

基于网络平台的混合式教学法在密码学教学中的效果评价

吴万青, 杜瑞忠

(河北大学网络空间安全与计算机学院, 河北 保定 071002)

摘要: 针对密码学课程的特点, 通过网络平台设计了混合式教学法。为了得到教学的实施效果, 从“教学方法、教学内容、教学态度、教学环境、综合评价”5 个方面进行评价。评价结果显示使用混合式教学法以后, 学生的学习效果得到了提高。反馈结果提示我们: 要不断地优化教学内容、教学方法; 提高课堂掌控能力, 引导学生学习; 团队合作提高效率, 降低授课教师强度。这些结果为进一步提高密码学课程实践教学提供有用帮助。

关键词: 混合式教学法; MyCOS 教学质量管理平台; 密码学教学; 教学效果评价

中图分类号: G642

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2019030

Evaluation of blended instruction based on network platform in cryptography teaching

WU Wanqing, DU Ruizhong

School of Cyber Security and Computer, Hebei University, Baoding 071002, China

Abstract: According to the characteristics of cryptography course, a hybrid teaching method was designed through the network platform. In order to get the implementation effect of teaching, the evaluation is made from five aspects: teaching method, teaching content, teaching attitude, teaching environment and comprehensive evaluation. The evaluation results show that students' learning effect is improved after using the blended teaching method. The feedback results suggest that we should constantly optimize the teaching content and teaching methods; improve the ability to control the classroom, guide students to learn; teamwork can improve efficiency and reduce the intensity of teachers. These results provide useful help for further improving the practical teaching of cryptography.

Key words: blended instruction, MyCOS teaching quality management platform, cryptography teaching, evaluation of teaching effect

收稿日期: 2019-03-23; 修回日期: 2019-05-16

通信作者: 吴万青, wuwanqing8888@126.com

基金项目: 河北省自然科学基金资助项目 (No.F2017201199); 河北省研究生示范课程和专业学位教学案例(库)建设基金资助项目 (No.KCJSX2018005)

Foundation Items: The Natural Science Foundation of Hebei Province (No.F2017201199), Graduate Demonstration Courses and Professional Degree Teaching Cases (Library) Construction Project of Hebei Province(No.KCJSX2018005)

论文引用格式: 吴万青, 杜瑞忠. 基于网络平台的混合式教学法在密码学教学中的效果评价[J]. 网络与信息安全学报, 2019, 5(3): 96-101.

WU W Q, DU R Z. Evaluation of blended instruction based on network platform in cryptography teaching [J]. Chinese Journal of Network and Information Security, 2019, 5(3): 96-101.

1 引言

随着我国信息化工作的不断深入推进,“互联网、云计算、区块链、大数据”等技术的发展,互联网正成为我国未来经济社会发展的重要推动力量。快速发展的信息化网络社会同时给人们的生活带来了巨大的影响与变革。同许多社会行业一样,教育行业也受到了信息化带来的各种影响。基于互联网的各种信息化技术的出现对我国传统的教育理念和方式不可避免地带来了挑战。如何适应新形势下的变化,有效地促进教育服务水平和提高教育质量,是摆在广大教育人员面前的一个重要课题。

高等教育承担着为社会培养优秀人才和智力支持的责任,同时也是产生新的科学技术的重要手段。高等教育处在教育行业的龙头,高等教育的信息化程度也是各类教育中最高的。在管理方面,所有的高校都建立了学校网站。大多数高校利用校园网络建立了电子邮件系统、电子办公系统等。在教学方面,大部分高校建立了不同程度的资源库。大量多媒体设备的购入、装备,慕课、翻转课堂、远程教育等信息化技术手段的大范围使用,为新教学法的探索和实施提供了良好的物质基础。目前我国大部分高校已经建立了较好的信息化应用体系。

