

ISSN 1671-024X
CN 12-1341/TS

天津工业大学学报

JOURNAL OF TIANJIN POLYTECHNIC UNIVERSITY

中文核心期刊 · 中国科技核心期刊 · RSSEC核心期刊



第35卷 Vol.35

2016 增刊

TIANJIN GONGYE DAXUE XUEBAO

高压钠灯电子镇流器的研究	刘小飞,高圣伟,张 梦,李 强,王 宏,娄贵鑫(116)
采用谐波电流注入法减小改进变压器电路中的储能电容	
开放实验室智能监控系统设计	张 梦,高圣伟,刘小飞,李 强,王 宏,娄贵鑫(120)
【经济与管理】	
以提升消费文化推动服装消费升级	史凤栋,何国聪,车恒毅(123)
服装生产自动化发展现状及趋势	陈苗森,马大力,张俊霞(126)
事业单位长期不在岗人员的应对机制与处理办法	张俊霞,马大力(130)
高校学生公益组织发展机制探究	范景和,武怡欣(133)
高等院校课时费计算体系优化研究	滕堃玥(135)
高职院校视角下灰色文献的特点与流通	张 贺,毋文峰,凌云翔(138)
完善医院资金管理的思考	宋小磊(142)
【教育教学研究】	
《复合材料结构设计》实践课程建设与改革	陈翠英(144)
提高机械类专业学生创新实践能力新探索	曹伟伟,王文一,赵义平,张兴祥,纪秀杰,耿宏章(146)
应用创新型机械工程专业全日制工程硕士培养探索	杜 宇,杨 涛(149)
以照明光源为例的《机器视觉》实验教学课程探索	陈丽莎,李 博,康荣杰(151)
电气传动控制系统实验教学改革	宋丽梅,魏 泽,郭庆华,朱新军,王红一,李金义(154)
适应工程教育认证的大学生辅导机制探索	蔡 燕,姜文涛(157)
电气类专业特色人才培养模式创新与实践	修春波(160)
通信工程专业实践教学体系的研究与实践	刘晓明,高圣伟,李 阳,谷 鑫(162)
《电力电子技术》课程群建设与探索	郭翠娟,武志刚,缪竞鸿,武欣桐(165)
自动化专业毕业要求达成度的评价机制	高圣伟,蔡 燕,王 炜,刘雪莉(168)
面向“工程认证”的《微机原理及应用》课程改革探索	陈奕梅,师五喜(171)
自动化专业基于 OBE 的课程体系改革	成 怡,修春波,宋丽梅,罗 菁(174)
基于工程教育认证的自动化专业培养目标的制定	罗 菁,陈奕梅,修春波,成 怡(177)
虚拟仿真技术在纱线卷绕机实验教学中的应用	田慧欣(179)
纺织综合自动化实践与复杂工程问题典型案例设计	赵永立,李丹丹,杨建成(182)
基于创新型人才培养为目标的创新创业教育体系研究与实践——以机电工程专业为例	陈云军(184)
基于 OBE 理念的《模式识别导论》网络课程平台建设	刘国华,岳建锋(187)
面向卓越工程师培养的线切割项目教学实践探究	王红一,宋丽梅(189)
《电力电子技术》教学中融入工程问题复杂性分析的改革探索	淮旭国,刘 健,张彦春(192)
基于项目式实验教学的微控制器结构与应用课程实例	李宝全,成 怡,修春波,宋丽梅(195)
信计专业《网络与信息安全技术》教学改革研究	姜文涛,蔡 燕,张海华(197)
虚拟仿真技术在纺织机械实验教学中的应用	赵 璐,张 霞,王国庆(202)
高校创业教育现存问题探析	李丹丹,杨建成,赵永立(204)
大学生单片机创新实验室人才培养模式的实践与探索	郭 兵(206)
大学生工程实践能力提升的探索	李春婵,熊 慧,刘进贞,涂丽平,沈振乾,史凤栋(209)
大学生思想政治教育中的生态文明教育	韩丽丽,修春波(212)
高校宣传思想工作抓住学生的新途径	成 煦,孙 哲(214)
基于 O2O 的混合教学模式研究——以“C 语言程序设计”教学为例	裴 蕾(217)
关于大学生课余时间使用情况的调查研究——以天津工业大学为例	马 菲(221)
.....	
.....	李 兰,原 平,李艳琦,杜玉红,姚福林,史 华(223)

