应用型本科院校基于 PBL 的实验混合式教学改革研究——以《密码学》课程为例

包致婷，王鑫，李梦泓，师凯，叶清清，王娇
重庆工程学院计算机与物联网学院，重庆 400051

DOI:10.61369/ETI.2025090010

摘　　要： 本文针对《密码学》课程实验教学中存在的内容简单难以培养学生综合能力、教学模式不够灵活、实验考核评价单一的三个问题，进行理论结合实践的研究。探究出适应当前应用型本科专业核心课程实验教学的新模式，通过基于项目式重构实验教学内容、实施 PBL 混合教学模式、设计多元化评价体系等改革措施，结合教学实践构建了有效的实验教学结构，旨在提升《密码学》实验教学质量，培养符合应用型人才需求的高素质技术技能型人才。

关 键 词： 密码学；PBL；混合式教学

Application Oriented Undergraduate Colleges Based on PBL Experimental HybridResearch on Teaching Reform — Taking the Course of Cryptography as An Example

Bao Zhiting, Wang Xin, Li Menghong, Shi Kai, Ye Qingqing, Wang Jiao
College of Computer and Internet of Things, Chongqing Institute of Engineering, Chongqing 400051

Abstract: This article conducts a theoretical and practical study on the three problems that exist in the experimental teaching of the course "Cryptography": simple content that makes it difficult to cultivate students' comprehensive abilities, inflexible teaching modes, and single experimental assessment and evaluation. Exploring a new mode of experimental teaching that is suitable for the current core courses of applied undergraduate majors, through reform measures such as project-based reconstruction of experimental teaching content, implementation of PBL mixed teaching mode, and design of diversified evaluation system, combined with teaching practice, an effective experimental teaching structure has been constructed, aiming to improve the quality of experimental teaching in Cryptography and cultivate high-quality technical and skilled talents that meet the needs of applied talents.

Keywords: cryptography; PBL; blended teaching

引言

随着信息技术高速发展，网络安全威胁日益严峻，密码技术作为保障信息安全的核心手段，其重要性愈发凸显。《密码学》课程作为培养学生密码技术应用能力的关键载体，实验教学环节更是重中之重。应用型本科院校以培养具备较强实践能力和解决实际问题能力的人才为目标，实验课程的教学质量直接影响学生能否满足行业对密码技术应用人才的需求 [1]。

然而，当前应用型本科院校《密码学》实验教学中存在诸多问题，制约了教学质量的提升和学生综合能力的培养 [2]。基于此，本研究引入项目式学习（PBL）教学理念和混合式教学模式，强调学生在真实问题情境中通过自主探究、团队协作完成项目任务，从而实现知识与技能的建构；混合式教学则融合线上线下教学优势，打破时空限制，为学生提供灵活的学习路径。将二者融合应用于《密码学》实验教学改革，有望解决当前教学中的痛点问题。本文结合应用型本科院校特点，以《密码学》实验课程为例，探讨基于 PBL 的实验混合式教学改革路径，为同类课程教学提供参考。

项目信息：2024 年重庆工程学院教育教学改革研究项目，项目名称：应用型本科院校基于 PBL 的实验混合式教学改革研究——以《密码学》课程为例（JY2024202）
作者简介：包致婷（1994-），女，重庆永川人，硕士，讲师，研究方向：密码学、网络安全。

一、《密码学》实验教学现存问题分析

《密码学》实验课程的核心目标是让学生能够实现 DES、RSA、Diffie-Hellman、哈希密码算法并测试性能；能熟练地使用 PGP 加密软件，能搭建身份认证环境；能搭建证书服务环境并完成 Win2012 证书服务的配置、验证。然而，在当前的教学实践中，由于教学理念、教学资源、教学模式等多方面因素的影响，实验教学效果未能达到预期，主要体现在以下三个方面。

