

A through information security course system based on knowledge module

Xie Xie

*School of Telecommunications and Information Engineering, Xi'an University of Posts and
Telecommunications, Xi'an 710061, China
xiexiexx@xupt.edu.cn*

Abstract: Modeled with Computing Curricula, a through information security course system based on knowledge modules is constructed, whose main threads are discretization, computation and security. The teaching practice shows that our course system has good effects.

Keywords: template; knowledge module; information security; course system

基于知识模块的贯通式信息安全课程体系

谢颢

西安邮电学院 通信与信息工程学院, 陕西 西安, 中国, 710061
xiexiexx@xupt.edu.cn

【摘要】借鉴 Computing Curricula 的思路, 以“知识模块”为基本要素, 以“离散”、“计算”和“安全”为主线, 构建了贯通式的信息安全课程体系。教学实践表明, 该课程体系的教学效果良好。

【关键词】Computing Curricula; 知识模块; 信息安全; 课程体系

1 引言

我国于 2001 年批准设置在有条件的高校开设信息安全专业, 目前全国开设信息安全本科专业的高校仅 80 余所, 而该专业所涉及教学内容较新, 国内外一直都在探索如何更好地培养信息安全专业人才, 但尚未找到较为合理的专业培养模式。由于目前信息安全专业的教学研究还不太多, 而且国内开设信息安全专业的高校在其学科建设的认识上也没有达到共识, 基本上按各自的基础条件和师资力量来建设该专业, 少数高校的一些成功经验其普适性也不够。西安邮电学院于 2004 年开始信息安全专业本科生的培养工作, 在如何培养出适应市场需要的信息安全专业型人才方面进行了一定的探索, 特别是课程设置体系上作了一些有益的尝试, 也取得了一定的成果。

考虑到信息安全专业与计算机科学、通信技术、网络技术、数学等学科联系紧密, 所以应借鉴与之相

关学科课程设置的成功经验。此外, 我们在完成信息产业部软科学计划项目“我国信息安全产业可持续发展研究”过程中, 通过调研走访积累了一些信息安全企业的科研和人才需求信息, 并结合自身的办学特点和学科特色, 形成了较为有效的信息安全专业的课程设置体系。经过若干届学生的教学实践, 我们逐步形成了以知识模块为基础、以“离散”、“计算”和“安全”为主线的贯通式课程体系。

2 基于知识模块的课程设置

传统的教学课程模块仅在大的思路规划了各种课程之间的联系和次序, 特别是模块之间的次序衔接。由于模块设置较大, 包含课程较多, 只能在宏观上界定课程之间的关系, 难以在微观上构造其知识内容的内在次序。如果模块的设计不恰当, 往往会造成知识内容的重复讲解或疏忽遗漏, 而且需要更为细致的设计与调整才能弥补, 尤其是在学时精简的现状下更需要优化知识结构和内容, 不但耗时耗力, 教学效果也会大打折扣。

资助信息: 本文得到西安邮电学院“信息安全专业特色建设的教学改革研究”项目支持。

国内外对课程模块设置问题已有初步的研究，而其中的佼佼者就是 IEEE-CS 和 ACM 制定的 Computing Curricula (简称 CC) [1]，这是为计算机科学与技术方面的教学与课程设置的经典参考方案，国内的《中国计算机科学与技术学科教程 2002》则是模仿 CC2001 的教学体系。CC 最初于 2001 年为计算机专业而设定 (简称 CC2001)，尔后 IEEE-CS 和 ACM 对其不断修订，形成了 5 个不同的分支：计算机科学部分的 CS2008、计算机工程部分的 CE2004、信息系统部分的 IS2002 与 MSIS2006、信息技术部分的 IT2008 和软件工程部分的 SE2004。令人遗憾的是，其它专业尚无类似的大型教学改革工程，主要是因为该项工作内容庞杂，耗费财力较大。

经历了多年的发展，CC 中的各个模块基本固定，其中与信息安全相关的典型模块有：DS、PF、AL、AR、OS、NC、SE、IM 等。CC 的特色是每个模块中由若干部分组成，不妨称之为“知识模块”，所有教学方案就是这些知识模块的合理安排和组合，而这正是我们需要解决的核心问题。

信息安全专业与 CC 有一定的重叠，借鉴 CC 思路有助于教学培养方案的设置乃至教学体系的改革。不过信息安全专业自身的特色鲜明，而且对理论和实践要求都非常高，特别是密码学为主体的一系列课程群，这对教学内容和课程设置提出了新的要求。我们在教学实践中针对信息安全专业的特点，以密码学为核心，精心设置了课程的知识模块，收效甚好。例如在算法类课程中加入了大数的运算和 GMP 库的相关知识模块，这样为后续的课程打下了很好的基础，学生学到这些知识有利于密码学的学习与掌握。

3 课程体系的“离散”主线

在 CC 中首先提到的就是“离散结构”(Discrete Structures, DS)，而信息安全专业也非常重视离散化的思想，这方面的体现是数学和信息论等课程。以“离散”形式讲授更为贴近信息安全专业的特色，而离散数学和信息论中的实例丰富，能够更好地让学生体会到“离散”这一思想的重要地位。

我们已对 CC 关于 DS 部分的课程体系作了一些讨论 [2]，它们同样适用于信息安全专业，这部分内容对应了《信息安全数学基础 I》课程。我们仍然特别强调“离散概率”的重要性，因为对于信息安全专业而言，“随机”这个概念更为重要，特别是在“现代密码学”中更是不可或缺的基石。我们将国外大学已经单

