文章编号：1672-5913(2016)11-0027-04
中图分类号：G642

信息安全数学基础的“讲一练二考三”改革方案设计

李瑞琪[1]，高敏芬[2]，贾春福[1]
（1. 南开大学 计算机与控制工程学院，天津 300353 ；2. 南开大学 数学科学学院，天津 300071）

摘　要：结合信息安全专业的特点以及“讲一练二考三”的本科教学指导思想，提出需要对信息安全数学基础课程的教学组织、教学方式和考核方式进行探索和改革，解决当前教学中遇到的问题，以便学生在学习过程中提高学习兴趣，更好地学习和掌握本课程涉及的知识和技能，为后续课程的学习打下坚实的基础。

关键词：教学改革；讲一练二考三；信息安全数学基础
DOI:10.16512/j.cnki.jsjjy.2016.11.007

0　引　言

所谓“讲一练二考三”，可解释为精讲、多练、广考[1]，要求控制教师的讲授量，增加学生的练习量以及扩大考试的涉及面[2]，从“以教为主”转变为“以学为主、教学相长”，努力形成学生自觉主动学习的局面，最终“授人以渔”，达到“教是为了不教”“学是为了会学”的目的[3]。这种教学理念从根本上改变了“单纯传授知识”的传统教学方式，使学生由依赖性学习转向自主性学习，更有效地调动学生的学习主动性，使其掌握知识、提高能力、内化素质，促进学生全面发展[4]。

信息安全数学基础是面向信息安全专业二年级本科生开设的一门专业基础课，讲授数学理论，其教学内容的最大特点是知识点具有很强的逻辑性与抽象性。这种类型的课程会让学生觉得这门课的内容晦涩难懂并且枯燥乏味，从而导致很多学生无法提起兴趣，从以往教学过程中学生反馈的信息也可以印证这一点。学生的反馈意见主要有两点：一是课程内容较多较难，无法抓住知识脉络；二是课程内容与实际联系不大，并不清楚所学内容的具体用途。针对学生提出的问题，本课程的教学改革势在必行，而“讲一练二考三”这种新的教育理念恰恰要求教师在教学中抓住知识主线对学生进行引导，将理论与实践相结合，使学生全面发展。因此，利用“讲一练二考三”的理念对信息安全数学基础课程进行改革是必要且可行的。

1　课程内容

信息安全数学基础课程主要涉及三大部分内容，分别是数论基础、抽象代数基础与椭圆曲线理论。数论基础包括整除、同余、原根与指数、二次剩余 4 个章节，首先介绍整除和同余的相关概念，在此基础上介绍原根与指数以及二次剩余，进而介绍密码学的一些重要数论原理。抽象代数基础是本门课程的核心部分，包括群、环、域 3 个章节，通过递进式地介绍 3 种代数系统的相关理论，逐步引出伽罗瓦理论以及有限域理论，这是当代编码与密码学等信息科学理论的基础。椭圆曲线理论包括椭圆曲线一章，教师在之前章节的基础上介绍椭圆曲线的相关概念，进而介绍椭圆曲线上的群结构和椭圆曲线上的离散对数问题以及上述数学理论在相应一类公钥密码中

基金项目：南开大学 2015 年本科教育教学改革项目（教字通 [2016]3 号）。
第一作者简介：李瑞琪，男，研究生，研究方向为密码学及其应用，rickylee@mail.nankai.edu.cn。

的应用[5]。

这3部分内容的教学侧重点有所不同。对于数论基础部分，在讲授时侧重于数学原理的实际应用，特别是在密码学中的应用，学生不仅仅学习了数论中的一些理论，更重要的是让学生更多地体会到如何利用这些原理设计密码体制。而对于抽象代数基础部分，教师在讲授时侧重于数学定理的理解与证明。由于这一部分理论比较难理解，因此教师在教学中需要对讲授的概念和定理进行细致的分析和证明，使学生能够理解透彻，并且培养数学逻辑思维能力，从而为学习密码学打下坚实的数学基础。对于椭圆曲线理论部分，教学时则侧重于椭圆曲线中的计算问题，这是基于椭圆曲线问题的公钥密码的基础，应当让学生熟练掌握计算方法。