2015年6月,为实施国家安全战略,国务院学位委员会和教育部联合下文,批准设立网络空间安全一级学科。截至2018年,全国共有122所高校开设了网络空间安全相关专业。这些高校成为我国信息安全人才培养的主要基地。密码学课程是信息安全专业的重要必修课之一,在信息安全人员培养方案中占据很重要的地位。目前各高校对密码学课程的教学方法改革、内容的设置及教材的建设进行了探索,取得了一些成果。但密码学课程是数学、计算机、通信、管理等多学

科交叉的产物,它既具有深入的数学理论基础,又具有很强的动手实践性^[1]。这些特点导致在密码学课程的教学普遍存在学生难学、教师难教、学生兴趣不高的现象^[2]。因此,如何协调理论与应用实践之间的关系以及如何合理组织教学,值得进一步探索改进。

河北大学自2015级设立信息安全专业开始,就将密码学课程列为信息安全专业的核心课程。在此背景下,为了提高密码学课程的授课质量,结合应用日益广泛的网络化平台,河北大学采用了混合式教学方法进行密码学课程的教学。本文结合河北大学信息安全专业密码学课程的教学经验进行探讨,并给出相关的教学总结和评价反馈,为信息安全人才的培养贡献一些经验和思考。

2 混合式教学法的定位和平台构建

2.1 教学定位

课堂讲授法是我国高等教育目前主要采用的教学法。课堂讲授法具有成本低、效率高、目的性强、通用性强的优点,但同时存在学生思维学习被动、不利于记忆等缺点,由于我国高校教育资源不足,优质资源紧缺的现状将长期存在,高校师生比例过大的现状不能在短期内改变。另外,我国高等教育资源的分配还是以应试教育为依据的,这些特点正是课堂讲授法的优势。虽然近年来出现了诸如慕课、微课、翻转课堂等新的教学模式,但它们都有各自不同的适用范围,并且没有从根本上代替课堂讲授法的主体地位。

混合式教学是指对所有的教学因素进行合理优化和组合,以达到教学目标的活动。具体地说,就是在教学的开展过程中,将各种教学方法、教学策略、教学模式、教学技术等教学因素进行有机结合并熟练运用,最终达到混合学习的目的,如课堂学习环境 with 网络学习环境的混合^[3]、多种学习的评价方法混合^[4]等。本文建立的基于网络

平台的混合式教学方法,在教学定位上仍坚持以课堂教授法为主、在线自助学习为辅的混合学习模式。授课教师根据教学的实际内容、教学目的选择恰当的教学方法,引导学生利用网络平台进行不同形式的学习。

具体地说,基于网络平台的混合教学学习模式是将传统的教学模式和网络模式进行合理安排,构建特殊的教学过程帮助学生在学习。在教学内容上围绕原定计划展开,通过网络平台对学生线上反馈、线下反馈调整教学环节的各个因素,以利于学生的个性学习。例如,可以通过网络平台线上或线下进行动态动画演示算法加密过程以利于学生理解和复习,这在传统教学中是无法展示的;还可以通过机械主义学习理论建构的问题反馈学习模式,通过实时掌握学生的学习效果做出调整,增加训练量等活动。

2.2 网络平台的构建

河北大学采用的是 MyCOS 教学质量管理平台,如图 1 所示,其用户分布 600 余所高校。该平台以课程教学为中心,利用网络进行教学管理的数字化环境,实现了教学过程的信息化,可以采用 PC 浏览器和手机等移动终端进行线上和线下的学习与管理。该教学平台由多个模块构成,主要包括教师上课信息及评价、课程问卷反馈、智能助教等。

