

The teaching reform exploration in discrete mathematics of information security profession

JIANG Wen-xing¹, DONG Yu-hua²

1. Tangshan Normal college, Hebei, Tangshan 063000

2. Hebei Tangshan Foreign Languages School, Hebei, Tangshan 063000

1.7786005@tstc.edu.cn, 2.dyh0420@yahoo.com.cn

Abstract: Discrete mathematics has certain theoretical abstraction and comprehensive content as one of the core courses of the basic theory in information security profession, which aims at arousing student's study enthusiasm and initiative, giving full play to the role of basic theory and promoting the healthy development of information security profession effectively by trying teaching reform.

Keywords: Discrete mathematics; Information security; Teaching reform

信息安全专业中离散数学教学改革探索

蒋文星¹,董玉华²

1. 唐山师范学院, 河北唐山 063000

2. 河北唐山外国语学校, 河北唐山 063000

1.7786005@tstc.edu.cn, 2.dyh0420@yahoo.com.cn

摘要: 离散数学作为信息安全专业基础理论的核心课程之一,具有一定的理论抽象性并且内容广泛,通过尝试教学改革,调动学生的学习积极性和主动性。充分发挥基础理论课的核心作用,有效促进信息安全专业的健康发展。

关键词: 离散数学; 信息安全; 教学改革;

1. 引言

离散数学是近几十年来产生的一门新课程,是计算机以及信息安全专业基础理论的核心课程之一。学生对这门课程掌握的好与坏,将直接影响学生的专业成长。但是该课程具有一定的理论抽象性并且内容广泛,导致实际教学中会出现课时量安排与教学内容不匹配的矛盾,学生学起来感觉抽象难懂。再加上如果按照数学专业课的传统教法(只重理论教学,与实际联系不紧密),学生又会感觉离散数学只是单纯理论与信息安全专业相距甚远,学生的学习积极性和主动性得不到有效促进。为了解决这一问题,笔者在教学过程中结合信息安全专业知识定位,在离散数学教学过程中,进行了教学内容的调整、教学方法的改进、教学手段多样化处理,这些有益的探索,收到了良好的教学效果。

2. 调整教学内容为专业服务

信息安全专业人才要求掌握计算机软、硬件加密;

计算机维护和系统支持的基本理论、知识和技能,具备信息安全防护与保密等方面的理论知识和综合技术。作为该专业的核心课程,离散数学整个内容体系都是围绕计算机可以接受和处理的数据对象展开研究,并随着信息科学的发展而逐步发展、逐步完善和逐步深入的。

离散数学的基本教学内容包含数理逻辑、集合与关系、代数结构、图论四部分。在教学中紧密联系信息安全专业内容,互相渗透,让学生理解离散数学在信息安全专业课程中的应用,克服数学教师只讲数学,专业教师只讲专业的弊端。

比如,把离散数学中的数理逻辑教学与信息安全专业培养逻辑推理能力结合起来;把离散数学中的集合与关系教学和信息安全专业中的软件工程、数据库结合起来;把离散数学中的代数结构教学与信息安全专业中的信息安全、现代密码学、通信原理等结合起来;把离散数学中的图论部分教学与信息安全专业中的数据结构、操作系统等结合起来,多科目教师集体探索,系统施教,使学生的基础理论和专业成长共同

推进。

3. 改进教学方法，使抽象问题具体化

按照数学课堂教学的惯例，一般为复习旧知识，引入新内容。为了使抽象的理论相对具体化，按照教学内容的相互匹配，选取适当的专业问题提出来，调动学生探索情绪，使师生共同融入到学习中来。

实际上就是随着学习的深入，可以将一些信息安全领域的例子数学模型化提出来，引导学生到离散数学中去寻求答案。使学生理解离散数学的抽象是相对的，只要能够和实例联系起来，理解和认识相对比较容易。

比如，离散数学中的模运算与信息安全技术中加密运算联系起来后，就可以联想到凯撒密码就是建立在 26 个字母之上字母与 Key 运算的剩余模群；再如，信息安全认证技术中的数字签名，能起到电子文件认证、核准和生效的作用，其实现方式是把散列函数和公开密钥算法结合起来，在实际运行过程中就有可能出现散列函数碰撞，导致签名识别正确，身份却可能是错误的，这就能够激起学生进一步研究函数的欲望；我们还可以在入侵信息检测技术中找到一些模式匹配、完整性分析的小例子运用到离散数学的具体教学中，帮助学生理解抽象概念。

4. 注重教学手段的多样化，提高趣味性、启发性

信息安全专业学生计算机水平相对较高，动手能力较强，我们应该充分利用这一优势，在教学中破除数学教学中以板书、PPT 为主的传统教学模式。一是要充分利用多媒体技术，增大课堂教学容量，提高课时利用率；二是引入计算机试验验证，提高数据科学

合理的直观性；三是结合应用实例教学，提高传统理论课与专业技术课间的衔接；四是利用典型启发性问题教学，培养学生敏锐的观察力。

例如，离散数学中的格尼斯堡七桥问题、邮递员投信线路问题、排课问题等，与信息安全技术中文件完整性检查、统计分析等思路相通；再如任勋益博士采取的在教学中增加安全编程上机的要求，发挥学生已经掌握的信息安全相关的很多算法都比较成熟的优势，要求学生将其解读分解，并把与离散数学相关的部分抽取出来，然后对其过程进行分析，改变参数，重新调试运行，起到了事半功倍的教学效果。

5. 结语

随着信息量的逐渐增大，安全威胁也越来越大，社会对信息安全技术要求也越来越高，其重要性也在逐渐增强。离散数学作为信息安全专业的核心基础课，理论内容将会越来越多地应用到计算机及信息安全中去。今后对离散数学的教学改革探索也会进一步展开，并得到更多教师的关注。

参考文献：

- [1] GENG supping, QU wanling, Discrete mathematics [M]. Higher Education Press, Beijing, 2004.
- [1] 耿素云, 曲婉玲. 离散数学 [M]. 北京: 高等教育出版社, 2004.
- [2] Ren xunyi, Discrete mathematics and computer security with teaching, Software guide, 2009(12).
- [2] 任勋益, 离散数学与计算机安全结合改进教学, 软件导刊, 2009 (12).
- [3] Wang jinyu < Discrete mathematics > Teaching methods of thinking[J], Zhongshan university journals, 2004(5).
- [3] 王锦玉. 《离散数学》教学方法之思考 [J]. 中山大学学报论丛, 2004 (5).