由于信息安全数学基础课程的教学内容设计了数学的多个分支，难度不同且讲授时的侧重点不同，因此在设计课程的改革方案时，应当针对不同的分支设计不同的“讲”“练”“考”的内容和形式，从而能够更好地让学生学习到各部分知识。

2 “讲一练二考三”改革方案设计

2.1 “讲一”

“讲一”，意味着讲授少而精。讲授并不等同于将全部内容填鸭式地教给学生，而应当着眼于对学生的引导。课上讲授的内容应是重点和难点，不仅要讲，还要讲透。课堂上不讲或者简略讲解的内容，教师应给予适当的引导，然后学生自主学习这部分知识。信息安全数学基础课程的内容涉及数学中几个不同的分支，难度和侧重点各有不同，因此可以用“讲一”的思想对本门课程的讲授进行改革并予以实践。

在第1章的预备知识中，关系和拓扑空间属于学生新接触的概念。关系是学习抽象代数的基础，拓扑空间是学习椭圆曲线的基础，因此这两个概念应当讲透。而集合、映射、函数等概念在中学和本科一年级的学习中都有所涉及，这些概念通过“练”等方式留给学生自己进行即可。

在数论部分，对基本概念的讲解需要简洁且透彻，而对重要的定理，例如欧拉定理、勒让德符号、二次互反律等，应当重点讲解。教师在细致讲解的同时要引导学生思考如何在密码学中运用这些数学原理，使学生主动探索课上所讲的数学原理与已有的密码算法之间的联系，并鼓励学生动手编程实现或者尝试运用数学原理构造密码体制。

抽象代数部分，由于其本身的难度较大，因此需要安排较多的课时讲授。这部分内容涉及的概念、定理较多，许多内容比较抽象，知识点层层递进、环环相扣，在讲授时需要对概念进行透彻地讲解，对定理证明过程进行详细地分析。陪集、商群（环）、同态、同构等概念在抽象代数的体系中都是非常重要的，特别是同态基本定理。在讲授这一部分时，应当注意引导学生建立抽象的数学思维，不能让学生死记硬背概念和定理。抽象思维的建立对深入学习相关知识以及理解一些复杂的密码算法有很大的帮助，而如何运用抽象思维留给学生在“练”的部分进行。

椭圆曲线部分既涉及数论知识又涉及抽象代数的知识，综合性较强，难点在于代数曲线、Weierstrass方程、椭圆曲线等概念和原理的理解，重点在于有限域上椭圆曲线的计算问题。讲授这一部分时应当重点强调计算问题，细致讲解计算中需要注意的问题，特别当涉及数论和抽象代数的内容时，可以帮助学生回顾之前学习的知识。而对于较难理解的代数曲线等内容，只需简略而精炼地讲授其核心原理。

2.2 “练二”

根据“讲一练二考三”的理念，“练二”意味着丰富学生的课下练习，教师应当布置多种形式的练习。这些练习不应拘泥于课上所讲，主要的练习方式有以下几种。

第一，课堂上随机提问。提问的内容可以是不容易理解的概念，让学生谈一谈对概念的理解，如果理解有偏差，可以让全班同学讨论；提问的内容还可以是重要定理的证明过程，让学生谈一谈证明思路，如果有不完善之处可让其他同学补充。比如首次学习陪集和商群的概念时，可以让学生说一下自己的理解，用图形化的方式表达这些概念；再比如学习同态基本定理时，可以让学生讨论其推论的证明过程。

