Three Elements in the Teaching of "The Basic of Math for Information Security"

LUO Fang，OU Qing-yv, WU xiao-ping
Depart. of Information Security, Naval University of Engineering, Wuhan, China
1. lf_0215@sina.com, 2. ouqingyv@sina.com, 3. wxp_08@sohu.com

Abstract: "The basic of math for information security" is important in the course system for information security major. In this paper, the objectives and characteristics of this course are analyzed and summarized. Aiming at the deficiencies in the teaching, the improvement and implementation of this course are discussed, concerning how to implement the teaching method of math theroies, how to combine the information security engineering with the math theories, and how to inspire the innovation of the student.

Keywords: cryptography; information security; the basic of math; teaching

"信息安全数学基础"课程教学三环节

罗芳，欧庆于，吴晓平
海军工程大学信息安全系，湖北武汉，中国，430033
1. lf_0215@sina.com, 2. ouqingyv@sina.com, 3. wxp_08@sohu.com

【摘要】"信息安全数学基础"在信息安全专业课程体系中占有非常重要的地位。本文分析并总结了该课程的教学目标和特点，紧扣教学过程中存在的不足，围绕如何进行相关数学理论教学，如何将数学理论与信息安全工程实践相结合，以及如何培养学生创新意识三个环节，系统地阐述了该课程教学方法的改进和实施。

【关键词】密码学；信息安全；数学基础；教学

1 引言

在信息技术与信息产业迅速发展的今天，信息安全正逐步融入到国家安全的各个方面，成为信息社会迫切关注的问题，各国都对其给予了极大的关注和投入。然而，在加大信息安全系统投入的同时，注重信息安全的人才培养，才是确保信息安全的关键所在。

在信息安全专业课程体系中，"信息安全数学基础"较为系统地介绍了信息安全所涉及的数学理论，是整个学科专业的理论基础。这正是缘于数学是一切自然科学的基础，因此，对于信息安全学科也不例外。事实上，数学的抽象概念是对信息安全中诸多对象的本质刻画，例如，在信息的编、解码，保密及认证等方面都是以数学作为其理论基础的。对于该专业的学员而言，只有具备了扎实的信息安全数学基础，才能真正地理解、掌握现有的密码算法及其核心设计思想，并设计出更先进的密码算法和安全协议，从而更好地适应未来信息安全领域的各种挑战。因此，切实提高"信息安全数学基础"这门专业基础课的教学水平，对于信息安全专业的人才培养是十分必要的。

2 问题的提出

数学作为自然科学的理论基础，其自身的理论性是毋庸置疑的，而"信息安全数学基础"作为一门数学课程，必然具有突出的理论性特点。

其次，作为一门新兴课程，"信息安全数学基础"有其区别于传统数学课程的地方。由于信息安全数学的诞生本身就是为了解决实际应用中大量数据的安全存储和传输问题，从而决定了其更贴近于实际的安全应用，具有较强的实用性。

此外，信息安全数学也是一门不断发展、变化的数学，随着外部计算环境的发展，许多旧的理论不再适用，

新的理论不断更新。

针对以上课程特点，笔者认为在该门课程的教学过程中普遍存在以下三个问题：

（1）“信息安全数学基础”围绕公钥密码学所基于的三个数学难题，重点介绍了数论、抽象代数和椭圆曲线三方面的相关数学理论。由于这些数学知识远比一般的高等代数难，对于非数学专业的学员而言，研究难度确实比较大，容易产生畏难情绪。尤其觉得数学在今后的学习和工作中都不是必需的，对于信息安全数学问题疏于思索和研究，理论基础不扎实的现象普遍存在。

（2）在课程教学中，教员往往只强调基本数学原理和方法的掌握，与信息安全工程实践结合不紧密，忽略了这些数学原理和方法的工程应用背景。由于没有将工程化思想融入课堂教学，导致学员对于“学习这些数学理论能干什么”、“在什么地方用”、“怎么用” 时常感到困惑，有悖于这门课程实用性的特点。

