

“大思政课”背景下密码课程教学模式改革与实践

蒋芃^{1*}, 徐蕾¹, 祝烈煌¹

(¹ 北京理工大学 网络空间安全学院, 北京 100081)

摘要: 在“大思政课”建设背景下, 针对密码课程教学中存在的思政融入碎片化、理论与实践脱节、教学模式相对单一以及评价维度不够完整等问题, 本文结合密码课程交叉性强、战略属性突出、理论与实践并重的学科特点, 系统分析其教学改革的现实基础, 构建了密码课程与“大思政课”深度融合的实施路径。在此基础上, 提出“理论+实践+思政”三位一体教学模式, 从融合原则、思政元素提炼、案例库建设、教学模块设计、实施流程与典型案例实践等方面进行了系统设计。研究采用文献分析、教学设计、行动研究与效果评价等方法, 围绕分组密码、Hash 函数、公钥密码与数字签名等典型内容开展教学实践。结果表明, 该模式有助于增强课程的现实关联性、问题导向性和育人整体性, 能够在提升学生知识理解、实践应用和综合分析能力的同时, 促进其国家安全意识、法治意识和责任意识的形成。本文研究可为网络安全及相关理工科课程开展课程思政与教学模式创新提供参考。

关键词: 大思政课; 密码课程; 课程思政; 教学模式改革; 三位一体

DOI: <https://doi.org/10.71411/jyyjx.2026.v1i4.1291>

"Great Ideological and Political Course" Context : Reform and Practice of Cryptography Course Teaching Models

Jiang Peng^{1*}, Xu Lei¹, Zhu Liehuang¹

(¹ Beijing Institute of Technology, School of Cyberspace Security, Beijing, 100081, China)

Abstract: Under the background of "Big Ideological and Political Education" construction, addressing issues such as fragmented ideological integration, disconnection between theory and practice, relatively singular teaching models, and incomplete evaluation dimensions in cryptography course instruction, this paper systematically analyzes the practical foundation for teaching reform by leveraging the interdisciplinary nature, prominent strategic attributes, and balanced emphasis on theory and practice characteristic of cryptography courses. It establishes an implementation pathway for the deep integration of cryptography courses with "Big Ideological and Political Education." On this basis, a trinity teaching model of "theory+practice+ideology" is proposed, with systematic design encompassing integration principles, ideological element extraction, case library construction, teaching module design, implementation processes, and typical case practices. The study employs methods such as literature analysis, instructional desi-

作者简介: 蒋芃 (1988-), 女, 博士, 研究员, 博士生导师, 研究方向: 密码学, 信息安全, 区块链, 网络空间安全

徐蕾 (1986-), 女, 博士, 研究员, 博士生导师, 研究方向: 隐私保护, 区块链安全

祝烈煌 (1976-), 男, 博士, 教授, 博士生导师, 研究方向: 网络空间安全

通讯作者: 蒋芃, 通讯邮箱: pengjiang@bit.edu.cn

gn, action research, and effectiveness evaluation to conduct teaching practices centered on typical content including block ciphers, hash functions, public-key cryptography, and digital signatures. The results indicate that this model helps enhance the course's relevance to reality, problem-oriented approach, and holistic educational integrity for Homo sapiens, while improving students' knowledge comprehension, practical application, and comprehensive analytical abilities, it also fosters the development of their national security awareness, legal consciousness, and sense of responsibility. This research can provide references for cybersecurity and related science and engineering courses in implementing ideological education and innovating teaching models.

Keywords: Big Ideological and Political Education; Cryptography Course; Curriculum Ideology and Politics; Teaching Model Reform; Trinity

引言

党的二十大报告强调为党育人、为国育才,《高等学校课程思政建设指导纲要》提出将思政工作贯穿教学全过程^[1]。高校课程改革转向知识、能力与价值协同培养,“大思政课”推动课程全场域育人。理工科课程需回应国家需求、发挥价值引导作用,网络空间安全学科更应推动专业与思政教育同向同行^[2]。密码学是网络空间安全领域的核心基础课程,兼具理论性和实践性,广泛应用于网络通信和电子商务等领域^{[3][4]}。随着网络安全形势日益严峻,密码技术在维护国家安全和信息基础设施安全中的作用不断提升,密码课程也成为信息安全人才培养体系中的关键课程^{[4][5]}。相较一般课程,密码课程更具思政融入优势:其一,密码技术直接服务国家安全和公共安全,天然承载国家安全观教育^{[5][6]};其二,我国密码事业实践蕴含丰富的科技报国、自主创新素材;其三,密码应用始终伴随法律边界、伦理约束和责任意识问题,将法治内容融入教学,有助于培养学生的职业素养^{[4][6]}。因此,以密码课程推进“大思政课”改革具有现实意义。

