA公钥密码的安全性及攻击RSA公钥密码的一些典型方法 2.4 素性检测 2.5 因子分解算法 2.6 RSA分钥密码的实现 2.7 参考与注记第3章 ELGamal公钥算法 3.1 离散对数问题 3.2 ELGamal加密算法 3.3 ELGamal签名算法 3.4 离散对数算法 3.5 ELGamal密码算法的实现 3.6 参考与注记第4章 椭圆曲线公钥密码 4.1 椭圆曲线上的基本运算 4.2 椭圆曲线公钥密码简介 4.3 椭圆曲线公钥密码的实现 4.4 参考与注记第5章 背包加密算法和其他公钥密码 5.1 Merkle-Hellman背包加密算法 5.2 Chor-Rivest 背包加密算法 5.3 背包公钥加密算法的破译 5.4 Diffie-Hellman公钥算法 5.5 Rabin公钥加密算法 5.6 McEliece公钥加密算法 5.7 LUC公钥算法 5/8 参考与注记参考文献

<<公开密钥密码算法及其快速实现>>

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>