<<数论与密码>>

图书基本信息

书名：<<数论与密码>>

13位ISBN编号：9787561778388

10位ISBN编号：7561778384

出版时间：2010-9

出版时间：华东师范大学出版社

作者：杨思熳 编

页数：133

前言

进入21世纪，世界各国都将提升教育质量确定为教育改革的重心，教师教育改革与创新更是成为重中之重。

中国教师教育改革发展同样面临的一个核心问题，即如何把国家教师教育的战略导向和基础教育新课程改革对教师教育的要求，转化为教师教育改革实践的具体目标与措施，加快传统师范教育向现代教师教育的转变，培养造就一大批优秀教师和未来教育家。

自教师教育产生发展至今，源起于为教师提供教学法训练的学科教育，在教师培养与培训过程中一直充当着重要角色。

自新中国建立以来，师范院校一直是教师教育的主阵地，因此，学科教育研究与实践的核心任务，就是研究基础教育，培养、培训中小学校教师。

其遵循的一个核心原则是，对不同学科的教学规律的发现与运用，要与教育学的一般理论紧密结合起来，一般而言，教育学理论对于学科教育研究与实践具有指导作用，而学科教育反过来促进教育学理论的发展。

1986年，美国公布霍姆斯报告，新一轮教师专业化运动迅速兴起，“学科教学知识”概念应运而生。

这一概念强调，学科知识既包括学科内容，也包括学科知识的逻辑结构，因此对学科知识结构的掌握，直接影响着教师传授知识的方法和效果。

这就要求学科知识与教育学知识要在更深层次和更广范围上实现结合，从而对传统的学科教育理论提出了挑战。

但是，迄今为止，大多数学科教育研究与实践者仍然尊奉的是传统原则。

基于各学科自身的知识逻辑，基于教师自身所需知识的逻辑结构，以及基于基础教育阶段各学科学习的认知规律和教学策略，尝试重新构建一个全新的学科教育理论框架，仍停留在一个讨论的层面。

<<数论与密码>>

内容概要

本书论述了公钥密码学的基本理论及实现，主要包括：RSA密码体制、ElGamal公钥密码体制、椭圆曲线公钥密码体制和数字签名。
本书的特点之一，内容涉及面广，在有限的篇幅内，包含了必要的预备知识和较完备的数学证明；特点之二，用系统的数学方法讲述了公钥密码学的主要数学原理；特点之三，从算法的角度进行论述，对每个主要的理论结果给出其可编程的实际算法；特点之四，对目前理论和实践前景最好的椭圆曲线密码的实现，结合最新的国际研究进展(如2009欧密会论文)给出了浅显的介绍。
本书的内容曾多次在华东师范大学数学系给本科生讲授。

<<数论与密码>>

书籍目录

第一部分 密码学中的数论 第一章 数论基础 1.1 导言 1.2 整数的可除性 1.3 算术函数 1.4 素数分布 1.5 同余理论第二部分 公钥密码学 第二章 古典密码学 2.1 几个简单的密码体制 2.2 古典密码的密码分析 习题 第三章 RSA密码体制 3.1 公钥密码学简介 3.2 计算复杂性理论 3.3 RSA密码体制 3.4 素性检测算法 3.5 因子分解算法 3.6 对RSA的攻击 3.7 Rabin密码体制和可证明安全性 习题 第四章 基于离散对数问题的公钥密码体制 4.1 离散对数问题算法 4.2 模p指数计算的Monte Carlo算法 4.3 基于离散对数的密码体制 4.4 椭圆曲线密码 习题 第五章 数字签名方案 5.1 RSA签名方案 5.2 改进的Rabin数字签名方案 5.3 ElGamal数字签名方案 5.4 数字签名标准和椭圆曲线数字签名 5.5 一次性签名方案 5.6 失败一停止签名方案 5.7 不可否认签名方案 第六章 信息安全的其他课题 6.1 秘密共享 6.2 互联网安全和电子商务参考文献部分习题解答

<<数论与密码>>

版权说明