Advances in Education 教育进展, 2026, 16(5), 1519-1525
Published Online May 2026 in Hans. https://www.hanspub.org/journal/ae
https://doi.org/10.12677/ae.2026.1651019

Hans汉斯

面向拔尖人才培养的《密码分析学》课程教学改革

王　薇，孙晓涵

山东大学网络空间安全学院，山东　青岛

收稿日期：2026年4月22日；录用日期：2026年5月20日；发布日期：2026年5月27日

摘　要

针对网络空间安全领域对拔尖人才培养的迫切需求，聚焦《密码分析学》课程中理论与实践脱节、教学内容前沿性不足等问题，探索系统化教学改革路径。构建“现代密码分析理念 + 数学模型 + 编程测试”融合的教学体系，将团队科研成果与国际前沿研究融入课堂，实现研教融合；同时，通过过程性评价机制强化实践导向，并将课程思政贯穿教学全过程。课程高阶性、创新性与挑战度得到显著提升，教学内容的前沿性与体系性明显增强，学生从分析视角理解设计问题的能力得到强化，系统性思维与原始创新能力得到有效培养。该教学改革实现了知识传授、能力培养与价值引领的有机统一，可为网络空间安全相关课程改革提供参考，具有良好的推广价值与应用前景。

关键词

拔尖人才培养，密码分析学，教学改革

Teaching Reform of the Cryptanalysis Course Aimed at Cultivating Top Talents

Wei Wang, Xiaohan Sun

School of Cyber Science and Technology, Shandong University, Qingdao Shandong

Received: April 22, 2026; accepted: May 20, 2026; published: May 27, 2026

Abstract

In response to the urgent need for cultivating top talents in cyberspace security and the challenges in the Cryptanalysis course, including the gap between theory and practice and limited exposure to frontier content, a systematic teaching reform has been implemented. An integrated teaching

文章引用: 王薇, 孙晓涵. 面向拔尖人才培养的《密码分析学》课程教学改革[J]. 教育进展, 2026, 16(5): 1519-1525.
DOI: 10.12677/ae.2026.1651019

system combining modern cryptanalysis concepts, mathematical modeling, and programming exercises has been established, incorporating the teaching team's research achievements and international advances to foster the integration of research and teaching. The course emphasizes practical skill development through a formative assessment framework, and ideological and ethical education is embedded throughout the curriculum. This approach cultivates students' analytical abilities, systematic thinking, and capacity for original innovation. As a result, the course demonstrates increased rigor, innovativeness, and challenge, while its content exhibits enhanced frontier relevance and systematic coherence. Students gain strengthened abilities to analyze cryptographic problems and understand design issues from a research-oriented perspective. Overall, this teaching reform provides an effective integration of knowledge transmission, skill cultivation, and value guidance. It offers a scalable model for curriculum innovation in cyberspace security education and demonstrates potential for broader application in related disciplines.

Keywords

Cultivating Top Talents, Cryptanalysis, Teaching Reform

1. 引言

密码是国家重要战略资源，是保障网络与信息安全的核心技术和基础支撑。密码安全直接关系国家政治安全、经济安全、国防安全和信息安全[1]。2016 年，由中央网络安全和信息化领导小组办公室、国家发展和改革委员会、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》[1]指出，“网络空间的竞争，归根结底是人才竞争”。伴随人工智能、量子计算等新兴技术的快速迭代，国家对高素质密码学人才的需求呈快速增长态势。高校作为网络安全人才培养的主阵地，其课程教学质量直接决定了国家在该领域的核心竞争力。

新时代的密码学拔尖人才不仅需具备扎实的数学基础与算法功底，更需兼备卓越的工程实践能力与前沿技术洞察力。然而，传统密码学课程教学中理论抽象性强、实践支撑不足的问题愈发突出，同时面临教学模式与高阶能力培养不匹配、课程体系割裂及评价方式单一等挑战[2]。因此，探索产教融合、科教融汇的新路径，深化密码学课程体系与教学模式改革，已成为高校网络安全人才培养的迫切任务。

高校教育应以立德树人为核心，将思想政治教育融入教育教学全过程，实现价值引领与知识传授的有机融合[3]。鉴于此，为全面贯彻落实立德树人根本任务，积极响应国家密码强国战略，依托山东大学在密码学领域深厚的学科积淀，本课程改革旨在打破传统教学的路径依赖，将顶尖科研成果与前沿实战案例深度融入课堂，构建“先进理念 + 数学模型 + 自动化平台”的全方位教学体系。通过引入项目驱动、翻转课堂等多元化教学方法，重塑多维度的过程性评价机制，力求实现从“知识传授”向“核心素养与实战能力培育”的根本跃迁，为国家培养一批具备家国情怀、扎实技术与创新精神的密码学拔尖人才。

