<<密码学>>

图书基本信息

书名：<<密码学>>

13位ISBN编号：9787508435909

10位ISBN编号：7508435907

出版时间：2006-3

出版时间：第1版 (2006年3月1日)

作者：邓安文

页数：217

字数：348000

<<密码学>>

内容概要

密码学的研究与应用已有几千年的历史，但作为一门科学是20世纪50年代才开始的。
不可否认，互联网的广泛应用大大推动了密码学的研究与发展。
大多数国家和地区都成立了密码学学会，这些学会定期召开学术会议进行学术交流，促进了密码学的研究与应用。
国内外已出版了大量有关密码学的书籍，其理论研究也相对比较成熟，很多观点已达成共识。
本书具有以下几个方面的特点：表述清晰、论证严谨、内容新颖、选材精良、内容丰富翔实。
本书共12章，包括：古典密码、基础数论、信息理论，对称密钥密码系统、RSA密码、非对称密钥密码系统与离散对数、数字签名、质数与大整数算术、椭圆曲线密码、公开钥基础建设、量子密码。
写一本密码学方面著作的最大困难，就是确定应包含多少数学背景知识。
密码学是一个涉及广泛的学科，它需要多个数学领域的知识，包括数论、群论、环论、域论、线性代数、概率论以及信息论。
同样地，熟悉计算复杂性、算法和NP完全性理论也是很有用的。
在笔者看来，正是因为需要广泛的数学背景知识，所以导致学生们在开始学习密码学时感到很困难。
笔者试图不使用太多的数学理论，在大多数情况下，只有需要时才引入相应的数学工具。
当然，如果读者熟悉基本线性代数和模算术是会很有帮助的。
另一方面，对于更专业的主题，例如信息论中熵的概念，仅给出白描似的介绍。
本书理论阐述严格完备，实例丰富，包含有大量的算法程序以及形象的图形图表，适合于读者自学，也可作为学习密码学的参考书。

<<密码学>>

书籍目录

版权说明