（一）实验内容缺乏培养学生解决复杂性、综合性问题的能力

目前实验教学内容大多以验证性实验为主，这些内容往往步骤固定、目标明确，学生只需按照实验指导书的要求进行操作即可完成。在实际应用中，密码学技术的应用往往是复杂的，需要综合运用多种密码算法和技术，考虑系统的安全性、效率、可扩展性等多方面因素。而现有的实验内容无法让学生接触到真实的复杂应用场景，导致在面对实际问题时，难以将所学的零散知识整合起来，缺乏解决综合性问题的思路和能力。

（二）实验教学模式不够灵活

传统的《密码学》实验教学模式大多采用“教师讲解 --学生操作 --教师评阅”的固定模式，教师在实验课堂上先讲解实验目的、原理和步骤，然后学生按照教师的要求在实验室进行操作，最后教师对学生的实验结果进行评阅。这种教学模式缺乏灵活性，学生无法根据自己的学习进度和需求进行自主安排。此外，传统教学模式中师生互动和生生互动不足，学生在实验过程中遇到问题时，往往只能向教师请教，缺乏与其他同学的交流和合作，不利于培养学生的团队协作能力和沟通能力 [3]。

（三）实验考核评价单一，不利于应用型本科人才对实验的掌握

当前《密码学》实验教学的考核评价方式较为单一，主要以实验报告评阅为主，实验报告往往侧重于对实验步骤和结果的记录，难以全面反映学生的实验过程、思维方式和创新能力。这种单一的考核评价方式无法准确评估学生在实验过程中的参与度、团队协作能力、问题解决能力等，也不能及时发现学生在学习过程中存在的问题并进行针对性的指导。对于应用型本科院校来说，培养学生的实践能力和应用能力是关键，而现有的考核评价方式难以满足这一要求，不利于激发学生的学习积极性和主动性 [4]。

二、基于 PBL 的《密码学》实验混合式教学改革措施

（一）基于项目式重构实验教学内容

基于项目式学习（PBL）的理念，重构《密码学》实验教学内容，以实际项目为载体，将密码学的理论知识和实验技能融入到项目中，培养学生解决复杂性、综合性问题的能力。在具体实施时设计以下几个项目案例：

1.CA 证书服务配置

服务器证书受到了越来越多企业的青睐，它不仅可以显示网站的真实性，还可以在网站用户输入密码与用户名时对这些信息进行加密，全程保护用户信息安全。通过 Win2012 的证书服务配置，加深学生对数字证书，身份认证等知识的理解。本综合案例融合了《密码学》课程的公钥加密技术、哈希技术、数字证书、身份认证等知识点，学生自主地在虚拟机安装操作系统，检查客户端和服务器的连通性，更好地让学生理解申请证书的整个流程，提高检验证书和站点配置的能力，一定程度培养了学生的迁移能力 [5]。

2.基于密码技术的信息保护系统

数字化时代，政务、金融等领域核心信息存传面临泄露、篡改威胁，安全防护需求迫切。项目要求学生设计信息加密系统，需完成数据加密、密钥全生命周期管理、校验完整性，适配多系统与数据库并实现核心模块。此项目助学生理解信息安全需求，掌握密码技术应用，提升理论转实践能力。

3.基于密码技术的电子邮件系统

当下电子邮件常存信息泄露、内容篡改风险，隐私与数据安全受威胁。项目要求学生根据某企业对电子邮件系统的实际需求进行规划设计。主要包括系统总体架构设计、用户管理设计、密钥管理设计、邮件加解密设计、邮件签名验证设计。此项目帮助学生明晰邮件安全需求，掌握密码技术落地方法，提升在通信领域的安全实践能力。

（二）PBL 混合教学模式研究及实施

以学生实践动手能力培养为中心，将传统课堂与现代网络教学有机结合，突破课程学习空间与时间的限制，做到课前、课中、课后全覆盖。课前，教师设计问题，可以通过超星平台发布学习任务与目标，推送相关学习资源，学生带着问题进行在线项目预习；课中，教师将问题导入，进行重点内容讲解，学生根据所学知识、实验室条件等积极主动地独立设计、完成实验；课后，教师发布课后作业和小组作业，对学生进行答疑解惑和问题研判，学生进行巩固复习、总结讨论和创新实践。

