

<<密码学>>

图书基本信息

书名：<<密码学>>

13位ISBN编号：9787508411163

10位ISBN编号：7508411161

出版时间：2002-7-1

出版时间：水利水电

作者：宋震

页数：179

字数：253000

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>

<<密码学>>

内容概要

本书是一本面向初学者的密码学书籍。

在本书的前一部分，主要讲述了密码学及密码工程中的一些基础知识，如密码学的基本概念、密码体制的分类以及所用到的数学知识。

然后，对各种密码体制的基本概念与原理进行简要的讨论，如古典密码体制、流密码、分组密码体制、公开密钥密码体制等，并详细描述各种密码体制中典型的密码算法过程及其安全性。

本书结构紧凑，语言严谨，论述清晰，条理性强。

在内容的安排上由浅入深，详略得当，并且有丰富的算法实例，使理论与实践相结合。适于用作各大专院校相关专业教材。

书籍目录

第1章 绪论

- 1.1 密码学的基本概念
- 1.2 密码体制的分类
- 1.3 密码学的发展历史

第2章 数学基础

2.1 数论基础

- 2.1.1 整除
- 2.1.2 素数
- 2.1.3 欧拉函数 $\varphi(n)$
- 2.1.4 最大公约数与最小公倍数
- 2.1.5 欧几里德(Euclid)算法
- 2.1.6 同余
- 2.1.7 模运算
- 2.1.8 逆

2.2 代数基础

- 2.2.1 群
- 2.2.2 有限域
- 2.3 计算复杂性理论基础
- 2.3.1 算法与问题
- 2.3.2 算法的复杂性
- 2.3.3 问题的复杂性

第3章 古典密码

3.1 易位密码

- 3.1.1 倒置法
- 3.1.2 方格易位法

3.2 代替密码

- 3.2.1 单表代替
- 3.2.2 多表代替
- 3.2.3 转轮加密算法

第4章 流密码

4.1 流密码概述

4.2 二元加法流密码

- 4.2.1 密钥流的性质
- 4.2.2 密钥流生成器的结构
- 4.2.3 基于LFSR的流密码模型

4.3 流密码算法介绍

- 4.3.1 A5算法
- 4.3.2 LFSR算法

第5章 分组密码

5.1 分组密码概述

- 5.1.1 分组密码
- 5.1.2 分组密码的设计
- 5.1.3 分组密码的分析

5.2 Feistel结构

5.3 分组密码的使用模式

<<密码学>>

- 5.3.1 电码本模式(ECB—Electronic CodeBook)
- 5.3.2 密文分组链接模式(CBC—CipherBlockChaining)
- 5.3.3 密文反馈模式(CFB—CipherFeedBack)
- 5.3.4 输出反馈模式(OFB—OutputFeedBack)
- 5.4 数据加密标准DES
- 5.4.1 DES算法描述
- 5.4.2 安全性
- 5.4.3 三重DES(3-DES, TripleDES或TDES)
- 5.5 数据加密算法IDEA
- 5.5.1 算法描述
- 5.5.2 安全性
- 5.6 RC5
- 5.6.1 RC5的参数
- 5.6.2 RC5的算法过程
- 5.6.3 安全性
- 5.7 AES(高级加密标准)
- 5.7.1 Rijndael密码设计原则与简要描述
- 5.7.2 AES算法的数学基础
- 5.7.3 AES算法过程
- 5.7.4 安全性及效率
- 第6章 公开密钥密码
- 6.1 公开密钥密码概述
- 6.2 基于大整数分解的公开密钥密码体制
- 6.2.1 RSA体制的有关数学背景
- 6.2.2 RSA体制的算法过程
- 6.2.3 RSA体制的实现
- 6.2.4 RSA实现的效率与安全性
- 6.2.5 RSA体制实用中的一些问题
- 6.3 基于离散对数的公开密钥密码体制
- 6.3.1 对数与 Z_p 上的离散对数问题
- 6.3.2 Diffie-Hellman密钥交换协议
- 6.3.3 ElGamal体制
- 6.3.4 推广的离散对数问题及推广的ElGamal体制
- 6.4 基于椭圆曲线的公开密钥密码体制
- 6.4.1 椭圆曲线的有关数学背景
- 6.4.2 定义在椭圆曲线上的密码系统
- 第7章 单向散列(Hash)函数
- 7.1 单向散列函数概述
- 7.1.1 单向散列函数
- 7.1.2 单向散列函数的设计、构造
- 7.1.3 单向散列函数的攻击
- 7.2 MD5
- 7.2.1 设计目标
- 7.2.2 算法步骤
- 7.2.3 安全性
- 7.3 安全散列算法(SHA-1)
- 7.3.1 SHA的算法步骤

<<密码学>>

7.3.2 安全性

7.4 消息鉴别码

7.4.1 算法描述

7.4.2 安全性

第8章 数字签名

8.1 数字签名的基本概念

8.1.1 数字签名的基本概念

8.1.2 基于公开密钥密码体制的数字签名

8.2 RSA数字签名体制

8.2.1 算法描述

8.2.2 安全性及其弱点

8.3 ElGamal数字签名体制

8.3.1 算法描述

8.3.2 安全性

8.4 数字签名标准(DSS)

8.4.1 DSS的签名与验证过程

8.4.2 DSA算法描述

8.4.3 实现细节

8.4.4 安全性

第9章 密钥管理

9.1 密钥的组织结构和种类

9.1.1 密钥的组织结构

9.1.2 密钥的种类

9.2 密钥生成

9.3 密钥分配和密钥协商

9.3.1 密钥分配

9.3.2 密钥协商

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>