现有研究表明,网络安全类和密码类课程思政改革已具备一定基础。相关成果多从知识目标、能力目标和价值目标重构课程体系,并围绕国家安全观、科技报国、法治意识、职业伦理和科研精神提炼思政元素^{[4][5]}。在教学设计上,案例教学、翻转课堂、混合式教学、项目驱动和讨论式教学较为常见^{[3][6][7]}。如张雪莲提出知识、能力、思政三位一体的课程目标体系;苏婷等强调从法制法规、家国情怀和科研精神三个维度挖掘思政资源;王平辉等则从内容、方法和实践环节改革入手,提出通过案例教学和多元评价提升教学质量^{[3][4][5]}。这些研究为本文提供了重要参考。

现有研究的不足:一是停留于“课程思政”的局部嵌入,对如何从“大思政课”视角统筹国家战略、课程体系与人才培养目标论述不足^{[4][5]};二是多为经验总结,缺乏基于“目标—内容—方法—评价”的系统设计^{[3][6]};三是密码课程在“理论+实践+思政”框架下实现知识、能力、价值协同提升的研究不充分,尤其对混合式教学、情景模拟和案例资源库建设缺少整体性讨论^{[3][5]}。

本文聚焦“大思政课”背景下密码课程教学模式改革与实践,围绕国家安全观、科技报国和信息安全伦理等育人要素,探索密码课程与“大思政课”深度融合的实施路径。研究目标包括:系统梳理课程思政元素,构建专业教育与价值引导相统一的内容框架;针对理论与实践脱节、教学方式单一和思政融入碎片化等问题,设计“理论+实践+思政”三位一体教学模式;并通过案例教学、项目驱动和混合式教学开展实践,验证实施效果。研究综合采用文献分析、教学设计、行动研究等方法,通过课堂观察、作业、实验报告、项目成果和问卷反馈等数据,对改革实施效果进行分析,为后续课程优化提供依据^{[3][4][5][6][7]}。

1 “大思政课”背景下密码课程教学改革的现实基础

密码学课程的学科特征分析: 密码技术不仅是保障信息保密性、完整性和真实性的关键手段, 也是维护国家安全、数字主权和网络空间安全的重要基础支撑^{[3][4]}。课程中涉及的算法安全、自主可控、国密体系和安全治理等知识点, 与总体国家安全观和网络强国建设高度契合, 因此密码课程天然具有鲜明的战略育人价值。密码课程既要求学生掌握算法原理和安全机制, 也要求其具备实验实现、协议分析和场景应用能力^{[3][5]}。如果教学只停留在概念和公式层面, 学生难以形成完整的专业能力结构。因此, 课程改革必须把理论学习、实验验证和应用场景统筹起来, 这也是后文提出三位一体教学模式的重要依据。

现有教学存在的主要问题: 当前密码课程思政融入存在碎片化现象。部分教学实践虽然能够插入科学家事迹、国家安全案例或法律法规内容, 但这些内容往往以补充性方式出现, 尚未与课程目标、知识模块、教学活动和评价方式形成系统衔接^{[4][6]}。因此, 思政内容容易停留在浅层嵌入阶段, 难以形成持续稳定的育人效果。传统密码课程多采用教师讲授为主的方式, 强调概念讲解和公式推导, 但在互动性、应用性和学生主体性方面存在不足^[3]。对于抽象性较强的密码原理, 如果教学方式过于单一, 学生容易产生畏难情绪, 学习主动性和实践参与度难以充分调动。因此, 有必要推动案例教学、讨论式教学、项目驱动和混合式教学等方式协同应用。现有密码课程评价偏重结果考核, 多以期末考试成绩作为主要依据, 对学习过程、实践表现和价值塑造成效关注不足^{[3][5]}。这种评价方式难以全面反映学生在实验能力、项目能力和国家安全意识、责任意识等方面的发展状况。因此, 课程改革需要构建知识、能力、价值相统一的多维评价体系。

