Creative Education Studies 创新教育研究, 2024, 12(9), 330-336
Published Online September 2024 in Hans. https://www.hanspub.org/journal/ces
https://doi.org/10.12677/ces.2024.129625

Hans汉斯

《现代密码学原理》课程教学改革探索与实践

——以仲恺农业工程学院为例

陈文文，邹　莹，罗志杰，张世龙

仲恺农业工程学院信息科学与技术学院，广东 广州

收稿日期：2024年7月31日；录用日期：2024年9月2日；发布日期：2024年9月10日

摘　要

为提高教学质量，培养网络安全高尖人才，文章分析了《现代密码学原理》课程中存在的课程目标与产业需求不匹配、学生学习主动性差和实践能力培养不足等问题，并从教学目标、教学内容、教学方式和教学评价入手，深入探讨了《现代密码学原理》课程教学改革的途径，并提出了“以学生为中心、多元融合、以赛促学”的混合式教学改革方案，取得一定成效。

关键词

OBE，混合式教学，改革，现代密码学

Exploration and Practice of Teaching Reform of “Modern Cryptography Principles”

—A Case Study of Zhongkai University of Agriculture and Engineering

Wenwen Chen, Ying Zou, Zhijie Luo, Shilong Zhang

College of Information Science and Technology, Zhongkai University of Agriculture and Engineering, Guangzhou Guangdong

Received: Jul. 31st, 2024; accepted: Sep. 2nd, 2024; published: Sep. 10th, 2024

Abstract

To enhance the teaching quality and cultivate top-notch talents in cyber security, this paper analyses the issues existing in the course “Modern Cryptography Principles”, including the mismatch between the course objectives and industrial demands, students’ poor initiative in learning, and the insufficiency in cultivating practical abilities. Beginning with the teaching objectives, teaching contents, teaching approaches and teaching evaluations, it deeply investigates the pathways of the

文章引用: 陈文文, 邹莹, 罗志杰, 张世龙. 《现代密码学原理》课程教学改革探索与实践[J]. 创新教育研究, 2024, 12(9): 330-336. DOI: 10.12677/ces.2024.129625

teaching reform of the "Modern Cryptography Principles" course and puts forward a blended teaching reform scheme of "student-centered, multi-integration and promoting learning through competitions", which has achieved a certain effect.

Keywords

OBE, Blended Teaching, Reform, Modern Cryptography

1. 引言

2016 年，由中网办、发改委、教育部等六部门联合印发的《关于加强网络安全学科建设和人才培养的意见》指出："网络空间的竞争，归根结底是人才的竞争，为加强网络安全学院学科专业建设和人才培养，需加快网络安全学科专业和院系建设，完善本专科、研究生教育和在职培训网络安全人才培养体系。"国家安全人才的培养，对实施网络强国战略、维护国家网络空间主权和国家网络安全有着重要的价值和意义。

2016 年，仲恺农业工程学院将网络空间安全专业的申请和建设列入"十三五"发展规划中，将网络安全课程体系加入网络工程专业人才培养方案。《现代密码学原理》是仲恺农业工程学院网络安全人才培养的核心基础课程。然而，随着信息技术的快速发展和移动互联网的普及，受在线开放课程及娱乐活动等影响，学生在课堂教学中呈现出注意力缺失的趋势。同时由于《现代密码学原理》课程知识覆盖面广、数学基础要求高、更新快等特点，学生在课程学习上出现了兴趣低下、质量下降等问题。传统教学模式已经不能满足课程教学的需求。

2. 《现代密码学原理》课程教学改革的理论基础

党的十九大报告提出了建设教育强国的战略任务，并指出要加快教育现代化，深化教育体制机制改革，创新教育模式，推进教育信息化。其中，混合式教学和成果导向教育(Outcome-Based Education, OBE)被广泛应用于我国高等教育的教学改革之中。混合式教学的概念开始由美国斯隆联盟做了界定，定义为"在线教学与面授教学的混合"，随着互联网的发展，正式演变为"基于移动通信设备、网络学习环境与课堂讨论相结合的教学情境"[1]。OBE 的核心理念为"产出导向，学生中心，持续改进"，为满足新工科建设发展和工程教育改革需求，被我国工程专业认证所倡导并运用于教学。如郭文俊等[2]将 OBE 理念应用于数字逻辑课程改革，依托超星尔雅平台构建线上线下混合式教学模式，极大增加了学生的学习兴趣，提升了学生的综合能力和培养了学生的情操素养。王志华[3]提出利用现代信息技术和混合式教学的密码学"金课"建设方法，提高了课堂教学质量，并加强了学生创新实践能力培养，提高了人才培养质量。