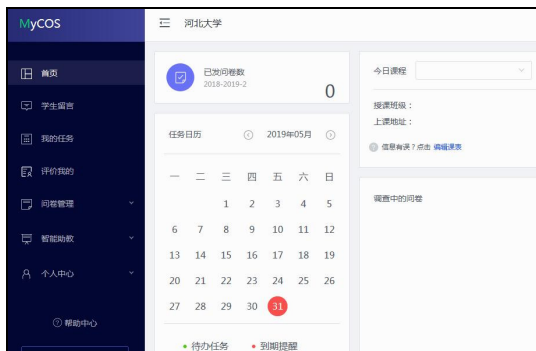


图 1 平台全局菜单展示

1) 教师上课信息及评价:教师在上课之前

需要建立课表、导入与课程相关的内容,使学生明确这堂课的内容、目标等。

2) 课程问卷反馈:教师在上课前设计好这堂课的教学目标、采用的教学模式、板书及 PPT 设计等。在设计教学效果问卷调查时,通过“综合评价、教学方法、教学内容、教学态度、教学产出、教学环境”6 个方面进行评价和反馈。学生对该堂课的及时反馈可以帮助教师了解学生的学习状况,从而改进课程,帮助学生更好地理解知识。

3) 智能助教:教师可以利用平台的辅助手段进行课前指导,课堂讲课资料展示及反馈、课堂交互,课后复习及作业评阅。尤其针对学生的个性化学习起到帮助作用,这是对目前以讲授法为主的教学方法的有效补充。

3 基于网络平台的混合式教学设计与评价

3.1 教学任务设计

《高等学校信息安全专业指导规范》^[5](以下简称《规范》)是我国信息安全领域人才培养的体系建设指导性规范文件。根据《规范》的要求,本科阶段的现代密码学主要包括古典密码系统、分组密码系统、序列密码系统、公钥密码系统、Hash 函数、数字签名、认证协议、密钥管理等基础内容,涉及内容广泛。学生通过这门课程的学习掌握密码学的基本概念,有利于今后的进一步学习。

密码学是一门理论性和实践性较强的课程,涉及多门学科知识,前置知识内容较多。一般应放在本科三年级左右,此时,学生已经学会计算机的相关基础知识、信息安全数学基础等理论知识,具备进一步学习的知识储备。同时,学生拥有一定的网络使用能力,可以完成教师分配的学习任务。

教学任务设计是教学实践环节的关键一步。

混合式教学包括课堂教学和线上、线下教学。传统的讲授法只能依靠教材，而基于网络平台的在线教学可以将慕课、动画、视频、课件等资源进行上传，将网络平台与讲授法结合，达到优势互补的目的，从而实现混合式教学的思想和学习方式。

下面以教学内容、教学方式为主线进行教学任务设计。在设计时要综合考虑知识的严谨性、趣味性、实用性。表 1 中给出了具体的教学任务设计。

混合式教学的评价是整个教学过程的重要组成部分。从学生的反馈中发现教学的不足，调整教学方法，有针对性地教学。对学生的形成性评价有在线自评、在线自测、教学活动评价、互评的方式。我们从“教学方法、教学内容、教学态度、教学环境、综合评价”5 个方面作为衡量指标。结合平台中提供的模块化问题模版，选择其中 12 项常用的评价指标作为形成性反馈评价，分别如下。① 同其他课程相比，你认为这门课程难度如何？② 你认为采用课件、视频等辅助手段对你的学习是否有帮助？③ 你认为教材对你的学习是否有帮助？④ 你是否同意授课教师对学生要求标准高？⑤ 你是否认为授课老师设置的任务太难？⑥ 你是否对授课教师的热情满意？⑦ 学校的设施设备是否齐备？⑧ 教师是否能营造积极的课堂氛围？⑨ 你对该课程是否有兴趣？⑩ 该

课程对你的后续学习是否有帮助？⑪ 你如何评价自己在这门课中的表现？⑫ 这门课的作业量是否合适？我们将这 12 个评价指标分配到 5 个衡量指标中，如表 2 所示。

3.2 教学反馈评价

为了获得学生对密码学课程的教学结果反馈，我们对 2015 级、2016 级本科生各一个班级展开教学效果反馈评价，参加人数均是 40 人。其中，2015 级采用传统的讲授法，2016 级采用混合式教学法，最后将两个年级的结果进行对比，结果如表 3 所示。