教学改革目标定位: 密码课程改革首先要帮助学生构建系统完整的密码学知识体系, 使其准确理解基本概念、核心理论、经典算法和典型应用场景^{[4][5]}。课程知识目标应强调体系化理解, 避免停留在“知道概念、记住结论”的浅层学习。课程改革还应着力培养学生在算法分析、实验实现、场景建模、系统设计和综合应用等方面的专业能力^{[3][5]}。密码课程学习不应仅以掌握原理为终点, 而应进一步推动学生将知识迁移到真实安全问题中, 形成解决复杂问题的能力。密码课程改革的落脚点在于价值目标的实现, 即通过课程教学引导学生形成国家安全观、科技报国意识、法治观念和信息安全伦理责任^{[4][5][6]}。课程不仅要回答“技术是什么、怎么做”, 还要回答“技术为什么重要、应当如何使用、应当为谁服务”。

2 密码课程与“大思政课”融合的路径构建

融合的基本原则: 在“大思政课”背景下推进密码课程改革, 首要原则是坚持知识传授、能力培养与价值引领相统一^{[3][4][5]}。密码课程既承担基础理论与应用机制教学任务, 也承担培养学生工程实践能力、创新意识和价值判断能力的职责。课程思政不能作为外加内容附着于专业知识之外, 而应从知识点内部自然生成, 通过课程目标、内容组织和教学活动设计, 实现专业教育与价值引导同向同行。密码课程与“大思政课”融合, 还应坚持历史、现实与未来三维贯通^{[3][4][5]}。历史维度有助于学生理解密码学发展脉络和我国密码事业演进, 增强文化认同与学科自信; 现实维度使学生认识密码技术与国家安全、社会治理、个人隐私保护的联系; 未来维度通过国密算法演进、区块链安全、后量子密码等前沿议题, 拓展视野并激发创新兴趣。密码课程思政融入还应坚持显性教育与隐性教育相结合^{[4][7]}。显性教育体现在国家安全观、法治意识和科技报国等内容的明确讲授, 隐性教育则体现在案例分析、实验项目、课堂讨论和情景任务中。只有将二者结合, 才能避免生硬灌输, 实现润物无声的育人效果。

密码课程思政元素的提炼: 国家安全观是密码课程核心的思政元素。密码技术不仅关系个人隐私和商业安全, 更关系国家政治安全、经济安全和网络空间主权^{[4][5][8]}。因此, 在对称密码、公钥密码和密码应用模块中, 应结合国密算法、自主可控体系和关键基础设施安全内容, 引导学生

理解密码技术在国家安全体系中的地位。密码课程中可从中国数学传统、密码技术创新历程和代表性科学家贡献中提炼科技报国与文化自信元素^{[3][4]}。例如,可通过中国剩余定理、豪密算法、国密算法发展和科学家攻关案例,引导学生认识中华优秀传统文化和我国密码事业发展的价值,增强家国情怀与创新意识。法治意识与伦理责任是密码课程不可或缺的育人内容。密码技术具有“双刃剑”特征,必须在法律规范和伦理约束下使用^{[4][6][9][10]}。因此,课程中应结合《密码法》《网络安全法》《数据安全法》以及隐私泄露、网络诈骗等案例,引导学生明确技术使用的制度边界和职业责任。密码学强调严密逻辑、反复验证和持续迭代,其发展过程本身蕴含工匠精神与科研精神^{[4][5]}。通过算法推导、实验验证、漏洞分析和科研案例引入,可引导学生形成严谨求真、精益求精、敢于质疑和勇于创新的专业品格。

课程思政案例库建设:历史案例库围绕古典密码、中国数学传统和密码发展史构建^{[4][5]}。如恺撒密码、中国剩余定理、豪密算法和我国密码事业发展历程等,既增强课程趣味性,又承载文化自信与科技报国教育。现实案例库围绕典型网络安全事件、国家安全场景和社会热点问题建设^{[3][6][7]}。如隐私泄露、勒索攻击、电子政务安全和金融支付安全等案例,能够增强学生的问题意识、责任意识和风险意识。前沿案例库围绕国密算法、区块链安全、隐私计算和后量子密码等方向构建^{[3][4]}。前沿案例有助于体现课程与学科发展同频共振,增强学生创新兴趣和继续深造意愿。

融合路径的具体表达:为避免思政融入停留在经验操作层面,可建立“章节内容—思政元素—教学活动”映射表^{[4][5][7]}。例如,将分组密码对应国家安全观和自主可控意识,将 Hash 模块对应科研精神与技术伦理,将数字签名模块对应法治意识与社会信任责任,并匹配案例导入、课堂讨论、实验验证和项目活动。在映射关系基础上,还需构建“目标-内容-方法-评价”闭环机制^{[3][4][6]}。课程改革应围绕知识、能力、价值目标展开,在内容上嵌入思政元素,在方法上综合运用案例教学、项目驱动和混合式教学,在评价上纳入课堂参与、实验表现、项目成果和问卷反馈等指标,实现由内容嵌入走向模式生成。