"以赛促学"早期应用于高职教育中的学生技能技术教学，后被推广至高等教育中学生实践能力和工程能力的培养环节。"以赛促学"是指通过组织大学生参加各类竞赛，激发学生的学习兴趣，促进良好学风的形成，同时通过比赛促使学生动手操练、实践、创新，提升综合素质[4]。实践能力作为网络安全人才的核心能力之一，"以赛促学"也应用于网络安全课程的教学改革中。教学实践表明"以赛促学"是有效的改革措施。如光焱等人将 CTF 竞赛与密码学实验课程相结合，研究总结出一套题目引入、攻防

对抗、考评激励的为主要特点的教学模式[5]。魏为民等人将学生身边故事结合 CTF 竞赛方式将“莫尔斯码破译”和“乱码图片制作”教学竞赛案例加入到课程实验教学中并取得良好效果[6]。

教育部高等教育司关于开展新工科研究与实践的通知指出，新工科的建设要围绕工程教育改革的新模式，要深化产教融合和校企合作的体制机制。网络安全作为新工科建设的重要部分，产业技术更新迭代快，传统人才培养模式和教学模式下的毕业生往往满足不了企业用人需求。产教融合能够更好地面向产业需求，借助企业的资源和技术优势，培养适应市场的应用型人才。

2016 年，习近平总书记在全国高校思想政治工作会议上强调要坚持把立德树人作为中心环节，把思想政治工作贯穿教育教学全过程[7]。新工科的内涵是以立德树人为引领，培养未来多元化、创新型卓越工程人才[8]。立德树人是新工科建设的核心目标。作为新工科建设的重要组成，挖掘思政元素，融入课程教学，潜移默化引导学生，培养学生的科学思维，塑造学生的道德情操，是网络安全人才培养的重要任务。

因此《现代密码学原理》课程教学团队提出了“以学生为中心、多元融合、以赛促学”的混合式教学模式。使用 OBE 作为教学理念，坚持以学生为中心、成果导向、持续改进。在教学过程中，坚持与产业结合，校企协同育人；坚持立德树人，将思政融入课程。注重培养学生的实战能力，将网络攻防竞赛融入实验课教学中，激发学生的学习热情。

3. 《现代密码学原理》课程教学改革的意义

《现代密码学原理》作为教育部高等学校网络空间安全专业教学指导委员会指定专业基础课程，是高等本科院校网络安全学科建设的核心部分，也是网络安全人才培养的重要环节。《现代密码学原理》课程教学改革旨在激发学生的学习兴趣、提升教学质量的同时，加强学生的密码设计、密码分析、密码应用的综合能力、科学思维和塑造道德情操，为后续的网络安全专业课程教学和网络安全人才培养打好基础。《现代密码学原理》课程在网络安全专业课程中具有典型代表性，教学改革解决了网络安全专业课程中的共性问题，具有推广的价值和意义。

4. 《现代密码学原理》课程现状及存在问题

4.1. 网络安全技术发展迅速，课程设置与产业需求脱轨

网络安全技术发展迅速，课程设立的教学目标和教学内容与网络安全产业需求脱轨，培养的学生在知识体系和素质能力上不符合企业实际需求。产业界对网络安全人才的需求不断变化，从传统的防火墙和杀毒软件，到如今的云安全、人工智能在安全中的应用等，要求学生学习更广泛和更深入的知识体系。《现代密码学原理》课程设置的教学内容仍停留在基础理论层面，缺乏对新兴威胁和前沿安全技术的及时覆盖。同时，企业生产工作过程中人才亟需的团队合作能力、问题解决能力和职业道德素养在课程教学目标上也并未体现。

4.2. 学生对课程表现为有畏难情绪、主动性较差、兴趣度较低

《现代密码学原理》课程存在知识覆盖面广、知识点庞杂、数学基础要求高、更新快等特点。密码学的发展可以推及至公元前四百多年，其覆盖的知识包括数学、语言学、信息论等，是多学科交叉的课程。同时密码学包含许多相对复杂的数学基础知识，难度较大。密码学的应用遍布军事、金融和工业等行业。为适应产业发展，密码学的知识更新和发展速度较快。学生对课程存在畏难情绪。课程教学以教师为中心，教师讲授、学生听讲为主要模式，学生学习自主性较差。教学以课堂教学为主，课堂教学手段和教学方法单一，以课件讲授方式进行，学生课堂的参与度低，注意力较差，课堂的教学效果一般。在教学资源上，课程教学中缺少教学案例进行支撑，密码技术是较为抽象的、理论性较强的技术，学生