2. 传统教学面临的多维困境

2.1. 教学模式与高阶能力培养存在显著的“适配性鸿沟”

长期以来，课堂教学仍然深陷于以教师为中心、以知识传递为主导的传统路径依赖，多偏重离散化

[1]http://www.moe.gov.cn/srcsite/A08/s7056/201607/t20160707_271098.html

的算法推演与公式演绎，缺乏面向批判性思维、系统性分析能力与创新研究能力的整体性培养机制。同时，部分教材与教学内容更新滞后，未能及时反映学科领域的前沿研究进展与技术演进趋势，难以有效对接行业发展需求[4]。尤其是在引导学生研读国际前沿英文文献、理解科学研究范式及掌握规范化研究方法等方面，现有教学模式支撑不足，难以满足拔尖创新人才对高阶能力发展的要求。

2.2. 课程体系呈现“学科割裂”状态，理工融合与攻防实战脱节

当前课程体系中，传统学科壁垒依然明显，基础理论研究(理)与工程实践应用(工)之间缺乏有效衔接机制，尚未形成覆盖“基础理论–技术应用–原始创新”的全链条贯通式课程结构。在应对网络安全领域攻防技术快速迭代的背景下，教学内容更新节奏相对滞后，难以支撑“攻防一体化”能力培养目标[5]。与此同时，具有中国特色、自主可控的知识体系构建仍显不足，制约了学生对复杂安全问题的系统性认知与综合应对能力。

2.3. 学业评价体系偏离“能力导向”，存在严重的评价惯性

当前评价体系中，“重分数、轻能力”的导向仍然较为突出，笔试在成绩构成中占据主导地位。现有评估机制评价维度较为单一，对学生在实践能力、创新潜质及复杂问题求解能力等方面的考察不足[6]。同时，开放式命题、研究型任务与创作性考核等非标准化评价方式应用范围有限、实施深度不足，难以真实反映学生的综合素养与核心竞争力，制约了能力导向型人才培养目标的实现。

2.4. 数字化转型相对滞后，缺乏智能协同的教学资源生态体系

当前教学资源整体呈现碎片化分布特征，智能化教学手段应用不足，尚未构建起“知识图谱–能力图谱–数字资源”三维联动的数智化教学体系[7]。由此导致优质资源难以实现高效组织、精准检索与个性化推送。此外，跨院校、跨平台的师资协同机制与科研成果转化机制尚不完善，在一定程度上制约了教学模式创新与资源共享效率的提升。

2.5. 课程思政建设存在“表层化”与“弱融合”问题

在教学中，课程思政实践仍面临多重挑战。首先是融合深度不足，部分专业教师仍以理论推导与算法实现为主要教学内容，将思政元素视为外在附加内容，导致专业知识体系与价值引领之间缺乏内在逻辑耦合，难以实现“润物无声”的育人效果[8]。其次是元素挖掘不充分，对学科发展历程中所蕴含的家国情怀、科学精神与国家安全战略价值挖掘不够深入，未能充分发挥学科历史积淀与科研成果的育人功能。最后育人协同机制有待加强，尚未形成由高水平教师团队引领、贯穿教学全过程的协同育人体系，多主体协同育人格局尚不完善，学生对“科技报国”的使命认同与职业伦理意识仍有待进一步提升。

3. 密码分析学教学改革的系列措施

3.1. 构建高阶能力导向的“三元融合”创新教学模式

本课程以“先进理念 + 数学模型 + 自动化平台”为总体框架，系统构建以能力培养为导向的“现代密码分析理念 + 数学模型 + 编程测试”三元融合教学模式，推动教学重心由单一知识传授向高阶能力塑造与复杂问题求解能力培养转变。该模式的构建紧密对接国家关于深化教育教学改革与推进教育数字化转型的总体部署，体现“以学生为中心、以能力培养为导向”的教育理念。

在教学内容组织上，将密码分析领域近四十年的代表性研究成果进行教学化重构，转化为可理解、可操作的模块，并系统融入课堂与实验环节。依托团队自主研发的自动化密码分析平台，构建“抽象模型–算法实现–实验验证”的一体化转化路径，引导学生在“问题提出–模型构建–算法实现–结果验

证”的完整科研链条中深化对理论本质的理解。同时，通过“板书推导 + 代码验证”的协同机制，强化数学建模能力与工程实现能力的深度融合，促进学生形成研究导向的学习方式。