3 “理论+实践+思政”三位一体教学模式

教学模式总体框架:“理论+实践+思政”三位一体教学模式,是针对密码课程理论抽象、实践要求高且具有鲜明育人属性而提出的整体性教学设计方案^{[3][4][5]}。该模式以知识传授为基础、能力培养为核心、价值引领为灵魂,强调在课程教学全过程中实现专业知识学习、实践能力训练和思想价值塑造的协同推进。该模式以课前导学、课中建构、课后拓展和评价反馈为基本运行链条^{[3][5][7]}。课前通过案例推送和问题导学激发兴趣,课中通过理论讲授、讨论互动、实验验证和项目训练完成知识建构,课后通过资料检索、专题报告和反思总结促进深化内化,最后通过知识、过程和实践评价形成改进闭环。

理论教学模块设计:案例导入是密码课程理论教学的重要起点。通过引入国家安全事件、现实工程问题和典型应用场景,可有效缩短抽象理论与现实世界之间的距离,使学生在具体问题中理解知识用途与价值^{[3][4][5]}。如以数据泄露引出对称加密,以电子合同引出数字签名,以自主可控需求引出国密算法。讨论式教学与翻转课堂有助于增强学生主体性和课堂深度^{[3][6]}。对于基础概念和流程,可通过课前视频和阅读材料让学生预习;对于算法设计思想、安全性分析和场景适配等内容,则放到课堂中通过小组讨论、问题答辩和师生互动完成,从而推动学生由“听知识”转向“建构知识”。章节教学结束后,应对知识意义、技术价值和社会责任进行总结提升^{[4][5]}。这种总结不是机械拔高,而是建立在本章知识结构和案例分析基础上的自然延伸,如由 Hash 函数引出技术边界与安全责任,由数字签名引出数字信任与规则意识。

实践教学模块设计:验证性实验是密码课程实践教学的基础环节。通过算法实现、结果验证和基础仿真实验,可帮助学生将抽象理论转化为可观察、可操作的实践认知^{[3][4][5]}。实验内容应紧

扣课程核心知识点,同时兼顾原理解、安全边界和规范操作意识。综合性项目是推动学生由“掌握知识”走向“综合应用”的关键环节^{[3][5]}。课程围绕安全通信、身份认证、数字签名和系统安全主题构建项目任务,引导学生在需求分析、方案设计和技术实现过程中整合知识,并在协作中培养责任意识和工程素养。情景模拟与攻防体验能够增强学生对密码技术价值、边界和责任要求的理解^{[4][11][12]}。通过设计数字签名伪造、协议缺陷分析和攻防对抗等情境,让学生在“做中学”的过程中理解技术与非法攻击之间的边界,强化法治意识和底线意识。

混合式教学支持体系:线上资源建设是三位一体教学模式的重要支撑^{[4][5]}。课程围绕算法原理微课、案例材料、法律法规解读、实验指导和拓展任务建设资源体系,为学生课前预习、课后拓展和个性化学习提供支持。线下教学重点承担深度研讨、能力训练和价值引领任务^{[3][6]}。通过案例讨论、实验指导、成果展示和答辩交流,帮助学生把线上获得的基础知识转化为问题意识、分析能力和价值判断。教师能力支撑是三位一体教学模式落地实施的关键保障^{[4][6]}。教师不仅要具备课程知识整合能力和教学设计能力,还要能够准确提炼思政元素并在课堂教学中自然融入。为此,需要集体备课、案例共建、专题教学研讨等方式提升教师课程思政素养和课堂驾驭能力。

4 教学实施过程与典型案例实践

教学实施流程:课前导学通过问题清单、案例材料、视频资源和预习任务,引导学生在进入课堂前初步了解相关知识背景、现实场景及其价值议题^{[5][7]}。例如,在讲授分组密码前推送数据泄露案例,在讲授数字签名前布置电子合同和身份认证材料。课中建构围绕“案例导入—理论讲授—互动讨论—实验验证—总结提升”展开^{[3][5][7]}。教师讲授知识点时突出“解决什么问题、如何解决、适用什么场景、有哪些边界”四个层面,通过小组讨论和课堂演示推动学生把理论认知转化为场景理解和价值判断。课后拓展通过资料搜集、专题报告、热点追踪和反思总结,帮助学生持续深化课堂中的知识认知和价值判断^{[4][5]}。例如,在分组密码教学后比较 AES 与 SM4 的应用特点。