学生通过超星平台的视频、PPT 课件和文档资源可以进行课前预习，通过主题讨论可以查阅相关文献资料，加深对知识的理解，通过课堂前测、随堂练习和章节测试可以检验自己对知识的掌握程度，同时，教师可以通过在线平台开展辅导答疑，鼓励学生多质疑、相互交流、相互探讨，提升教学效果，提高学生学习兴趣。

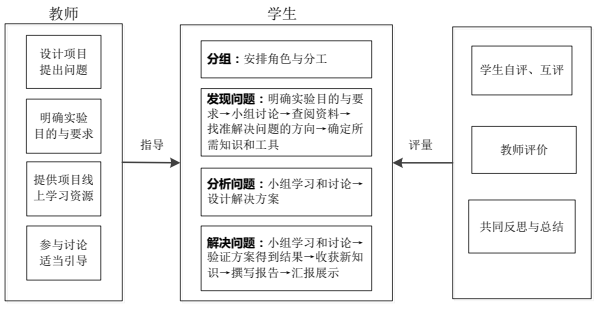

图1 PBL混合教学流程

（三）设计评价体系，实施多元化考核

为使学生全面发展，强化过程性评价，确保学生学习目标达到预期效果。课程实施 OBE 理念考核，由过程性考核 40% 和期末考试 60% 两部分组成，其中针对实验的考核是目标 2，如下图所示：

此外，针对以项目为导向的实验教学，对学生的过程性考核主要体现在实验报告和代码，每一个实验项目要求书写对应的实验报告，并在规定时间内提交到智学重工平台。实验报告由核心算法原理、源程序代码、测试结果和总结等模块构成。会对实验报告加入查重检测和使用 ChatGPT 等工具的 AI 检测，同时学生的实验报

告由教师评阅成绩转变为学生互评、学生自评和教师评阅三部分构成，对实验项目的线上学习也会占该次实验报告的比重。

1.考核内容与课程目标对应关系

课程目标	考核环节	考核内容	占总评分比重
目标 1	作业 1-3	能够掌握密码学的基本概念、基本属性；能够掌握经典的密码算法构造原理；能够区别不同的密码体制并将这些知识运用于信息安全系统的分析与理解；能根据安全属性要求去设计相对应的密码模型。	9%
	阶段测试 1-2		8%
	期末考试		42%
目标 2	实验报告 1-6	能够实现 DES、RSA、Diffie-Hellman、哈希密码算法并测试性能；能熟练地使用 PGP 加密软件，能搭建身份认证环境。能搭建证书服务环境并完成 Win2012 证书服务的配置、验证。能够针对复杂信息安全工程问题，选择与使用恰当的技术、资源、现代工程工具和信息技术工具。	9%
	实验报告 7		8%
	期末考试		18%
目标 3	作业 4-5	了解企业文化和 IT 行业（特别是信息安全行业）的职业道德和规范，并在工程实践中理解并遵守，履行责任。通过讲解近十年来国产密码的发展及应用，引导学生树立核心技术国产化意识，培养学生的安全保密意识，增强爱国自豪感和民族自信心。	6%

2.期末考试题型及分值比例（试卷考核类）

题型 / 目标	密码体制分析与计算	密码模型设计	综合应用	合计
目标 1	40	20	10	70
目标 2			30	30
合计	40	20	40	100

图2 考核成绩比例分布

三、教学改革效果分析

以应用型本科（重庆工程学院）23级信安1-3班的数据为例，总结改革效果：

（一）学生学习积极性提高

下图为各班级同学密码学课程超星积分图，从整体积分情况来看，大部分同学表现优异，课堂参与度极高。积分主要考核了同学们作业、视频学习、测试、课堂讨论、课堂练习等环节。通过努力，各班级平均积分都是70分以上，说明大部分同学积极参与课堂，课前认真完成线上实验视频学习。