兴趣度较低。

4.3. 教学过程对学生的实践能力培养不足，以演示型实验为主，缺乏综合实践平台

《网络安全人才实战能力白皮书》指出企业对网络安全人才实战能力和应用能力的需求。但《现代密码学原理》课程在教学内容上存在实践环节不足和教学目标上实战能力培养匮乏的问题，使学生无法将密码设计和分析应用到实际场景里，完成网络与信息安全技术研究、产品开发、服务与运维等工作。同时，实验课缺乏一个综合实践平台作为实验课的支撑平台，集合实验工具和提供课堂及课下的实验环境。并且，实验课以演示型实验为主，需要其他综合型或设计型的实验，提升学生的实践能力。

4.4. 课程在传授专业知识的同时缺乏对学生内在思想的引领

《现代密码学原理》课程中涉及的专业知识和技术是一把“双刃剑”，它可以成为保障国家数字经济和关键性基础设施安全的利器，也可能成为危害人民财产、社会稳定的凶器。学生作为手握双刃剑的人，大都活泼好动，精力充沛，有好奇心，但自我意识薄弱，世界观、人生观、价值观尚在建立过程中。然而，《现代密码学原理》课程的教学只停留在知识层面的教与学，缺乏法律、政治和道德的多维思考，无法在思想层面引领学生，将双刃剑变成利刃。

5. 《现代密码学原理》课程教学改革方案

《现代密码学原理》课程教学团队提出了“以学生为中心、多元融合、以赛促学”的混合式教学模式，从五个维度进行改革，分别为走访企业、思政教育、以赛促学、课堂教学改革和以 OBE 为教学理念的混合式教学模式实施。

5.1. 走访企业，与企业人员开展研讨会讨论，调研一线工作人员及往届毕业生，具体化课程知识和技能要求

课程团队与网络信息安全技术公司开展研讨会，结合企业需求，就《现代密码学原理》课程的知识体系和能力要求展开讨论。同时，团队采访了网络工程专业毕业生，结合毕业生在企业的实际情况，了解网络安全产业的人才需求，将需求具体化到课程的知识和技能要求。最后，团队将知识技能要求转化成课程教学目标，并调整教学内容。调整完成的教学目标如表 1 所示。

Table 1. Teaching objectives of “Modern Cryptography Principles”
表 1. 《现代密码学原理》课程教学目标

教学目标	细分目标
知识目标	1) 能够掌握安全模型、安全要求、安全攻击和相关安全机制等信息安全基本概念 2) 能够掌握密码学的基本知识，包括典型密码的基本概念、密码组成与原理、密码的实现与应用 3) 能够掌握密码算法的安全要求和设计思想 4) 能够掌握密码的攻击手段和分析方法
能力目标	1) 能够掌握与团队合作和沟通的能力 2) 能够掌握密码分析中的逆向思维、辩证思维、创新思维和逻辑推理能力 3) 能够掌握密码分析中抽象问题、分析问题和总结问题的能力 4) 能够掌握密码的安全设计，具备在密码设计中规避安全漏洞的能力，将密码技术应用到网络与信息安全系统的设计与开发中 5) 能够对密码进行安全分析，将所学知识应用到评估不同场景下密码应用安全性的工作中

续表

素质目标	1) 能够了解到中国在密码学发展的重要贡献，增强民族自豪感和民族自信心，培养爱国情操 2) 能够了解中国密码法等法律法规，知道蓄意攻击是违法行为，在学习和工作过程中能够遵守法律，培养法治精神 3) 能够了解密码学家设计的密码为社会带来的价值，激发学习密码学的热情，为社会和国家创造价值 4) 能够了解黑客给不同行业带来的经济损失和网络安全工程师为企业、政府和社会创造的价值，培养职业道德和职业操守 5) 能够学习前沿科研论文，紧跟前沿科研知识，以前沿科研知识为基石，培养勇攀科学高峰、不断探索的精神

5.2. 以案例形式将思政教育融入到课程教学中，坚持立德树人

在课程教学中，坚持立德树人，坚持知识传授与价值引领相统一，显性教育与隐性教育相统一。课程思政作为一种思想教育，在融入课程教学的过程中要做到润物细无声，案例引入是一种合适的方式。课程教学团队收集整理出课程对应章节的思政案例、设计思政目标。章节对应的思政案例和思政目标如表 2 所示。

Table 2. Ideological and political cases and objectives of “Modern Cryptography Principles”
表 2. 《现代密码学原理》课程思政案例与思政目标

