新工科背景下以“创新、实践”为导向的密码学与网络安全课程教学改革

代敏君[1*]，李智凯[2]

（[1] 广东东软学院 计算机学院，广东 佛山 528000；[2] 广东东软学院，广东 佛山 528000）

摘要：在新工科建设深入推进和网络空间安全战略需求日益凸显的背景下，传统密码学与网络安全课程面临教学内容滞后、教学方式单一、实践能力薄弱及育人实效不足等问题。本文以 OBE（成果导向教育）理念为指导，融合 Keller 的 ARCS 动机设计模型，提出“创新·实践”双轮驱动的教学改革模式。通过构建动态更新的知识体系、设立“密码学五分钟”探索分享机制、深化赛教融合与校企协同、重构实验教学平台与多元评价体系，并将课程思政有机融入全过程，形成“基础夯实—前沿牵引—主动探究—价值塑造”的一体化教学路径。实践表明，该模式有效提升了学生的学习主动性、工程实践能力和职业责任感，实现了从“知识传授”向“能力生成”与“价值内化”的转变。

关键词：密码学与网络安全；教学改革；OBE；ARCS 模型；课程思政

DOI：https://doi.org/10.71411/jyyjx.2025.v1i7.874

Teaching Reform of Cryptography and Network Security Courses Oriented by "Innovation and Practice" under the Background of New Engineering

Dai Minjun[1*], Li Zhikai[2]

([1] Neusoft Institute Guangdong, College of Computer Science, Department of Network Engineering, Foshan, Guangdong Province, 528000, China; [2] Neusoft Institute Guangdong, Foshan, Guangdong Province, 528000, China)

Abstract: Under the background of the deepening of new engineering construction and the increasing prominence of the strategic demand for network space security, traditional cryptography and network security courses face problems such as lagging teaching content, single teaching methods, weak practical ability, and insufficient effectiveness in talent cultivation. Guided by the OBE (Outcomes-Based Education) concept and integrated with Keller's ARCS Motivation Design Model, this paper proposes a teaching reform model driven by the dual wheels of "innovation and practice". By constructing a dynamically updated knowledge system, establishing a "Cryptography in Five Minutes" exploration and sharing mechanism, deepening the integration of competition and teaching as well as school-enterprise collaboration, reconstructing the experimental teaching platform and diversified evaluation system, and organically integrating ideological and political education into the whole process, a one - stop teaching path of "solidifying the foundation - leading the cutting - edge - active exploration - value shaping" is formed. Practice has shown that this model effectively enhances students' learning initiative,

作者简介：代敏君（1997-），女，四川南充，硕士，研究方向：区块链、群智能算法

李智凯（1997-），男，湖北孝感，硕士，研究方向：网络空间安全

通讯作者：代敏君，通讯邮箱：daiminjun@nuit.edu.cn

engineering practice ability, and professional sense of responsibility, and realizes the transformation from "knowledge transmission" to "ability generation" and "value internalization".

Keywords: Cryptography and Network Security; Teaching Reform; OBE; ARCS Model; Ideological and Political Education in Courses

引言

随着 5G、人工智能、区块链、隐私计算等新兴技术快速发展，数据已成为国家战略资源，而密码技术作为保障信息完整性、机密性、不可否认性的核心技术，在国家网络安全体系中扮演着重要的角色。在新工科建设的时代背景下，网络安全领域正经历着深刻变革，“密码学与网络安全”作为网络安全及相关专业的核心课程，其重要性日益凸显。

然而，当前高校密码学与网络安全课程普遍存在“重理论轻应用、重讲授轻探究、重技术轻伦理”的问题，难以满足新工科背景下对复合型、创新型、责任型信息安全人才的需求[1]。教学内容集中于 RSA、AES 等经典算法，对后量子密码、零知识证明、联邦学习中的隐私保护等前沿领域涉及较少，导致学生“学到的东西企业不用”，缺乏对未来技术趋势的认知与适应能力[2]。

立足新工科建设要求，依托 OBE（Outcome-Based Education）反向设计框架[3]，明确毕业生在企业岗位中应具备的知识、能力与素质目标，再据此重构课程体系，确保教学活动始终服务于人才培养的根本目的。同时，引入 Keller 的 ARCS 动机设计模型[4]，通过真实安全事件导入吸引注意力、结合产业应用场景增强相关性、设置分层任务建立自信心、通过成果展示带来满足感，系统提升学生的学习主动性。

1 密码学与网络安全课程现状

当前密码学与网络安全课程在实施过程中暴露出诸多结构性问题。首先，教学内容更新滞后，难以匹配技术发展速度。目前课程内容集中于经典加密算法（如 RSA、AES），而对后量子密码、零知识证明、联邦学习中的隐私保护等新兴领域涉及较少。学生普遍反映“学的知识用不上”，缺乏对未来技术趋势的认知。