由于该课程是同一个教学组完成的，因此在教学态度方面变化不大，没有在表中进行说明。通过比较可知，2016 级学生对课程的满意度整体提高。在主观的多项选择中，增加密码发展的历史事例、照片、视频等材料，提高了学生对古典密码的兴趣，采用观看算法动画视频、分解课程任务等辅助教学方法增强了学生学习近代密码的兴趣。这些辅助教学方法的采用增加了教学的内容，使原本一些抽象的内容现在相对直观、易于理解。但材料、课堂教学方法的准备需要占用教师大量的课后时间，考虑到材料和内容的更新，相比单一的讲授法，这种更多时间的付出现象是持续存在的。在当前的形势下，教师是否有更多的精力投入这样的教学中也是需要考虑的。

表 1 教学任务设计		
章节名称	教学内容	教学方法
古典密码	简单密码、代换密码、置换密码	讲授为主，兴趣教学法相辅
密码系统	分组密码、序列密码、公钥密码、Hash 函数	讲授为主，动画/算法演示相辅
密码协议	数字签名、认证协议	讲授为主，慕课、任务驱动为辅
密钥管理	分组密码密钥管理、公钥密码密钥管理	讲授为主，视频、项目教学法为辅

表 2 评价指标					
衡量指标	教学方法	教学内容	教学态度	教学环境	综合评价
评价指标	②、⑫	①、③、④、⑩	⑥	⑦、⑧	⑤、⑨、⑪

表 3					教学指标评价				
2015 级					2016 级				
指标等级	A	B	C	D	指标等级	A	B	C	D
教学方法	17%	38%	40%	5%	教学方法	20%	45%	29%	6%
教学内容	5%	31%	58%	6%	教学内容	9%	41%	46%	4%
教学环境	6%	43%	34%	17%	教学环境	10%	44%	37%	9%
综合评价	8%	40%	45%	7%	综合评价	6%	50%	42%	2%

注 A：十分满意；B：满意；C：一般；D：不满意

在以讲授法为主的教学设计中，教学环境的选项学生的整体体验反而下降了。我们分析可能的原因是学生在漫长的教育过程中习惯了讲授法，对待新事物能理解也愿意接受，但无所适从者居多；另一个可能的原因是这些教学内容的增加、辅助教学法的使用使授课教师对课堂整体控制力下降。这就需要授课教师进一步引导学生自主学习。

在教学内容的反馈中，学生感兴趣的课程内容顺序是古典密码、密码协议、密码算法、密钥管理。由于古典密码在讲授时结合更多的历史事例，容易激发学生的兴趣。同时，学生对大部分的应用性内容也产生了浓厚的兴趣，尤其是通过算法动画演示活跃了课堂的学习气氛。在综合评价中，参与反馈的 2016 级同学参与度有了一定的提高，通过将课程内容以任务的形式进行分解降低了难度，并能较好地引导学生的学习，具有一定的针对性。采用项目教学法使学生参与密钥系统的管理，增强了学生的动手能力，提高了课堂上学生与老师、学生与学生之间的交互能力。

在最重要的总结性评价中，我们分析了学生的期末考试测验成绩。试卷采用百分制，试卷题目难易比按 1：3：6 分配，其中 60%是对基础知识内容的考察、30%是对基本技能的考察、10%是对知识灵活运用的考察。我们对数据计算平均值、方差并进行了 T 检测^[6]，结果如表 4 所示。

表 4 期末成绩结果比较					
	2015 级		2016 级		T 检测
	平均分	方差	平均分	方差	
成绩	76	1.44	82	1.45	3.4

通过表 4 的分析，可以得知，在进行混合式教学后，学生的平均分有了提升。经过 T 检验得到两个班的差异值小于 0.001，表明数据存在显著性差异。这说明采用混合式教学有利于学生的学习。通过卷面分析，2016 级学生的基础知识掌握情况相对以前有了一定提高，同时中等题目、高难度题目的得分率也有不同程度的提升。

