<<现代密码学理论与实践>>

图书基本信息

书名：<<现代密码学理论与实践>>

13位ISBN编号：9787505399259

10位ISBN编号：750539925X

出版时间：2004-1

出版时间：电子工业出版社

作者：毛文波

页数：477

字数：800000

<<现代密码学理论与实践>>

内容概要

很多密码方案与协议，特别是基于公钥密码体制的，有一些基础性或所谓的“教科书式密码”版本，这些版本往往是很多密码学教材所包含的内容。
本书采用了一种不同的方式来介绍密码学——更加注重适于应用的密码学方面。
它解释了那些“教科书式密码”版本仅适合于理想世界的原因，即数据是随机的、坏人的表现不会超越预先的假定。
本书通过展示“教科书式密码”版本的方案、协议、和系统在各种现实应用场合存在着很多攻击，来揭示“教科书式密码”版本在现实生活中的不适用性。
本书有选择性的介绍了一些实用的密码方案、协议和系统，其中多数已成为了标准或事实上的标准，对其进行了详细的研究，解释了其工作原理，讨论了其实际应用，并且常会以建立安全性形式证明的方式来考察它们的强（实用）安全性。
另外，本书还完整地给出了学习现代密码学所必备的理论基础知识。

本书可作为高学院校计算机专业研究生或高年级本科生的教材，也可供密码安全架构师、工程人员、开发人员以及管理人员参考。

作者简介

Wenbo Mao，1993年获英国格拉斯哥Strathclyde大学计算机科学博士。
1992年到1994年在英国Manchester大学做博士后研究期间，与C.Boyd博士对密码协议和协议形式的分析进行了深入研究并做出了贡献。
后加入HP公司做高级技术成员，在英国的Bristol研究实验室的可信赖系统实验室

<<现代密码学理论与实践>>

书籍目录

<<现代密码学理论与实践>>

版权说明