《信息安全数学基础》

图书基本信息

书名：《信息安全数学基础》

13位ISBN编号：9787118061628

10位ISBN编号：711806162X

出版时间：2009-4

出版社：吴晓平、 秦艳琳 国防工业出版社 (2009-04出版)

页数：181

《信息安全数学基础》

前言

21世纪是计算机技术和网络技术快速发展的信息时代。信息安全已经成为世人关注的社会问题和信息科学领域的热点研究课题。信息安全与国家的军事、外交、政治、金融，甚至人们的日常生活有着密切的联系。世界各国都在信息安全的基础设施建设、教学以及研究开发方面投入了大量的人力和资金。人才是发展信息安全的关键，自2001年武汉大学创建了全国第一个信息安全本科专业至今，全国已有30多所高校建立了信息安全专业。信息安全是计算机、通信、电子、数学、物理、生物、法律、管理、教育等多个学科的交叉学科。而数学则是信息安全学科的基础，有专家指出“未来的信息战争在某种程度上是数学的战争”，可见数学在信息安全中的地位和作用。在信息安全和密码学的学习和研究中，如信息安全模型的建立、密码体制的设计（尤其是公钥密码体制的设计）、密码分析破译、密码体制的形式化分析以及安全性证明（尤其是可证安全证明）等涉及和使用了数论、抽象代数、布尔函数、椭圆曲线理论、图论、计算复杂度等方面的数学知识。这些数学知识在高等院校工科数学中大部分是没有介绍过的，因此非数学专业学生在学习这些与信息安全紧密相关的数学知识时遇到了很大的困难，而有关数论、代数和椭圆曲线论等方面的书籍多半是针对数学专业的学生，难度大、内容多，其中应用于信息安全的数学理论和知识只是一小部分，不便于非数学专业的学生进行阅读和学习。因此，本书希望将这些应用于信息安全的数学理论，以及信息安全研究和应用中所产生的一些新的数学成果做一次系统全面的介绍，以方便信息安全、计算机科学技术、通信工程等专业的学生及信息安全领域的工作者学习。本书第1章一第5章分别介绍了数论中的整数的唯一性分解定理、同余式、二次剩余、原根、紊陆检验等内容，第6章、第7章介绍了抽象代数中的群、环、域，第8章介绍了布尔函数的概念和基本性质，第9章简单介绍了应用于椭圆曲线密码体制的椭圆曲线理论，第1O章介绍了图论的基本知识和应用，第11章介绍了NP完全理论的相关内容。由于篇幅所限，本书在编写过程中有选择性地略去了部分定理较为繁杂的证明过程，学有余力的读者可查阅列于书末的参考书目或其他相关书籍。由于学时数有限，建议授课教师根据学生实际情况适当选取课堂讲授内容，其他内容可安排学生进行自学。本书内容翔实、概念表述严谨、语言精练、例题丰富，切合教学之用。但由于时间和水平有限，不妥和错误之处在所难免，希望老师们和读者提出宝贵意见，以使本书能够进一步修改完善。本书在编写过程中得到海军司令部机要局的大力支持和海军工程大学电子工程学院信息安全系许多教师的热情帮助，在此向他们表示衷心的感谢。作者2008年12月

《信息安全数学基础》

内容概要

《信息安全数学基础》包含初等数论、抽象代数、布尔函教、椭圆曲线论、图论、NP完全理论等方面的内容,结构合理,内容系统全面。书中以大量例题深入浅出地阐述各数学分支的基本概念、 基本理论与基本方法。注重背景、强调应用,便于读者理解掌握。《信息安全数学基础》可作为信息安全、计算机科学与技术、通信工程、电子等领域的研究生和本科生相关课程的教科书,也可作为这些领域工程技术人员的参考书。

《信息安全数学基础》

书籍目录

《信息安全数学基础》

章节摘录

插图：第2章同余式在日常生活中，我们所要注意的常常不是某些整数，而是这些数用某一固定的数去除所得的余数。例如，我们知道某月2号是星期一，那么9号、16号都是星期一，总之用7去除某月的号数，余数是2的都是星期一。这样，就在数学中产生了同余的概念，这个概念的产生大大丰富了数学的内容。本章首先介绍同余的概念和基本性质，进而介绍所谓完全乘余系和缩系，然后建立了著名的欧拉定理和费马定理，最后介绍了解某些同余式的一般方法。2.工同余的概念和基本性质定义1.1 给定一个正整数m，如果用m去除两个整数。所得的余数相同，我们就说a、b对模数m同余，记作a-b（mod m），如果余数不同，我们就说0、b对模数不同余。从同余的定义出发，可得到模m同余的等价关系，即：（1）（自反性）对任一整数a，a＝a（mod m）；（2）（对称性）若a=b（mod m），则b＝a（mod m）：（3）（传递性）若a=b（mod m），b=c（mod m），则a=c（mod m）。定理1.1 整数a、b对模数m同余的充分必要条件是m （a-b）。证明：设a=b（mod m），则有a=mq1+r，0≤r

《信息安全数学基础》

编辑推荐

《信息安全数学基础》由国防工业出版社出版。

《信息安全数学基础》

版权说明