（3）学员容易产生信息安全数学是一成不变的思想，对信息安全的发展方向认识不足。其次，往往由于缺乏对密码算法、协议所基于的数学基础的深入了解，无法对算法、协议进行优化实现，导致其所设计的安全系统在速度和效率等方面存在瓶颈的现象屡见不鲜，对于设计、实现新的算法、协议更是感到无能为力。这将严重阻碍信息安全产业自主化进程。

综上所述，对于信息安全数学基础的教育工作者而言，如何针对这门课程的特点，改变传统数学教育模式，在积极引导学员牢固掌握课程知识点的同时，重点培养其灵活运用基本的数学原理和方法，发挥创新思维有效解决实际安全问题的能力，已成为“信息安全数学基础”课程教学中一个全新的课题和挑战。

3 课程教学三环节

要上好“信息安全数学基础”这门课，对教员的要求是很高的。教员必须具备较高的理论水平，才能将抽象的数学理论重新做一个梳理，关键是穿插进信息安全工程思想重新整合成一套思维体系，深入浅出地传授给学员，让其能够建立形象的印象，以至深刻领会。

3.1 夯实数学基础，掌握证明方法

信息安全中的几个经典密码算法，如：RSA、DES、Elgamal 等都是建立在一些基本的数学理论之上的，如果不牢固掌握这些数学理论，就谈不上对这些算法的真正理解，对后续专业课的学习也势必会造成影响，从而丧失了“信息安全数学基础”作为一门专业基础课的意义。因此，在教学过程中必须有意识地让学员加深对重点概念的理解，帮助其打牢数学基础。这就必然要沿袭传统数学：定义、定理、推论以及证明的教学模式[1]，学员在学习过程中难免会觉得条理不清晰，且内容枯燥。

因此，教员要善于将较难的数学问题转化为一些容易的小问题，通过补充适当的例子帮助学员消化、理解。在授课过程中还应及时对所讲内容进行梳理，做到脉络清晰，从而体现数学理论深入浅出，由简到难，由形象到抽象的特点。

此外，应当充分调动学员的积极性和主动性，在帮助其打牢基础的同时，营造快乐、轻松的学习氛围，例如，教员在授课过程中，可以经常为学员讲述一些数学家的故事，像费马、欧拉、高斯等等[2]，引导其对于数学研究的兴趣，使原本枯燥的数学理论不再乏味。

在教学过程中笔者发现，学员反映课程难度大的普遍原因在于对定理的证明和推导方法感到困惑，如广义 Euclid 除法，模重复平方法、中国剩余定理、有限域的构造等。事实上，以上数学理论的推导经常要用到存在性和构造性证明方法，因此，教员在授课过程中不应简单地将书本上的内容传授给学员，而应使其重点掌握信息安全数学的研究方法，学会用严格的数学语言对信息安全和密码学所涉及的一些具体数学理论进行推理和说明，养成良好的数学思维，做到触类旁通。

3.2 紧扣密码学与信息安全的联系

信息安全数学具有鲜明的应用性特点，因此，不应仅从数学的角度来探讨其教学模式。笔者认为，贯穿于“信息安全数学基础”课程教学体系的核心思想应是如何构建一个安全、有效的密码系统。换言之，该门课程的另一个重要的目的就是引导学员掌握如何将所学的信息安全数学理论应用到一个实际的密码系统中去，这就要求教员将信息安全数学的工程应用背景讲透。例如，在课程初期可以通过介绍一些日常生活中接触到的信息安全数学问题的典型应用，如数字证书，数据加密传输以及常见的攻击手段等，来回答“学习这些数学理论能干什么”、“在什么地方用”等问题，使学员深刻领会到信息安全数学与日常生活的紧密联系，加深其对这门课程教学目的的理解，激发其学习兴趣。在授课过程中谈及欧拉函数和欧拉定理，就可介绍其在 RSA 公钥密码算法中的具体应用；讲到抽象代数中置换群的概念，就可为学员揭示分组密码的数学本质。通过以上将数学理论与信息安全具体应用相结合的教学模式，真正

978-1-935068-09-9 © 2010 SciRes.

