

<<数论与密码>>

图书基本信息

书名：<<数论与密码>>

13位ISBN编号：9787030178855

10位ISBN编号：7030178858

出版时间：2007-3

出版时间：科学出版社

作者：冯克勤

页数：131

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<数论与密码>>

### 内容概要

密码学和信息安全是一个重要的科学技术领域，不仅关系到国家的安全，而且与人们的经济活动和社会生活息息相关。

通信的数字化和计算机技术的发展使得离散型数学（数论、代数、组合学等）在通信中得到广泛而深刻的应用。

本书通俗地介绍密码学和信息安全的历史发展与进步，用例子解释重要密码体制和信息安全的一些基本问题，讲述初等数论的基本知识及其在密码学和信息安全中的应用。

本书读者对象为对初等数论和密码学有兴趣的广大读者，具有高中以上数学知识的人均可阅读。

## <<数论与密码>>

### 作者简介

冯克勤，清华大学教授。

1941年生，1968年研究生毕业于中国科学技术大学教学系。

1973年至2000年在中国科学技术大学数学系和研究生院（北京任教，2000年后到清华大学教学系工作

。

从事代数数论和代数编码理论研究。

出版了《分圆函数域》，《代数数论简史》等专著；《整数与多项式》，《交换代数基础》，《代数数论》，《代数与通信》等大学生和研究生教材；主编《走向数学》丛书。

## <<数论与密码>>

### 书籍目录

序言1 什么是保密通信2 密码学中的格言3 凯撒密码——整除和同余4 维吉尼亚密码——周期序列5 流密码——移位寄存器6 M序列与图论——周游世界和一笔画7 M序列的实现——费马小定理和布尔函数多项式表达式8 什么是公钥体制9 RSA公钥方案——素数判定和大数分解10 PSA公钥方案——欧拉函数和欧拉定理11 离散对数公钥方案——原根与指数12 密钥管理和更换——有限域上的多项式13 密钥共享——拉格朗日插值公式14 量子密码：保密通信的未来

<<数论与密码>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>