信计专业《网络与信息安全技术》教学改革研究

赵璐, 张霞, 王国庆
(天津工业大学理学院, 天津 300387)

摘要: 在总结以往《网络与信息安全技术》课程教学经验的基础上, 结合我校信计系开设课程的实际情况, 通过分析教学中存在的问题, 本文从教学内容、授课形式和考核方式三个方面进行改革, 力求建立教学新模式, 激发学生的学习兴趣, 全面提高学生的应用实践能力。

关键词: 信计专业; 网络与信息安全技术; 课程建设; 教学改革

中图分类号: TN911.2

文献标志码: A

文章编号: 1671-024X(2016)增刊-0202-02

计算机技术的快速发展促进了网络技术的迅速发展和广泛应用, 信息化已成为当今世界发展的主要趋势, 也是衡量一个国家现代化水平的重要标志。信息科学可以理解为信息获取、传输、处理与控制的科学。我国信息科学发展的时间相对较短, 但发展迅猛。随着信息技术的发展, 信息安全的重要性日渐凸显。通过网络传输或获取信息, 已从军事、政治、外交等重要领域日益普及到人们日常生活的各个领域。因而, 保障信息在网络传输的过程中不受各种干扰破坏或不发生泄露, 亦成为当今信息时代的一个重要问题^[1]。

教育部1998年颁布的普通高等院校专业目录中, “信息与计算科学专业”被列为数学类下的一个新专业。这一新专业的设置很好地适应了新世纪以信息和计算技术为核心的数学人才的培养。按照教育部发表的《信息与计算科学专业教学规范》, 信息与计算科学专业是以信息技术和计算技术的数学基础为研究对象的理科类专业。其目标是培养学生具有良好的数学基础和数学思维能力, 掌握信息与计算科学基础理论、方法和技能, 能解决信息科学与工程计算中实际问题的高级专门人才^[2]。天津工业大学理学院在国内较早地开办了信息与计算科学专业。为了配合教育部制定培养目标, 信计系开设了《网络与信息安全技术》课程, 向学生介绍信息安全及密码学的相关知识, 为今后学生从事信息安全方面的研究及工作打下坚实的基础。

本文结合我校信计系专业开设《网络与信息安全技术》课程的实际情况, 分析教学中存在的一些问题

与不足, 分别从教学内容选择、考核方式及授课方式等三方面进行课程改革探索。

1 信计专业《网络与信息安全技术》课程教学中存在的问题

通过分析近几年企业招聘信息安全方面人才出的相关要求, 总结往年《网络与信息安全技术》课程教学的情况, 我们发现课程教学中主要存在以下方面的问题:

(1) 《网络与信息安全技术》课程涉及面广, 内容不充足, 不能为学生做全面系统的介绍。本门课程讲授信息安全和密码学的基本知识, 主要包括古典密码、分组密码、序列密码、公开密钥密码、数字签名、HASH函数、秘密共享及零知识证明等几方面内容。课程内容丰富, 课时相对较少, 导致我们只能在上述内容中挑选一些经典密码体制和密码协议进行介绍。无法对密码学进行深入系统的讲解。

(2) 《网络与信息安全技术》课程在学习时要要求学生具有较强的数学功底。上述提到的课程内容要求学生掌握并能够应用数论、代数学及有限域等相关知识, 但是这已经超出了信计系本科生在数学方面的学习范畴, 因此成为了《网络与信息安全技术》课程学习的一大难点。为了克服这一困难, 往年在教学中, 我们要安排大量的课时对学生进行相关数学知识的讲解。这对课时本不充裕的课程讲授来说, 无疑是雪上加霜。

(3) 《网络与信息安全技术》是一门具有很强的

收稿日期: 2016-04-10

基金项目: 天津工业大学高等教育教学改革研究项目(2014-2-29); 天津工业大学重点教学改革研究项目(2014-1-31); 天津市普通高等院校本科教学质量与教学改革研究计划重点项目(D02-0701)

通信作者: 赵璐(1984—)女, 讲师, 博士, E-mail: zhaolu@tjpu.edu.cn

性的课程,传统的“讲授”模式不能培养学生的实践能力。近几年,企业招聘信息安全方面人才时注重对毕业生在安全算法的实现和研究等方面能力的考察,这就对《网络与信息安全技术》课程的教授提出了新的要求:在讲授密码学基本知识的同时,要培养学生对算法的实践能力以及能够运用所学知识解决实际问题的能力。然而,我们传统的“老师讲,学生听”的教学模式,不能培养学生的相应能力,不能为我们的学生在应聘或考取信息安全方面研究生的时候增加优势。