独开设的《概率与计算》课程 [3-5] 中的内容加以精选，补充到《信息安全数学基础 I》课程中，特别是概率算法的一些数学基础，并给出了常见的随机数生成算法。

数论的相关知识同样依照“离散”这条主线设置，这部分内容主要讲解一些计算数论的基本知识和内容，并配合抽象代数与数论的交叉融合，形成了《信息安全数学基础 II》课程。通常的课程内容安排是讲授初等数论知识过多，而较少涉及到计算数论，我们尝试讲解一些计算数论的简要成果，以期让学生更多地体会到其应用。

以“离散”为主线的信息论课程是我们的一个有益的尝试。信息论是信息科学诸多专业的一门专业基础课程，为信息安全专业开设的信息论应该突出其关注点，即 Shannon 理论、算法信息论和密码的信息理论，它们均可用“离散”串接。在此基础上，我们将信息论课程分解为若干知识模块，精选内容、注重实用，收效甚好。

4 课程体系的“计算”主线

在信息安全的课程体系中，计算机科学与技术相关的课程占有一定的比例。尽管 CC 给出了良好的模块设置，但我们需要根据信息安全专业的特色予以改进。

在具体的教学实践中，我们主要针对最重要的 Algorithms and Complexity(AL)部分进行改革。近年来，我们为学生开设了《信息安全算法基础》，专门优化了知识模块，其目的是直接为后续的《密码学基础》和《安全协议》服务。《信息安全算法基础》强调 ADT 的原理、应用和组合，弱化关于 ADT 实现的教学内容。在选用不同数据结构和实现时，以实际需求和 ADT 的性能为准绳，并在整体上从分摊复杂度来考察应用程序，培养学生对程序设计精益求精的态度。实践证明，学生非常适应这样的教学方式，不但易于入门，还能激发他们的学习兴趣。

在知识模块的设置上，《信息安全算法基础》包含 CC 的如下知识模块：

PF/AlgorithmicProblemSolving
PF/DataStructures
PF/Recursion
AL/BasicAnalysis
AL/AlgorithmicStrategies
AL/FundamentalAlgorithms

AL/BasicComputability

AL/CryptographicAlgorithms

此外,《信息安全算法基础》特别关注散列、数论算法实践、代数算法这3方面,主要要求学生能掌握散列函数设计、基于GMP的算法和代数算法的下界证明等内容,这样不但与前面的《信息安全数学基础》紧密地结合,还为后续课程给出了合适的铺垫。

在《信息安全算法基础》的教学中,我们特别注重理论功底的培养,例如算法分析、计算理论的相关内容。尽管这些内容难度较大,但学生通过学习它们可对学科有更深入的了解,更可为今后的工作学习打下坚实的基础。

5 课程体系的“安全”主线

对于信息安全专业,我们的主要专业课安排是:

《信息安全概论》、《网络安全基础》、《密码学基础》、《安全协议》、《网络安全技术》和《通信网安全》。在这个体系中,我们以《密码学为基础》为指导,以《安全协议》为桥梁,配以《网络安全基础》和《网络安全技术》,并着重介绍了邮电院校的特色课程《通信网安全》。

以《通信网安全》课程为例,该课程要求学生学习现代通信网的主要理论,掌握现代通信网的基本概念和工作原理,特别是结构、协议和业务,并在此基础上学习通信网安全的基本分析和防御技术。学生学习本课程后能对目前的公众通信网络有所理解,对此类通信网络传递信息所面临的问题有所认识,特别是能了解目前为加强通信网的安全所采用的技术。由此可以看出,《通信网安全》不但具有通信课程的背景,还体现了信息安全大部分先修课程的应用,这样不但为学生今后的学习提供了公共背景知识,还对他们信息安全工作的开展有启发性的作用。

6 教学效果与教学成果

我们在信息安全专业的教学实践中,坚持以知识模块为核心元素,以贯通式为主要指导思想,取得了较好的教学效果。通过以知识模块组合方式来组织的课程设置体系,不但能保证教学内容的前后衔接,还能优化课程内容,且容易修改、难以遗漏和重复,这充分体现了知识模块的完整性与灵活性。

教学质量的直接体现是学生的学习效果,学生普遍反映新的课程体系与教学模式更有目的性、针对性,学习兴趣不断提高,能力也得到加强。在2009年的大学生信息安全竞赛中,西安邮电学院获得全国二等奖一组,全国三等奖一组,实现了较大的突破。在学科竞赛中需要多种知识内容的组合,我们提前组织教师对“知识模块”进行一定的讲解,保证了学生参加竞赛的知识能力储备。

教材是教学质量的另一面镜子,我们已出版由西安电子科技大学出版社组织的《密码学基础》教材,并将于2010年在北京大学出版社出版《离散信息论基础》教材。目前的教材编写以核心课程为导向,已经体现了知识模块划分思路,计划对信息安全专业其它课程按知识模块组织编写成书。

References (参考文献)

- [1] Computing Curricula.
<http://www.acm.org/education/curricula.html>
- [2] Xie Xie, Ming Fang. Mathematical education in computer science. Computer Education, 2008, 14: 144-146. (In Chinese)
谢颢, 方明. 计算机科学中的数学教育 [J]. 计算机教育, 2008, 14: 144-146.
- [3] Probability and Computing, CMU Course 15-359.
<http://www.cs.cmu.edu/~15359/>
- [4] Probabilistic Methods in Computer Science, Brown Course CS 155. <http://www.cs.brown.edu/courses/cs155/>
- [5] Michael Mitzenmacher, Eli Upfal. Probability and Computing: Randomized Algorithms and Probabilistic Analysis. Cambridge University Press, 2005.