通过纵向对比，发现学生的学习兴趣、学习效果、业绩评价都有所提高，这些反馈结果给我们带来了一些启示。

- 1) 适当采用一些新的教学方法。密码学的教学一直存在抽象、难以理解的现象，单纯依赖讲授法不能提高学生的学习效率，需要授课教师不断探索新的教学模式。同时，讲授法的地位没有受到动摇，不能为了追求改革而改革。
- 2) 增强授课内容的应用性。随着技术的不断进步，一些密码学的知识内容和技术显得落后于发展，这需要授课教师关注密码学理论和技术的最新进展，将最新的成果引进课堂。同时结合企业和社会的需求，补充更多应用相关的内容，缩短人才培养的知识储备与社会、企业需要的差距，实现学生与工作岗位的对接。

3) 增强与其他学科的联系。密码学是一个多学科的交叉学科,跟其他学科有着密切的联系,授课教师可以根据学院学科建设特点加强与相关学科的联系。

4 结束语

基于网络平台的混合式教学有利于针对不同的知识内容进行特定的教学。本文以密码学课程为例,探讨网络平台、传统教学模式相结合的教学模式在人才实践教学改革方面的影响。为了评估和反馈混合式教学的效果,对比了两届学生的学习和考试情况。从反馈结果得知混合式教学的多元化有利于学生成绩的提高,但同时降低了学生的课堂体验,容易给学生带来倦怠感,这需要授课教师积极引导。在教师的反馈中,教师觉得混合式教学中教学工作压力变大,需要投入更多的精力,可以通过平台模块化、团队合作的模式提高效率,以降低教师的工作强度。这些工作和总结为我们进一步完善密码学课程实践教学体系提供了有用帮助。

参考文献:

- [1] 张焕国,唐明. 密码学引论(第三版)[M]. 武汉:武汉大学出版社,2015.
ZHANG H G, TANG M. Introduction to cryptography (third edition) [M]. Wuhan: Wuhan University Press, 2015.
- [2] 王后珍,张焕国. 密码学课程建设及教学方法探讨[J]. 高教学刊, 2016(7):78-79.
WANG H Z, ZHANG H G. Cryptography curriculum construction and teaching methods [J]. Journal of Higher Education, 2016(7): 78-79.

- [3] 张恩,王岁花,代丽萍. 翻转课堂在密码学课程教学中的应用案例[J]. 计算机教育, 2016, 259(7):64-67.
ZHANG E, WANG S H, DAI L P. Application case of flipped classroom in cryptography course teaching [J]. Computer Education, 2016, 259(7):64-67.
- [4] 范新民. 基于移动学习和翻转课堂深度融合的网络信息安全课程教学创新实践与探索[J]. 网络与信息安全学报, 2017(9): 65-70.
FAN X M. Practice and exploration of network information security course teaching innovation based on mobile learning and inverted classroom depth integration[J]. Chinese Journal of Network and Information Security, 2017(9):65-70.
- [5] 教育部高等学校信息安全专业教学指导委员会. 高等学校信息安全专业指导性专业规范[M]. 北京:清华大学出版社, 2014.
Advisory Committee of Information Security Teaching in Higher Education, Ministry P.R. China. Institutions of higher learning informatics professional safety guidance professional norms[M]. Beijing: Tsinghua University Press, 2014.
- [6] 武松,潘发明. SPSS 统计分析大全[M]. 北京:清华大学出版社, 2014.
WU S, PAN F M. SPSS statistical analysis[M]. Beijing: Tsinghua University Press, 2014.

[作者简介]



吴万青(1981-),男,河北邢台人,博士,河北大学讲师,主要研究方向为量子密码学。



杜瑞忠(1975-),男,河北沧州人,博士,河北大学教授,主要研究方向为信息安全、可信计算。