其次，教学方式单一，学生学习动机不足。密码学涉及大量抽象数学与复杂协议逻辑，易引发畏难情绪。当前教学多采用“教师讲—学生听”的线性模式，缺乏情境导入与互动设计。基于 ARCS 动机模型分析发现，学生在“注意力”“相关性”“自信心”三个维度得分偏低，直接影响其学习投入[5]。再次，实践教学碎片化，综合能力训练不足。多数实验为孤立的验证性任务，缺乏综合性、对抗性和真实场景支撑[6]。学生无法锻炼系统设计、漏洞挖掘与应急响应能力，与企业岗位所需的“攻防一体、系统思维”存在明显差距。此外，课程思政融入浅层化，育人实效有限。尽管部分课程尝试加入国家安全法等内容，但多停留在“贴标签”式宣传，未能真正实现技术与价值的深度融合[7]。

2 教学改革思路

立足新工科背景下对高素质信息安全人才的迫切需求，针对当前密码学与网络安全教学中存在的内容滞后、方式单一、实践脱节、育人浅层等问题，提出以“能力生成”为核心、“价值塑造”为引领的教学改革思路。改革遵循“以学生发展为中心、以学习成果为导向、持续改进”的教育教学理念，依托成果导向教育（OBE）反向设计框架，首先明确毕业生在企业岗位中应具备的知识、能力与素质目标，再据此重构课程体系，确保教学活动始终服务于人才培养的根本目的。

同时，引入 ARCS 动机设计模型，通过问题引导、案例驱动、成功体验等方式增强学生学习主动性，解决“不愿学”“不敢做”的心理障碍。例如，通过讲述 Cambridge Analytica 数据泄露事件吸引注意力；通过分析企业实际应用场景增强知识的相关性；通过分层实验任务让学生获得成就感，提升自信心；通过成果展示与竞赛激励带来满足感。

在此基础上，构建“输入—过程—输出—反馈”四位一体的教学改革总体架构（如图 1 所示）：以动态更新的资源库实现教学内容与时俱进；以“双轮驱动”模式推动师生共研、生生互学；以情景化实验和赛教融合强化综合能力训练；以课程思政协同贯穿全程，实现技术能力与职业伦理的双重塑造。

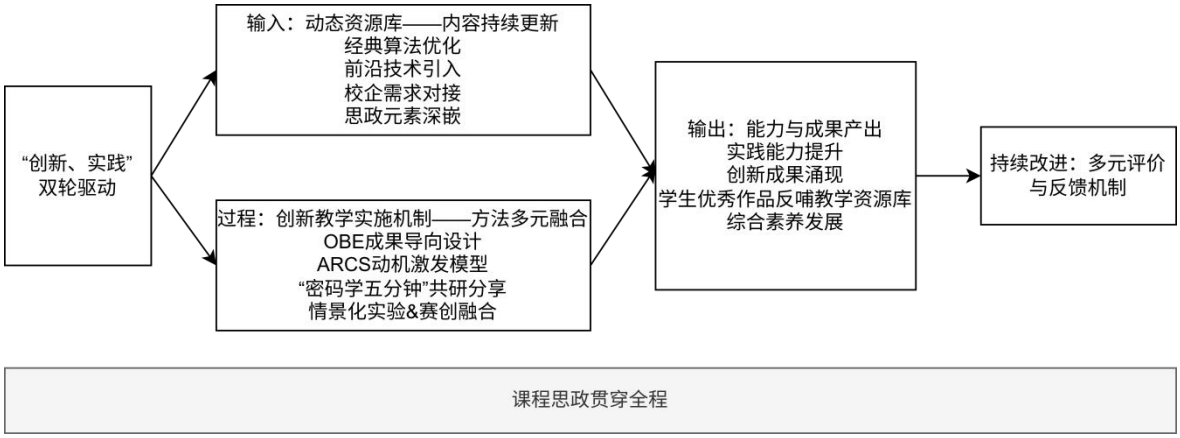

图 1 教学改革总体架构（笔者自绘画）

该模式将实现三大转变：从“知识灌输”向“能力塑造”转变；从“被动接受”向“主动探究”转变；从“技术训练”向“价值引领”转变，全面回应新工科背景下人才培养的新要求[8]。

3 教学具体措施

3.1 课程内容改革

为确保课程建设与新时代信息安全人才需求高度契合，课程团队坚持“以产出为导向”的 OBE 理念，通过企业调研与毕业生追踪，深入了解产业在数据安全、隐私计算等领域的实际需求，并系统梳理《密码学与网络安全》课程应具备的知识体系与关键能力。基于产业反馈与职业发展路径，将需求转化为可衡量的教学目标，从知识、能力、素质三个维度进行系统设计：知识层面夯实基础并融入前沿算法；能力层面强化算法实现、漏洞分析与方案设计；素质层面注重工程伦理、隐私保护意识与创新思维[9]。该目标体系有效指导了教学内容的优化，实现课程建设与行业需求的深度对接。

