<<密码学理论与应用基础>>

图书基本信息

书名：<<密码学理论与应用基础>>

13位ISBN编号：9787118064247

10位ISBN编号：7118064246

出版时间：2009-9

出版时间：国防工业出版社

作者：王文海　等编著

页数：214

<<密码学理论与应用基础>>

内容概要

本书是为大学本科信息类专业《密码学》课程教学编写的教材。
内容共分为10章。
第1章密码学引论：概括地阐述密码学研究的主要内容、基本概念、常用术语、算法分类、保密通信系统模型等；第2章古典密码学：介绍古典密码学中的基本运算、典型的古典密码体制、古典密码的统计分析示例；第3章密码学的数学基础：简单讲解信息论、复杂性理论、数论基础、有限域上的离散对数等基本概念和基础知识；第4章分组密码：主要讲述分组密码，重点讲述数据加密标准算法（DES）、高级数据加密标准（AES）、典型分组加密算法；第5章公钥密码体制：主要讨论公钥密码体制和算法，包括背包公钥密码系统、RSA算法、椭圆曲线密码体制等；第6章序列密码：主要讲述流密码的基本概念、密钥流产生器、移位寄存器序列、线性反馈移位寄存器的表示、m序列等内容；第7章密钥管理：主要讲述密钥的组织结构、种类、产生、分配、协商等；第8章数字签名：主要讲述数字签名的基本概念、要素、种类、产生方式、执行方式、安全性的证明方法、签名方案和标准等；第9章身份认证技术：主要讨论身份识别的种类、认证协议、交互证明系统、Fiat-Shamir身份识别方案、简化的Fiat-Shamir身份识别方案、零知识证明、基本的认证加密方案等：第10章密码学应用：结合一个保密通信系统的设计案例，讨论系统的安全性要求和系统设计方案，为读者提供一个密码学理论“全景式”综合应的用样本和系统原型，展示解决实际问题的一般思路和方法，以利读者完成“知识一技术一技能”的转变。
在每一章之后，都附有适当数量的习题，以便读者测验学习成效。
本书也可作为信息工程和信息管理类专业的研究生及工程技术人员从事密码学理论与应用研究的参考书。

作者简介

王文海，山东省滕州市人，1953年3月出生，1970年12月入伍，1976年毕业于第二炮兵技术学院（现第二炮兵工程学院）计算机专业，两次出国担任计算机专家，现任第二炮兵工程学院指挥自动化系教授，硕士生导师，培养青年教员先进个人，军队院校育才奖银奖和军队优秀专业技术人才岗

<<密码学理论与应用基础>>

书籍目录

第1章　密码学引论 1.1 密码学概述 1.2　基本概念　1.2.1　常用术语　1.2.2　算法分类　1.2.3　保密通信系统模型　1.2.4　哈希（Hash）函数 1.3 密码体制的分类　1.3.1　对称密码体制（Symmetric Encryption）　1.3.2　非对称密码体制（Asymmetric Encryption）　习题1 第2章　古典密码学 2.1 古典密码学中的基本运算　2.1.1　单表古典密码中的基本加密运算　2.1.2　多表古典密码中的基本加密运算 2.2　几种典型的古典密码体制　2.2.1　几种典型的单表古典密码体制　2.2.2　几种典型的多表古典密码体制 2.3　古典密码的统计分析　2.3.1　单表古典密码体制的统计分析　2.3.2　多表古典密码体制的统计分析 习题2 第3章　密码学的数学基础 3.1　信息论　3.1.1　信息　3.1.2　信息量和熵 3.2　复杂性理论　3.2.1　算法　3.2.2　算法的复杂性　3.2.3　问题与问题的复杂性 3.3 数论基础　3.3.1　模运算　3.3.2　素数　3.3.3　最大公因数和最小公倍数　3.3.4　求模逆元　3.3.5　欧拉定理　3.3.6　费马（Fermat）小定理　3.3.7　中国剩余定理　3.3.8　二次剩余 3.4　有限域上的离散对数 习题3 第4章　分组密码 4.1　分组密码概述　4.1.1　分组密码的研究背景、意义及现状　4.1.2　数学模型与设计思想 4.2　数据加密算法标准（DES）　4.2.1 DES算法描述　4.2.2 DES组织模式　4.2.3 DES算法的安全性 4.3　高级数据加密标准（AES）　4.3.1　AES的产生背景　4.3.2　预备知识　4.3.3　AES的算法描述 4.4　典型分组加密算法　4.4.1　IDEA算法　……第5章　公钥密码体制第6章　序列密码第7章　密钥管理第8章　数字签名第9章　身份认证技术第10章　密码学应用参考文献

章节摘录

第1章 密码学引论　　1.1　密码学概述　　密码学是以研究秘密通信为目的的一门科学，它主要包括两个分支：密码编码学和密码分析学。
密码编码学主要研究对信息的加密和解密变换，以保护信息在信道的传输过程中不被通信双方以外的第三者窃用；而收信端则可凭借与发信端事先约定的密钥轻易地对信息进行解密还原。
密码分析学则与密码编码学相反，它主要研究如何在不知密钥的前提下，通过唯密文分析来破译密码并获得信息。

密码编码学和密码分析学是同一问题的两个方面，两者的研究目的既是对立的，又是统一的。在对立中互相促进，在统一中共存发展。

密码学的历史极为久远，其起源可以追朔到远古时代，人类有记载的通信密码始于公元前400年。

密码学的发展可以分为三个阶段：古代加密方法、古典密码学和现代密码学。

古希腊墓碑的铭文、密写术以及帮会行话（黑道隐语）都是古代加密方法，这种加密方法已体现了密码学的若干要素，但只能限制在一定范围内使用。

古典密码一般采用手工或机械变换的方式实现，它比古代加密方法更复杂，但其密钥变化量仍然比较小。
古典密码时期的密码系统已经初步呈现出现代密码系统的雏形并和数学联姻。
古典密码的加密方法一般是文字替换，使用手工或机械变换的方式实现。
古典密码的代表密码体制主要有单表代替密码、多表代替密码以及转轮密码。

<<密码学理论与应用基础>>

版权说明