教学章节	教学内容	思政案例	思政目标
第一章	信息安全基本概念	民族英雄戚继光发明“密电码”进行军事通信，击败倭寇	培养学生的民族自豪感，激发学生的爱国热情
第二章	密码学基本概念与传统加密技术	图灵用译码器破解恩格玛机，帮助英国取得二战胜利	培养学生的家国情怀，树立网络强国的爱国意识
第三章	分组密码和数据加密标准	Feistel 密码学家设计加密结构与解密结构相同的 Feistal 密码的故事	鼓励学生以密码学家为榜样，学习 Feistel 等密码学家身上求索创新和精益求精的精神
第四章	高级加密标准	AES 发展历史中秘密设计算法的失败到公开征集算法的成功	鼓励学生对密码研究和开发要保有开放态度，学会包容兼听
第五章	分组加密的工作模式	中国国家密码管理局发布的商用密码算法标准——SM4 分组密码算法	培养学生的民族自豪感，树立网络强国的爱国意识
第六章	公钥密码学与 RSA	《孙子算经》中中国剩余定理在 RSA 算法加解密计算效率提升上的作用	培养学生的民族自豪感和自信心
第七章	密钥管理与其他公钥密码体制	Diffie 和 Hellman 两个密码学家钻研探索密码设计，提出公钥密码	鼓励学生以密码学家们为榜样，培养刻苦钻研、精益求精的工匠精神。
第八章	密码学 Hash 函数	王小云教授领导的团队在 Hash 函数的安全性分析方面做出的创新性贡献	培养学生的民族自豪感，激发学生的爱国热情
第九章	消息认证码	中国科学院微小卫星创新研究院成功发射 50 次卫星的卓越成绩的新闻	鼓励学生学习工程师们的敢于担当作为、勇于攻坚克难，拼搏奉献精神
第十章	数字签名	电子签名法和行政执法平台管理办法	让学生看到我国在电子签名方面法律建设的前瞻性，培养学生法治意识和遵纪守法的职业道德

5.3. 搭建综合实践平台，改造实验课堂

课程团队搭建综合实践平台，集合实验需要的工具和所需编程语言的编译器，构建《现代密码学原理》课程实验环境，包括在线加密实验、在线解密实验和密码分析实验三个模块的实验环境。改造实验课堂，结合网络攻防竞赛题目设置不同的实验背景、实验内容和实验要求。将实验课堂分成难题求解和攻防对抗两种方式进行，激发学生的兴趣。难题求解以国安人员秘密通信为背景设置难题，要求学生进行加密或解密。攻防对抗将学生分成红蓝两队，一队出难题一队解答再进行对调。

5.4. 借助现代信息技术，使用多样化教学方法进行课堂教学

在现代信息技术的发展下，智能教学终端软件应运而生，如超星学习通、雨课堂等。在《现代密码学原理》的课堂教学中使用“雨课堂”作为智能教学终端软件，通过题目作答、匿名投票、弹幕投送和随机提问的方式增加与学生的互动。在课堂教学中引入多种教学方法，情景导入、问题导入、图形演示、案例教学、启发式教学等。在第三章，通过 1980 年代香料秘方传输案例进行 DES 密码课堂的导入。在第八章，通过“QQ 账号丢失后如何找回”问题进行 Hash 函数课堂的导入。在第四章，通过动图和视频的形式进行 AES 密码的十轮变换的演示。课程组教师完成了课程每个章节的案例收集并进行课堂案例教学，如美国无线电视使用 DES 进行信息加密、区块链使用 Hash 函数进行信息完整性保护等，同时，也为每次课堂设置提问的问题、回顾的内容和引出的知识点。

思维导图也是现代信息技术发展下的产物，是表达发散性思维的有效图形思维工具。使用思维导图串联章节知识点把各个知识点的隶属关系和层级关系进行表示，可以加深学生对知识点和知识点之间关系的理解，更好地构建知识体系。课程组教师为课程每个章节构建了思维导图，并使用“雨课堂”进行课前发放，并在讨论区开启讨论，要求学生结合思维导图进行课堂的预习工作，提前为课堂教学预热。

5.5. 使用以 OBE 为教学理念的混合式教学模式，以学生为主体

OBE 教学理念的基本原则为“坚持以学生为中心、成果导向、持续改进”。《现代密码学原理》课程教学过程中坚持以学生为中心，采用混合式的教学模式。课程组教师使用超星平台上的 MOOC 资源，包括微课视频、随堂测验、分组讨论和课后作业，要求学生在课堂学习前先进行线上微课视频的学习，完成随堂测验，参与线上分组讨论。上课教师通过随堂测验，了解学生的掌握情况，调整课堂教学的内容和安排。通过线上学习，充分调动学生的学习主动性。微课视频可以反复观看，也为基础薄弱的学生提供了回顾再次学习的机会。