本次课程改革秉持"夯实基础、前瞻引领"的教学理念，致力于构建一个贯通经典与前沿的密码学知识体系。在教学实施中，将密码学核心原理作为教学基石，系统讲授对称密码、非对称密码、哈希函数等经典算法的设计思想、数学基础与安全机制，确保学生建立扎实的知识框架。在此基础上，课程将前瞻性地融入后量子密码、全同态加密、零知识证明等关键前沿领域[10]，同时，结合行业实践，剖析蚂蚁链、腾讯 TrustSQL 等平台中密码技术的落地案例，提升学生的现实感知力[11-1]。通过揭示密码学从经典理论到现代应用的演进脉络，引导学生既深入理解当前网络安全的核心基石，又敏锐把握未来技术发展的趋势动向。

3.2 构建“密码学五分钟”探索分享机制

为将密码学的前沿视野有效转化为学生的内在学习驱动力，本课程将创新性地设立“密码学五分钟”探索分享环节。打破传统教学中“教师讲、学生听”的单向知识传递模式，推动教学范式向师生共研、生生互学转变。在该环节实施中，鼓励学生以个人或小组形式，主动扮演知识发现者的角色。具体任务包括但不限于：密码学的小故事、持续追踪密码学领域会议的最新研究成果；选择性阅读发表于重要期刊的前沿论文；深入分析知名科技企业在数据安全、区块链、隐私计算等领域的密码学应用实践。

学生需将探索所得进行系统梳理与提炼，并形成个性化的见解。每周课程将固定安排特定时段，邀请若干位学生走向讲台，在五分钟时间内向全体师生展示其最新发现与独到思考。分享内容可涵盖新技术解读、经典算法的新应用、有深度的安全性分析，或是提出值得探讨的开放性问题。通过这种“自主探索-共同分享”的良性循环，不仅能够有效点燃学生的学术好奇心与探究热情，更能促进观点碰撞与思维激荡，最终将整个课堂打造成为一个充满活力、教学相长的密码学学术共同体。

3.3 实验教学改革

3.3.1 实验设计分层递进

为破解传统密码学实验脱离实际、学生“知其然不知其所以然”的问题，本课程以情景化任务驱动为核心，构建“验证—设计—对抗”三级递进式实验体系。第一层级为验证性实验，将实验嵌入真实场景，如在“电商平台数据泄露”背景下实现 SHA-256+Salt 密码保护，或在“政务文件传输”中验证哈希完整性，帮助学生在问题情境中理解基础原理。第二层级为设计性实验，通过项目式任务锻炼工程思维，如设计远程医疗病历加密系统或校园社交 App 的端到端加密功能，综合运用多种密码技术，提升系统设计与方案整合能力。第三层级为对抗性实验，开展红蓝攻防演练，如模拟金融系统中间人攻击防御，或参与 CTF 勒索软件解密挑战，培养学生实战能力与应急响应素养。通过层层递进的情景化实践，实现从知识理解到综合应用再到实战创新能力的全面提升。

3.4 实验平台与资源建设

为支撑情景化实验的有效实施并促进学生创新成果转化，首先，依托 CryptoHack、PicoCTF 等国际知名开源安全教学平台作为技术底座，充分发挥其内容丰富、交互性强、社区活跃的优势。提供涵盖古典密码、RSA 攻击、椭圆曲线等主题的交互式题目，支持即时反馈与排行榜激励[12][13]。同时，通过游戏化学习和 CTF 挑战激发学生的学习兴趣与竞争意识[14]。

其次，自主建设情景化实验资源库，将全球典型网络安全事件转化为可操作的教学案例。例如，基于“Facebook-Cambridge Analytica 数据滥用事件”设计隐私访问控制实验，引导学生实现基于属性加密（ABE）的细粒度权限管理；结合“西北工业大学遭 APT 攻击”事件，剖析攻击链中密码认证环节的薄弱点，组织学生设计多因素认证与零信任加固方案[11-2]。每个案例均配套背景资料、技术分析文档与分层实验任务卡，形成“事件导入—问题驱动—方案设计—实践验证”的完整教学闭环。

尤为重要的是，建立学生创新成果遴选与反哺机制，鼓励学生成果从“作业”走向“资源”。设立“创新贡献学分”，支持学生以开源项目、技术博客、竞赛获奖等形式替代部分考核内容，进一步激发创造力。让优秀作业‘从纸上走到线上’，真正实现教学相长、生生互学的学术共同体愿景。”

