<<现代密码学>>

图书基本信息

书名：<<现代密码学>>

13位ISBN编号：9787030226617

10位ISBN编号：7030226615

出版时间：2008-8

出版时间：科学出版社

作者：陈鲁生，沈世镒 著

页数：199

前言

随着计算机和通信网络的迅速发展，信息的安全性越来越受到人们的重视，密码学是信息安全的基础，近三十年来，密码学的理论和应用得到了长足的发展，其内容变得越来越丰富。

本书作为信息科学系列教材之一已出版6年多了，在此期间已重印7次，受到国内多所高校师生的欢迎，本书于2006年被列入普通高等教育“十一五”国家级规划教材，借此机会，我们根据在南开大学数学科学学院为信息科学专业的本科生讲授现代密码学的教学实践和有关反馈信息，对第一版中的内容做了一些修订，讲授本书内容大约需要54个课时，如果教师在本书基础上，适当增加一些内容，本书也可以很容易地扩充为一门72课时的密码学课程教材。

对于本次修订，我们增加了一些内容，主要在内容组织上进行了一些修改，对分组密码的结构和工作模式进行了补充，增加了公钥密码的一些数学基础，另外，我们还增加了一些例题和习题，在文字表达上也做了一些修改。

本书的修订被列入“南开大学教材资助立项项目”，并得到了一定的资助支持，在此向相关人员和单位表示感谢。

尽管本书做了一些修订，但书中难免存在不妥之处，敬请读者批评指正。

<<现代密码学>>

内容概要

本书是一本关于现代密码学的基础教材。
本书延续了第一版既通俗易懂又有一定广度和深度的特点，第二版更突出了实用性和可读性。
全书共分9章。
第1章介绍现代密码学中的一些基本概念和术语。
第2章介绍古典密码的加密方法和一些典型的古典密码体制，以及古典密码的统计分析方法。
第3章介绍Shannon的密码学理论。
第4章和第5章分别讨论分组密码和公钥密码。
第6章介绍流密码和线性移位寄存器序列。
第7章和第8章分别讨论数字签名和Hash函数。
第9章介绍了一些重要的密码协议。
每章后面均附有习题，其中部分习题是对正文内容的补充。
本书除校正了第一版中的一些排印错误外，在内容上也做了一些修改和增补，特别是对第四章中的分组密码的结构和工作模式进行了补充，并在第五章中增加了公钥密码的一些数学基础。
本书可作为高等院校信息科学专业或其他相关专业的本科生教材，也可作为相关领域中的教学、科研人员以及工程技术人员的参考书。

<<现代密码学>>

书籍目录

章节摘录

1.5 密码体制的安全性　　对于一个密码体制，如果密码分析者无论截获了多少密文以及无论用什么方法进行攻击都不能破译，则称其为绝对不可破译的密码体制。
绝对不可破译的密码在理论上是存在的。
但是，如果能够利用足够的资源，那么任何实际的密码都是可以破译的。
因此，更有实际意义的是在计算上不可破译（computationally unbreakable）的密码。
所谓计算上不可破译是指密码分析者根据可利用的资源来进行破译所用的时间非常长，或者破译的时间长到使原来的明文失去保密的价值。
　　评价密码体制的安全性有一些不同的途径。
现在我们简单介绍评价密码体制安全性的三个不同的概念。
　　1）计算安全性（Computational security）：如果我们使用最好的算法来破译一个密码体制至少需要n次操作，而n是一个非常大的数，则我们称这个密码体制是计算上安全的。
计算上安全的密码体制就是计算上不可破译的密码体制。
遗憾的是，到目前为止，还没有一个实际的密码体制被严格证明是绝对的计算上安全的。
在实际中，我们通常针对某些特定的攻击类型来研究密码体制的计算安全性。
譬如，证明一个密码体制对于穷举攻击是否是计算上安全的。
当然，一个密码体制对于一种攻击类型是计算上安全的，并不意味着对于其他类型的攻击也是计算上安全的。
　　2）可证明安全性（provable security）：如果一个密码体制的安全性可以归结为某一个数学问题，而这个数学问题目前是难解的，则我们称这个密码体制是可证明安全的。
譬如，我们可以证明，如果一个给定的大整数无法有效地分解为素因子的乘积，则给定的密码体制就是不可破译的。
应当指出，可证明安全性只是说明一个密码体制的安全性是与一个数学难题相关的，并没有完全证明这个密码体制是安全的。
　　……

版权说明