图3 超星课堂积分分布

（二）目标达成度较好

对实验考核的课程目标 2包含验证性实验 6次、综合性实验 1次和期末考 试两个部分，主要考核学生能够实现 DES 、RSA 、Diffie-Hellman、哈希密码算法并测试性能；能熟练地使用 PGP 加 密软件，能搭建身份认证环境。能搭建证书服务环境并完 成 Win2012证书服务的配置、验证。能够针对复杂信息安 全工程问题，选择与使用恰当的技术、资源、现代工程工具和信息技术工具。课程目标 2达成度为0.7，说明教学方法可行，教学效果良好。

密码学课程目标达成情况评价表（课程总表）

一、课程基本信息						
基本信息	课程名称	密码学			课程编号	20212018
	课程类别	专业核心课			课程学时	48
	开课学期	2025春	授课对象	信息安全专业	课程学分	3
	选课人数	132	任课教师	包敬婷		

二、课程目标达成度评价信息					
课程目标达成情况	毕业要求指标点	课程目标	考核依据	目标分值	学生平均得分	目标达成情况
	1.3 能将相关知识和数学模型方法用于信息安全复杂工程问题解决方案的比较和综合。	课程目标1	期末考试 过程性考核	59	46.25	0.78
	4.3 能够根据实验方案构建实验环境、系统，安全开展实验，科学采集实验数据。	课程目标2	期末考试 过程性考核	35	24.59	0.70
	8.1 树立和践行社会主义核心价值观，理解个人与社会的关系，了解中国文化、中国国情。	课程目标3	过程性考核	6	5.25	0.88
	课程总体达成情况			100	76	0.76
课程目标考核支撑材料清单		材料名称			份数	
		成绩册			5	

三、目标达成度统计表								
课程目标	0-0.6	0.6-0.7	0.7-0.8	0.8-0.9	0.9-1	平均值	最低值	最高值
课程目标1	4	21	41	48	18	0.78	0.45	0.94
课程目标2	23	41	34	26	8	0.70	0.38	0.96
课程目标3	0	0	8	52	72	0.88	0.70	0.95
总目标	3	26	55	42	6	0.76	0.46	0.92

图4 23信安1-3班总体课程目标达成度图

（三）学生竞赛能力、科研能力明显增强

学生们踊跃参与行业及企业的相关竞赛，真正把所学知识在实践中进行运用。近年来多人次在各类学科竞赛中取得企业及行业的一、二、三等奖，学生还发表了与密码学相关的科研论文。更可喜的成效是在课程学习之余，大部分同学考取了行业内的证书。

四、总结

本研究针对应用型本科院校《密码学》实验教学中存在的问题，提出了基于 PBL的实验混合式教学改革方案，通过基于项目式重构实验教学内容、设计多元化评价体系以及实施 PBL混合教学模式，取得了良好的教学效果。在今后的教学改革中，将进一步优化项目案例设计，及时更新项目内容，确保项目的先进性和实用性；加强教师培训，提高教师的 PBL教学水平和混合式教学组织能力。不断总结经验，为应用型本科院校的教学改革提供更多的参考和借鉴。

参考文献

[1]彭景惠 .项目式的应用密码学课程 OMO混合式教学探索 [J].计算机教育 ,2023,(11):145-149.
[2]董建阔 , 肖甫 , 沙乐天 .新工科背景下融合 OBE与 PBL的密码实践课程教学设计 [J].计算机教育 ,2023,(01):136140.
[3]王志华 .基于智慧教育和混合式教学的密码学“金课”建设 [J].计算机教育 ,2024,(08):155-158+164.
[4]徐伟光 , 王保华 , 曹铁勇 , 等 .基于 OBE理念的应用密码学课程教学改革 [J].计算机教育 ,2023,(11):99-103.
[5]王娜 , 刘建伟 , 付俊松 , 等 .现代密码学课程的混合教学模式探索 [J].计算机教育 ,2023,(03):14-17.