典型教学案例:以 AES 与 SM4 对比教学为例,可将算法原理讲授、应用场景分析和国家安全教育有机结合^{[3][4]}。教学中通过数据泄露和关键系统安全问题导入分组密码需求,在讲授基本原理后,引导学生比较国际算法与国产算法在现实场景中的意义,从而增强国家安全意识和自主可控意识。围绕 MD5 碰撞、消息完整性验证设计教学活动,可将技术原理、科研精神和伦理责任教育结合起来^{[3][4]}。通过漏洞案例、实验演示和课堂讨论,帮助学生理解算法演进的科学逻辑及技术应用必须遵守规范和边界。以 RSA 或 SM2 及其在身份认证、数字签名和可信通信中的应用为核心,可将密码原理教学与规则意识和社会信任机制教育结合起来^{[3][6]}。

实施过程中的阶段性表现:从课堂观察和任务完成情况看,随着教学模式改革推进,学生在课堂互动、任务投入和讨论深度方面表现出积极变化^{[5][7]}。课前导学使学生带着问题进入课堂,案例导入和讨论式教学增强了课堂的现实关联性,学生不再只关注“怎么做题”,而更愿意思考技术与安全、规则和责任之间的关系。在持续的理论学习与实践训练过程中,学生在知识理解、实验实现、场景分析和综合应用等方面表现出较为积极的变化^{[3][4]}。同时,通过国家安全案例、国密算法应用和法律法规引入,学生对国家安全观、法治意识和责任意识的认知也更加明确。

5 结语

本文围绕“大思政课”背景下密码课程教学模式改革与实践展开系统研究,系统分析了课程改革的现实基础,构建了密码课程与“大思政课”深度融合的实施路径,并在此基础上设计了“理论+实践+思政”三位一体教学模式。研究表明,密码课程不仅是专业技术课程,也是能够承载国家安全观和信息安全伦理责任教育的重要实践平台。通过教学实施可以看出,该模式能够较好解决传统密码课程中理论与实践脱节、课堂参与度不足和思政融入碎片化等问题,有利于增强

课程的现实关联性、问题导向性和育人整体性。学生在知识掌握、实验实现和综合应用等方面表现出较为积极的变化,同时在国家安全意识和责任意识等方面也呈现出更加明确的认知提升趋势。

参考文献:

- [1] 习近平. 高举中国特色社会主义伟大旗帜为全面建设社会主义现代化国家而团结奋斗—在中国共产党第二十次全国代表大会上的报告[M]. 北京: 人民出版社, 2022: 33-34.
- [2] 中华人民共和国教育部. 高等学校课程思政建设指导纲要[EB/OL]. (2020-06-01)[2025-02-26]. http://www.moe.gov.cn/srcsite/A08/s7056/202006/t20200603_462437.html.
- [3] 张雪莲. 密码学课程思政教学改革实践探索[J]. 网络安全技术与应用, 2025(6): 97-100.
- [4] 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.
- [5] 苏婷, 蒋琳, 魏宇虹. 融入思政的密码学课程教学探索[J]. 计算机教育, 2025(9): 79-83.
- [6] 赵柳, 游子毅. 课程思政建设背景下网络信息安全课程教学的探索与实践[J]. 电脑知识与技术, 2024, 20(4): 90-92.
- [7] 张辉. 应用型本科院校“信息安全技术”课程思政的教学改革[J]. 网络安全技术与应用, 2021(10): 107-109.
- [8] 全国人民代表大会常务委员会. 中华人民共和国密码法[S]. 北京: 中国民主法制出版社, 2019.
- [9] 全国人民代表大会常务委员会. 中华人民共和国网络安全法[S]. 北京: 中国民主法制出版社, 2016.
- [10] 全国人民代表大会常务委员会. 中华人民共和国数据安全法[S]. 北京: 中国民主法制出版社, 2021.
- [11] 周庆, 胡月. “对抗式学习”教学法及其在计算机网络安全课程中的应用[J]. 计算机教育, 2023(4): 58-63.
- [12] 胡为, 刘伟, 李小智, 等. 基于实战能力培养的网络安全课程教学创新体系建设[J]. 计算机教育, 2024(2): 85-89.