在课程教学中坚持以教学成果为导向，持续改进教学。教学评价是教学成果的一大体现。传统课程教学采用以终结性评价为主的评价模式，只有到学期终才有比较完备的教学评价，无法考察学生的过程表现，并持续反馈教学活动中，改进教学安排。因此，在《现代密码学原理》的课程改革中采用以形成性评价为主，终结性评价为辅的评价模式，其中形成性评价包括 MOOC 任务点完成数、MOOC 学习时长、讨论区回帖数、组内评价、课堂表现、实验成绩和课后作业等。

6. 《现代密码学原理》课程教学改革成效

《现代密码学原理》课程的教学评价数据如表 3 所示。由表可知，《现代密码学原理》的两次课堂教学，学生的参与率都达到 80%以上，对比传统课堂三分之一的抬头率，学生在课堂上的学习积极性明显提高。专业学生的 MOOC 学习的任务点完成百分比将近 70%，学生平均学习章节 76 次。课程视频学习进度将近 70%，平均学习时长为 117 分钟。讨论区的平均讨论数为 7 条，大部分同学参与了讨论。期末平均成绩为 74 分，对比传统教学模式下的平均成绩 65 分，说明学生专业理论知识掌握更好。课程培

养的实践能力在比赛上得到体现，学生相继在“长城杯”信息安全铁人三项赛、新华三杯全国大学生数字技术大赛、大唐杯全国大学生新一代信息通信技术大赛上获奖。

Table 3. Teaching evaluation data of “Modern Cryptography Principles”
表 3. 《现代密码学原理》课程评价数据

班级 / 评价点	班级 1	班级 2	平均值
课堂参与率	84%	80%	82%
MOOC 任务点完成度	70%	67%	68.5%
MOOC 章节学习次数	80 次	72 次	76 次
MOOC 视频学习进度	70%	68%	69%
MOOC 视频学习时长	120 分钟	113 分钟	117 分钟
讨论区回帖数	8 条	6 条	7 条
期末成绩	75 分	73 分	74 分

7. 结语

《现代密码学原理》课程作为仲恺农业工程学院网络空间安全人才培养的重要环节，存在课程设置与产业需求脱轨；学生对课程表现为有畏难情绪、主动性较差、兴趣度较低；教学过程对学生的实践能力培养不足，以演示型实验为主，缺乏综合实践平台；课程在传授专业知识的同时缺乏引领学生思想的问题。课程教学团队提出了“以学生为中心、多元融合、以赛促学”的混合式教学模式作为教学改革方案，从教学目标、教学内容、教学方式到教学评价完成了全方位的改革，并取得了一定效果。教学改革得到了企业和学生的认可。学生的上课积极性、专业理论能力、实战能力和综合素质有了一定提高。课程教学团队未来将持续改革和探索，优化课程教学方案，为国家培养出新一代网络安全高精尖人才。

基金项目

仲恺农业工程学院 2022 年度校级教学质量和教学改革工程项目(仲教字[2022] 39 号)。

参考文献

[1] 冯晓英, 王瑞雪, 吴怡君. 国内外混合式教学研究现状述评——基于混合式教学的分析框架[J]. 远程教育杂志, 2018, 36(3): 13-24.

[2] 郭文俊, 杨泽民, 张盛天, 等. 基于 OBE 理念的数字逻辑课程混合式教学改革[J]. 计算机教育, 2024(8): 114-119.

[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(8): 155-158+164.

[4] 陈英杰, 刘健, 唐新军, 等. 以赛促学、以赛促练、以赛促教——工科大学生竞赛与教学结合的教学模式探索与实践[J]. 中国管理信息化, 2015, 18(13): 246-248.

[5] 光焱, 康绯, 卜文娟. 网络安全专业基于 CTF 模式的密码学课程实验课教学改革[J]. 教育现代化, 2019, 6(90): 86-87.

[6] 魏为民, 杨朔, 酆华, 等. 结合 CTF 竞赛模式的信息安全课堂教学[J]. 计算机教育, 2017(6): 23-27.

[7] 把思想政治工作贯穿教育教学全过程[N]. 人民日报, 2016-12-09(010).

[8] 钟登华. 新工科建设的内涵与行动[J]. 高等工程教育研究, 2017(3): 1-6.