<<密码学导引>>

图书基本信息

书名：<<密码学导引>>

13位ISBN编号：9787302156796

10位ISBN编号：7302156794

出版时间：2008-1

出版时间：清华大学出版社

作者：德尔夫斯,克内贝尔

页数：266

译者：肖国镇,张宁

<<密码学导引>>

内容概要

《密码学导引：原理与应用》共10章，主要从两个方面介绍密码学的知识：第一部分介绍了经典密码学中的对称密码体制、非对称密码体制及相关的密码协议，重点讨论了模代数学和以模代数学为基础的非对称密码。
第二部分从Shannon经典的信息论工作出发，分析了概率算法和单向函数的安全性，并给出了基本的安全性定义。
在此基础上，对公钥加密和签名方案的可证明安全性做了详细的分析。
另外，在附录中，《密码学导引：原理与应用》还完整地介绍了密码学中需要用到的代数数论和概率信息论的基础知识。
各章的结尾声处都有相关的习题，读者可以在原著者公布的网站上查到习题的答案。
《密码学导引：原理与应用》可作为信息安全领域的大学生与研究生的相关课程的教材，也可作为密码学和信息安全领域的研究人员的参考书。

<<密码学导引>>

作者简介

肖国镇，西安电子科技大学教授，博士生导师，上海交通大学、武汉大学兼职教授，加拿大温莎大学、德国多特蒙德大学、荷兰爱因豪芬大学、法国勒芒大学、日本九州工业大学、新加坡国立大学、美国宾夕法尼亚大学客座教授。
国际著名密码学家。
长期从事密码学和信息安全的教学和科研工作。
曾任中国密码学会（筹）副理事长、中国电子信息学会信息论专业委员会副主任，中国计算机学会信息保密委员会副主任委员、中央办公厅机要局科技进步奖评审委员会副主任、国家教委数学与力学教学指导委员会委员、西安电：广科技大学信息安全与保密研究所所长。
在国内外学术刊物和会议上发表论文多篇，与著名科学家Massey联合提出的肖-Massey定理是国际上流密码领域的基础性定理，对流密码的发展起着非常重要的作用。

<<密码学导引>>

书籍目录

版权说明