第二，课后习题。本课程使用的教材在每一

章节后都设有 A、B 两组习题，A 组习题较为基础，B 组习题难度较大或者更加开放。在每章讲完后，都可从 A、B 两组中选择一定量的习题作为课后作业。A 组习题注重巩固学生对基础知识的掌握，而 B 组习题的内容较为丰富，包括难度较大的证明题、偏向实践的计算题、较为开放的主观题。这两组习题在一定程度上训练和培养了学生不同方面的素质，A 组习题的训练目的是希望学生能够重视数学原理，并通过习题巩固课上所学的重点理论，从而达到培养学生基本数学思维的目的，比如证明同态基本定理的两个推论；B 组习题的训练目的更加多样化，难度较大的证明题深入训练学生的数学思维，如果学生独立完成有困难，可以多人讨论，但应注明讨论与思考过程，不能“一抄了之”，偏向实践的计算题希望学生能够从这种类型的练习中体会数学原理在密码学的具体应用方式，开放性的主观题较为综合，锻炼学生的归纳总结能力以及培养学生的创新思维，比如归纳一下运用类似数学原理的加密算法有哪些、利用某个数学原理简单地设计一个密码体制等。

第三，编程训练。理论与实践应当是相辅相成的，在课堂上教师侧重于讲解理论知识，因此动手实践留给学生课下进行。本门课程涉及的编程训练参考了机械工业出版社《初等数论基础及其应用（第五版）》一书的课后编程题以及教材的编程题。编程训练主要分为两类：一类是利用计算机编程实现一些数学定理或计算问题，比如编程实现中国剩余定理、编程计算给定的有限域上椭圆曲线中的所有点等；另一类是利用课上所学的某种数学原理编程实现一个简单的加密算法。通过这种编程训练，学生可以对数学原理有更深的体会，并且可以初步了解密码算法的实现过程。

第四，科研素质培养。由于信息安全数学基础是密码学的基础课，学习数学基础的目的也是为了更好地研究密码学。因此在本门课程中，教师可以给学生推荐一些密码学文献，或让学生根据所学数学原理自己搜索相应的密码学文献，学生阅读文献后对文献内容和自身收获进行总结。学有余力的学生，可以尝试通过所学的数学原理设计一种简单的密码体制。学生在找文献、读文献、总结文献以及自身思考的过程中能够培养科研素质，为此后毕业设计、攻读硕士博士学位及科研工作打下基础。

2.3 “考三”

专业课考试的目的是检验学生的学习成果，考查学生对这门课程的整体掌握情况以及学生的专业能力。所谓专业能力，就是学生灵活应用专业知识的能力。学生学习专业课并不是为了记住书中的所有知识点，而是学会以专业的视角看待问题，以专业的思维思考问题，用专业的知识解决问题。因此，考试应当对学生数学思维能力和综合应用能力进行考查，考试题目涉及的知识点具有范围广、综合性强的特点，这符合“考三”的理念。

考试的题型主要有 3 种：计算题、证明题和实践题。

计算题和证明题考查学生的数学素养，其中既有基础题也有提高题。基础题考查重点定理的计算与证明，比如解同余方程组、证明同态定理等；综合题包含多个知识点，考查学生是否融会贯通，比如有关椭圆曲线的计算题既考查数论中的相关计算，也考查椭圆曲线中的一些计算方法，再比如抽象代数部分的证明题可以综合群、环、域的相关性质以及同态基本定理这些知识点。

实践题则考查学生将理论应用于实践的能力，题目更贴近实际应用，并且可以设置一些主观题目。比如在题目中描述一种加密算法和需要加密的信息，让学生计算加密结果。教师在出这类题目时最好能使用经典的加密算法或最新研究成果中的算法，并在题目中注明，这可以使学生在考试时有所收获。如果学生在平时练习时能够做到利用数学难题设计简单的密码体制，那么在考试中可以尝试加入利用数学难题设计加密方案的题目，或者评价题目中给定的加密方案是否安全并给出理由。类似于上述的主观题，学生在作答时言之成理、符合基本数学原理即可。

为了落实《国家中长期教育改革和发展规划纲要（2010—2020）》，2011 年南开大学推行的《素质教育实施纲要（2011—2015）》提出，教学活动应根据“公能”素质教育培养目标，逐步推动