做到寓理论于实际，让每名学员在体会信息安全的原理与理论源头的同时，使其懂得信息安全数学的实际应用，进而沉醉于数学之美。

其次，信息安全数学的应用性决定了对这门课程的讲授绝不能局限于书本本身，而应加入一些跨学科的工程实践环节，比如编程实践等，以更好地回答信息安全数学“怎么用”的问题，体现其应用性强的课程特色。在教学实施中，可重点针对某一个算法（如公钥密码算法 RSA）进行深入的探讨，展示该算法是如何应用计算机技术实现数据安全的，并要求学员通过分组编程实现加、解密功能，从而使其对信息安全数学的工程实践有更真切的体会。

3.3 构建“研究型、创新型”的人才培养模式

创新型人才培养是院校课程教学的重要目标。在“信息安全数学基础”的课程教学中应以素质教育和提高学员主体地位为主线，以“研究型、创新型”为鲜明特色，使学员在掌握扎实的数学理论、了解信息安全学科前沿的基础上，学会利用数学理论研究问题的一般方法，提高学员分析问题和解决问题的能力。这就要求教员在授课过程中并不局限于某一点，而应采取引导式教学，把问题发散开来，和学员一起进行开放式探讨，引导其发散思维，培养其解决问题的能力。

其次，由于信息安全数学的发展、变化性，导致书本上的知识往往滞后于实际应用，这就要求教员在讲授信息安全数学现有应用的同时，更多地关注最新技术进展，使学员逐步认识到不存在绝对的安全性，旧的算法会因外部计算环境的发展而被逐渐淘汰，而新的算法也会因此被提出并加以应用。让学员明白在变化和发展中所蕴藏的机遇和挑战，使其在及时跟踪和掌握信息安全学科最新进展的同时，尽可能发现和解决国家信息化进程中所遇到的问题，作出创新工作。

4 结束语

“信息安全数学基础”在信息安全专业课程体系中占有非常重要的地位。本文分析了其理论性、实用性和发展性三个特点，总结了教学过程中存在的不足。就如何进行数学理论教学，如何将数学理论与信息安全工程实践相结合，以及如何培养学生创新意识三个方面，系统地阐述了该课程教学模式的改进。教学实践表明，以上三个教学环节能够使学员真正体会到数学是信息安全的核心，激发其学习数学的兴趣。与此同时，学习态度也更为积极，能够主动跟上信息安全和密码学的最新进展，有效地促进了课程教学质量的整体提高。

但在教学过程中仍然暴露出一些不足，主要表现在现行的信息安全数学基础教材缺乏可供学生参与实践的内容，这就需要在教学过程中加入一些教材之外的有关密码算法的内容，使得学员能够参与到更多的实践环节中。在今后的教学过程中，还需要针对存在的问题，从教学内容和教学模式等方面进一步提炼和深化，促进该课程的整体教学质量继续提高。

References (参考文献)

[1] QIU Wei-dong, CHEN Ke-fei. New Interactive Model in Information Security Mathematics Teaching[J], Computer Education,2007(10),P19-21.
邱卫东，陈克非，信息安全数学教学的新型互动模式[J]，计算机教育，2007(10)，P19−21.

[2] FENG Ke-qin. views and practices on college algebra teaching[J], College Mathematics.2004,20(5),P5-7.
冯克勤，高校代数课教学的一些作法和看法[J]，大学数学，2004, 20(5)，P 5−7.

[3] LI Zhi-jun, LIAO Ming-hong. Research on Cryptography Teaching[J], Computer Education.2006(9), P18-26.
李治军，廖明宏，密码学课程的教学研究[J]，计算机教育，2006(9)，P28-30.

[4] FENG Deng-guo. Research status and trend of cryptography at home and abroad[J], Journal on Communications. 2002, 23(5), P18-26.
冯登国，国内外密码学研究现状与发展趋势[J]，通讯学报，2002, 23(5)，P18-26.

[5] William Stallings, Cryptography and Network Security--principles and practices, Fourth Edition,[M],Beijing: Publishing House of Electronic Industry,2006.33-34.
William Stallings，密码编码学与网络安全－－原理与实践（第四版）[M], 北京：电子工业出版社，2006.33-34.