在实践环节中，课程围绕国际主流密码算法展开，构建贴近真实应用场景的案例体系，并引入高水平竞赛题作为训练载体。通过“理论分析－工具实现－攻击验证”的闭环训练机制，强化学生在真实攻防语境中的安全分析能力与工程实践能力，推动其形成“设计－分析”双向贯通的认知结构，从而提升对复杂密码系统的整体理解能力。

课堂组织上，课程将引导式教学、案例驱动学习与翻转课堂有机结合，并借助 BOPPPS 模式对教学流程进行优化。从问题导入到参与式学习，再到总结与反思，各个环节层层递进。学生通过分组讨论、板演推导与代码实现增强参与感，并在项目式学习中完成复杂问题的协同分析与系统设计。同时，通过项目式学习(PBL)组织学生开展面向复杂问题的协同分析与系统设计任务，并通过规范化报告与答辩机制强化表达与论证能力；依托在线教育平台，进一步拓展跨校协同育人场景，全面提升学生的综合素养、协作能力与创新能力。

3.2. 打造自主可控的“纵横贯通”优质课程内容体系

课程以系统性与前沿性为导向，构建结构化、层级化与动态演进相结合的课程内容体系，推动知识传授由碎片化向体系化、由静态化向动态化转变。该体系建设紧密对接国家关于深化本科教育教学改革与推进教育数字化转型的总体要求，服务于高素质创新型人才培养目标。

在纵向结构设计方面，依托教学团队自主编写的《密码分析学》《密码学概论》等系列教材及配套教学资源，构建“数学基础→密码理论→算法分析”的分层递进式知识架构。通过典型问题牵引与应用场景贯通，实现各层级知识之间的有机衔接，使学生在逐层深入的学习过程中完成从理论理解到综合应用的能力跃迁，从而有效避免知识碎片化与学习断层问题，强化知识体系的整体性与逻辑性。

在横向融合拓展方面，强化理工交叉与多学科协同融合机制，构建“基础理论－工程实现－创新应用”一体化知识框架。通过持续更新教学内容与案例资源库，将最新科研进展与行业实践动态融入教学过程，促进学生在跨领域知识整合中提升综合分析与创新能力，确保课程内容始终对接国际学术前沿与国家战略需求。

3.3. 实施多源数据融合的多元化评价体系改革

课程以能力发展为核心导向，构建过程性评价与结果性评价相结合的多维评价体系，推动评价机制由“以分数为中心”向“以能力发展为导向”转变。该评价体系的设计紧密契合国家关于深化教育评价改革、完善人才培养质量评价机制的总体要求，强调对学生综合素养与高阶能力的系统考察。

围绕“知识掌握、实践能力、创新素养”三个核心维度，构建结构化、多层次的评价指标体系，将传统单一的理论考核拓展为“理论理解－工程实现－问题建模”相结合的综合性评价模式。通过多维指标的协同作用，强化对学生知识迁移能力、实践应用能力及创新能力的整体评估，推动评价体系由结果导向向能力导向转型。

具体实施过程中，课程系统引入开放性问题、研究型任务、综合设计实验及学科竞赛成果等非标准化考核形式，通过构建复杂任务情境，考察学生在不确定环境下的分析路径与决策能力。此类评价方式不仅增强了考核的真实性与挑战度，也有助于体现学生个体差异，促进个性化发展，契合国家关于推进多元评价与创新人才培养的政策导向。

与此同时，依托长江雨课堂、中国大学 MOOC 等数字化教学平台，对学生课前预习、课堂互动、实验过程及课后反馈等学习行为进行全过程采集与分析，构建多主体参与的形成性评价机制。通过数据驱

动的教学反馈与个性化指导，实现对学生学习轨迹的动态跟踪与精准干预，逐步形成“学习–应用–反思–优化”的闭环培养路径，推动教育评价向智能化、精细化方向发展。

3.4. 驱动数智赋能的“双图谱”资源生态建设

顺应教育数字化转型趋势，课程以数据驱动与智能协同为核心，构建体系化、平台化与可持续演进的教学资源生态系统。该体系建设紧密契合国家关于推进教育数字化战略行动与构建新型教育基础设施的总体部署，为高质量人才培养提供有力支撑。

在此基础上，课程首先从资源结构入手，构建“知识图谱 + 能力图谱”联动机制，依托网络空间安全领域虚拟教研室平台，系统梳理课程知识结构与能力要素，形成覆盖知识节点与能力指标的“双图谱”体系。通过知识图谱实现教学内容的结构化表达与学习路径引导，通过能力图谱对学生学习状态与能力发展进行精准刻画，从而实现个性化学习支持与差异化教学干预，提升教学的针对性与有效性。

