<<密码学导引>>

图书基本信息

书名：<<密码学导引>>

13位ISBN编号：9787111124788

10位ISBN编号：7111124782

出版时间：2003-12-1

出版时间：机械工业出版社

作者：Paul Garrett

页数：389

译者：吴世忠

<<密码学导引>>

内容概要

本书着重介绍现代密码学的加密思想及其实现方法，内容涉及数论、概率论、抽象代数、加密算法的思想及复杂度理论。
本书介绍了密码学的历史沿革，剖析了古典的加密算法为何会被现代的加密算法所取代，展望了密码编码领域的发展，为古典和现代密码体系提供了数学理论基础，还给出了一些针对各种加密算法的密码分析方法。
本书适合作为高校计算机安全与信息安全专业密码学导论的简明教材，也可供对密码学、数论和计算机数论有兴趣的技术人员参考。

作者简介

PaulGarrett：1973年21岁时获普渡大学硕士学位，1977年于普林斯顿大学获博士学位，之后在耶鲁大学任教。
1979～1981年在加州大学伯克利分校获得美国国家科学基金会资助的博士后奖学金，1979年成为斯坦福大学副教授，自1982年起，Paul Garrett开始在明尼苏达大学授课，1987

<<密码学导引>>

书籍目录

版权说明