(4) 以往教学内容无法让学生了解信息安全研究的前沿成果。随着信息技术的广泛应用,密码学的发展日新月异。但是通常信息安全类的教材都是对经典的密码体制、密码协议和密码算法进行介绍,这些无法让学生了解密码学的研究前沿。例如,量子密码是密码学的一个重要研究方向,但是此方面的技术还大多处于实验室阶段,距离应用阶段还需较长时间,因此很多信息安全类教材都未涉及此方面的内容。

综上所述,为了能全面解决上述问题,我们将从教学内容、授课形式和考核方式三个方面进行调整,力求建立《网络与信息安全技术》教学的新模式,促进教学深化改革,使我们的课程能为学生的就业和深入学习打下良好的基础,让学生在应聘及考研中可以脱颖而出。

2 《网络与信息安全技术》课程教学改革的探讨

2.1 优化教学内容,解决入门难和课时少的问题

在前面的分析中已经提到,本门课程需要学生具备数论、代数学及有限域等相关数学知识,为了克服这一困难,信计系开设了《信息安全数学基础》专业类课程,并由专业教师为学生授课,解决了学生在《网络与信息安全技术》学习中出现的入门难的问题。此外,本课程的课时较短,无法将密码学中的所有问题进行讲解,因此我们对课程设置也进行了调整。我们选用最新的信息安全类教材^[1],以适应密码学日新月异的发展。对目前应用广泛的密码体制、算法或安全协议进行详细讲解,对一些影响程度不大,或者应用范围不广的密码体制或算法,只做简单的介绍。此外,我们还会为学生提供一些补充阅读的文獻,作为对密码学有兴趣的学生或者有意从事信息安全工作的学生的自学内容,以此扩大知识面。

2.2 改进授课方式,增添课程趣味性,培养学生应用能力

我们将在授课过程中通过故事、新闻报道等形式向学生介绍现代密码学的基础知识和技术,内容紧贴

学生的学习和生活,并制作生动的PPT课件,将密码体制、算法的流程更形象生动地展现在学生面前,力求打破原有的充斥着繁杂抽象数学符号的密码学教学方式,让学生领悟到现代密码学的原理及应用场景,了解实际信息安全问题的解决方法,增加课程的趣味性,激发学生对现代密码学的浓厚兴趣,引领学生走进现代密码技术之门。

如前所述,企业在招聘信息安全方面人才时注重对毕业生动手能力的考核。我们将鼓励学生利用课余时间走进实验室,将一些经典的密码算法进行编程实现。本门课程将会委派专门的教师为学生提供编程指导,培养学生的实践能力,为学生的就业应聘与深入学习打下坚实的基础。

我们将会不定期地邀请一些国内的相关专家以讲座的形式,为信计系的教师和学生介绍密码学最新的研究成果和当前的研究热点,引导学生了解密码学领域及信息安全领域的新进展和新方向,开阔学生的视野,让学生在美妙的密码世界里享受着科学家的智慧,体验数学应用之美^[2]。

2.3 采用多种考核方式,培养学生的创新能力

除了传统的试卷考核之外,我们将选定一个密码学的研究热点问题,要求学生以小组为单位提出解决方案,对安全性进行初步分析,提交研究报告并计入期末成绩。我们希望以此种方式可以培养学生的灵活思维和团队协作意识,以及一定的研究、开发和创新能力。

3 问题与反思

我们希望通过课程的改革,使课程变得生动、有趣,激发学生的学习热情,力求信计系的学生不仅能掌握信息安全的基础知识,对信息安全有初步的认识,而且能为今后从事信息安全方面的工作或研究打下坚实的基础。但是,以上的思路和措施仅是我们在课程教学改革中迈出的第一步。今后,我们会继续总结教学中的经验,不断创新,争取使《网络与信息安全技术》成为具有信计系特色的专业课程。

参考文献:

- [1] 章照止. 现代密码学基础[M]. 北京:北京邮电大学出版社, 2004.
- [2] 徐茂智,游林. 信息安全与密码学[M]. 北京:清华大学出版社, 2007.
- [3] 谷利泽,郑世慧,杨义先. 现代密码学教程[M]. 北京:北京邮电大学出版社, 2015.
- [4] 彭长根. 现代密码学趣味之旅[M]. 北京:金城出版社, 2015.