3.5 课程思政的有机融合

改变以往“生硬插入”的做法，课程将思政元素深度嵌入专业知识点中。在讲授古典密码时，结合中国古代阴符、藏头诗等军事通信智慧，增强学生的文化自信；在讲解数字签名时，解读《电子签名法》《密码法》关键条款，培养法治意识；在分析数据泄露事件时，以 Facebook-Cambridge Analytica 事件为例[11-3]，引导学生认识隐私保护的重要性；在介绍国产密码标准 SM2/SM3/SM4 时，讲述其研发历程与国际竞争背景，激发科技报国情怀。

此外，开设“密码人的使命与担当”主题研讨课，邀请行业专家讲述一线实战经历与伦理抉择，讨论勒索软件、暗网交易中的技术滥用风险，帮助学生树立正确的职业观与道德底线。通过这些深度融合的设计，课程思政不再是“外挂”，而是成为学生专业成长的重要组成部分，真正实现“润物细无声”的育人效果。

3.6 考核评价改革

为突破“一张试卷定成绩”的局限，课程构建了多元化、过程性的评价体系。总评成绩由三部分构成：过程参与占 30%，包括“五分钟分享”表现、小组讨论贡献、课堂表现；实践能力占 40%，涵盖编程作业、系统设计方案、CTF 挑战赛成绩；期末考核占 30%，针对课程认知目标，通过精准化命题开展闭卷考试。例如，本学期闭卷考试试题覆盖了课程主要内容，不仅考查须记住的事实性知识且注重对概念性知识和过程性知识的理解和应用的考核，个别题目还对学员利用已学知识分析复杂问题和创造性求解能力进行了考核。

特别地，课程实行“成果替代制”：学生可用参加信息安全竞赛获奖、发表技术博客、完成开源项目等方式替代部分考试分数，鼓励创新产出与社会影响力。这种评价机制不仅关注结果，

更重视学习过程与能力发展，有效激发了学生的积极性与创造性，形成了正向激励循环。

4 结语

《密码学与网络安全》课程教学改革可以为学生提供更全面的理论体系，培养出更具综合素质和国际竞争力的密码科学与技术专业人才，为推动网络空间安全领域人才培养做出积极贡献。教学改革方案通过内容更新、方法创新、机制重构，可以有效提升密码学课程的教学质量和效果，为培养具有创新精神和实践能力的高素质信息安全专业人才提供有力支持。然而，现代密码学教学改革并非一蹴而就，需要我们不断探索和实践，逐步进行完善和优化。

参考文献:

[1] 王平辉，赵俊舟，张迪. 密码学课程教学改革探索[J]. 高教学刊, 2025(8): 53-57.

[2] 孙士锋. 基于“固本索源+前沿引领”的现代密码学课程教学改革探讨[J]. 计算机教育, 2025(4): 12-16.

[3] 李志义. 成果导向的教学设计[J]. 中国大学教学, 2015(3): 32–39.

[4] KELLER J M. Development and use of the ARCS model of motivational design[J]. Educational Technology Research and Development, 1987, 35(3): 23-34.

[5] 吴丹，刘建华. 基于 ARCS 模型的信息类课程教学设计研究[J]. 电化教育研究, 2020, 41(7): 102–108.

[6] 冯涛，王晓燕. 情景式教学在信息安全实验课程中的应用[J]. 实验技术与管理, 2022, 39(5): 189-193.

[7] 张伟，陈静. 开源平台驱动的网络安全实践教学模式探索[J]. 计算机教育, 2023(10): 45-50.

[8] 徐晓飞，王泉. 新工科人才培养模式改革探索[J]. 高等工程教育研究, 2018(2): 1-7.

[9] 黄天羽，李忠诚. CTF 竞赛与网络安全实践能力培养[J]. 中国电化教育, 2021(6): 114-120.

[10] BONEH D, SHOUP V. A Graduate Course in Applied Cryptography[M]. Cambridge: Cambridge University Press, 2023.

[11] MEYER D, BOSSERT M, KLEIN A, et al. Integrating real-world cyber incidents into university-level security education: A case study approach[C]//Proceedings of the 2023 IEEE Frontiers in Education Conference (FIE). College Station, TX: IEEE, 2023: 1–8.

[12] C RYPTO HACK. An interactive platform for learning modern cryptography[EB/OL]. London: CryptoHack Ltd., 2024[2025-04-05]. https://cryptohack.org/.

[13] PICOCTF. Cybersecurity competition for students[EB/OL]. Pittsburgh: Carnegie Mellon University, 2024[2025-04-05]. https://picoctf.org/.

[14] AL-MOMEN Z, KHAN F, ALTAMEEM A, et al. Enhancing student engagement in cryptography through gamified learning and CTF challenges[C]//Proceedings of the 2022 International Conference on Computational Science and Computational Intelligence (CSCI). Las Vegas, NV: IEEE, 2022: 1023–1028.