各个专业的教学改革，改进教学计划，调整课程结构，设计课程目标，更新教学内容，强化实践教学，创新教学方法；应坚持“以学生为主体、以教师为主导”；应在教学中推行启发式、讨论式等教学方法，加强教与学互动，引导学生主动学习知识，发现问题，开展自主研究；应探索以“讲一练二考三”为特点的教学组织与课程考试方式，强化“学习、实践、协作、创新”能力训练，激发学生自主学习的兴趣。根据以上指导思想及信息安全专业的特点，我们对南开大学信息安全数学基础课程进行了上述改革方案的设计。

南开大学信息安全数学基础课程改革前后的教材信息与课时分配情况如下。

南开大学信息安全数学基础课程采用的主要教材是南开大学贾春福、钟安鸣、赵源超所著《信息安全数学基础》[5]。这本教材是在信息安全数学基础课程所用讲义以及多年的教学经验的基础上编纂而成的，为南开大学信息安全专业本科生量身定做。另外，为了拓宽学生视野，在改革方案中选取了一些课外参考书目。上海交通大学陈恭亮教授的《信息安全数学基础》一书知识点较为全面，也具有一定的难度，课程中将其选为推荐参考书目，供学生在课后进一步学习使用。此外，在课程中也推荐了一些关于数论、抽象代数和代数曲线等方面的参考书目供学生有针对性地对课程某一部分进行深入了解。

课时分配：南开大学信息安全数学基础课程的课时分配表见表 1，表中展示了改革前后课时分配的对比情况。其中，原课时分配一列中的“+x”表示每章后的习题课占 x 课时；改革后课时分配一列中的“+x+y”表示每章后的习题课占 x 课时，开放性练习课占 y 课时。这里的开放性练习课包括编程实现某些数学原理或者密码算法的练习、对某个开放性问题进行小组讨论、研究某篇论文后作一个报告等几种模式。改革前后课时分配的区别在于减少了教师讲授的课时，增加了让学生进行各种开放性练习的课时，达到少讲多练的目的，从而促进学生的自主学习意识以及培养学生的综合素质。

表 1　南开大学信息安全数学基础课时分配情况

章节	原课时分配	改革后课时分配
第 1 章 预备知识	3+1	2+1+1
第 2 章 整除	3+1	2+1+1
第 3 章 同余	3+1	2+1+1
第 4 章 原根与指数	3+1	2+1+1
第 5 章 二次剩余	3+1	2+1+1
第 6 章 群	8+2	7+2+1
第 7 章 环	8+2	7+2+1
第 8 章 域	10+2	8+2+2
第 9 章 椭圆曲线	10+2	8+2+2

3　结　语

在今后的教学工作中，我们可以逐步运用这些改革思路和方案，通过教学成果检验改革思路和方案的可行性。在教学实践中根据学生的反馈情况动态地调整教学方法，效果好的方案要继续坚持，效果不好的方案应当及时改进并思考和总结问题所在。此外，在以后的信息安全数学基础课程的教学活动中，如果能够发现并总结出其他符合“讲一练二考三”理念的教学方法，也可以将其加入整体的课程改革方案中，以丰富和完善课程改革理论，并为教学实践提供多种选择。

参考文献：

[1] 赵迎新, 刘波, 李国峰. 模拟电路课程贯彻“讲一练二考三”的教学改革与实践[J]. 教育教学论坛, 2015(7): 77-78.
[2] 陈德富, 陈喜文. “讲一练二考三”在南开大学遗传学教学中的实践[C]// 中国遗传学会. 2014全国遗传学理论与实验教学研讨会会议手册及论文集.北京:中国遗传学会, 2014: 67-70.
[3] 蔡峻, 严冰. “讲一练二考三”教学理念的再思考[J]. 高校生物学教学研究(电子版), 2013, 3(4): 7-9.
[4] 徐娟, 宋继华, 胡佳佳. 初论“讲一、练二、考三”[J]. 计算机教育, 2006(6): 22-26.
[5] 贾春福, 钟安鸣, 赵继超. 信息安全数学基础[M]. 北京: 清华大学出版社, 2010.

（编辑：孙怡铭）