围绕这一结构，课程进一步优化资源供给方式，融合人工智能与大数据技术，建设模块化、可扩展的数字教学资源库，涵盖微课视频、案例库及算法工具包等多类型资源。通过对教学资源的标准化组织与标签化管理，实现资源的高效检索与按需推送，显著提升学习灵活性与资源利用效率，推动优质教育资源的共享与协同应用。

在实际运行中，上述资源与平台被统一整合进教学过程，覆盖课前预习、课堂互动与课后反馈等各个环节，实现教学过程的全流程数字化与可视化管理。同时，依托学习数据分析技术，对教学行为与学习效果进行持续评估与反馈，动态优化教学策略与资源配置，推动课程向前沿化、智能化与特色化方向发展。

3.5. 构建“家国情怀、社会担当”融入全过程的育人新生态

课程以立德树人为根本任务，系统构建“课程 + 思政”协同推进的育人体系。以《教育部关于印发《高等学校课程思政建设指导纲要》的通知》[2]为指引，进一步挖掘密码分析发展史、典型密码算法的安全性分析技术背后的伦理博弈等内容中的思政元素，同时，将山东大学在密码分析领域的发展历程、标志性科研成果及教师团队的真实科研经历有机融入教材建设与课堂教学之中，把抽象的价值引领转化为可感、可学、可践的教学内容。

在教学实施过程中，从国家安全与战略高度阐释密码学的重要意义，结合《密码法》《网络安全法》等法律法规强化学生的法治意识与安全责任；在知识讲解与案例分析中深入挖掘科研成果背后的科技报国精神，引导学生树立服务国家重大战略需求的使命担当，并设计相应的讨论题目或报告任务，将价值引领内化于知识探究过程中；在项目实践、课程考核与课堂互动中，注重培养严谨求实的科学精神与精益求精的工匠精神。同时，将思政目标系统纳入课程大纲与评价体系，通过翻转课堂讨论、技术答辩与综合性任务，引导学生在解决复杂工程问题的过程中主动思考技术伦理与社会责任，实现知识传授、能力培养与价值塑造的有机统一，全面营造德育与智育深度融合的高质量育人新生态。

4. 线性分析教学实施案例

本章以线性分析技术的教学实施过程为例，围绕教学目标设定、“三元融合”课堂活动组织及过程性评价实施，制定具象化教学改革方案，具体如下：

4.1. 精准设定教学目标

知识目标：掌握线性分析的核心定义，能自主推导线性掩码的传播规则，结合极大似然法自行得出

[2]http://www.moe.gov.cn/srcsite/A08/s7056/202006/t20200603_462437.html

正确密钥的判定依据，明确借助线性分析开展密钥恢复攻击的算法。

能力目标：具备 S 盒线性分布表构造、多轮有效线性逼近式搜索、验证及应用能力，能借助自动化工具完成线性分析相关操作，形成“理论推导－工具实现－结果验证”的完整思维。

素养目标：树立总体国家安全观，培养严谨求实的科研态度、自主探究的学习能力，强化“科技报国”的责任意识。

4.2. 践行“三元融合”模式，组织线性分析课堂教学

以“现代密码分析理念 + 数学模型 + 编程测试”三元融合为核心，分课前、课中、课后三个环节组织教学，实现知识、能力、思政的深度融合。

课前铺垫：依托在线课程平台，发布线性分析预习任务，同步推送我国学者在线性分析领域的原创研究成果，让学生了解我国密码学科发展实力，渗透家国情怀与科技自信。

课中实施：由一轮、二轮、三轮算法层层递进，讲解线性分析的核心原理，再结合具体的简化版本的分组密码，推演具体的线性逼近式，重点讲解线性掩码的传播规则、偏差计算和密钥恢复，融入“严谨治学”的科学精神。围绕“线性掩码的传播规则”“正误密钥的判定条件”等核心问题，组织学生分组讨论，通过雨课堂开展实时互动，鼓励学生主动发言、分享思路，培养逻辑思辨能力；教师结合学生发言，引导学生完善线性分析模型。结合我国线性分析领域的原创成果，讲解科研团队攻坚克难的历程，强化学生“关键技术自主可控”的意识，渗透保密伦理与责任担当。

课后巩固：依托自动化密码分析平台，让学生完成线性近似式的搜索和验证等实操任务，提交实验报告与代码，强化理论与实践的结合。借助线上教学平台，学生反馈学习疑问，形成“预习－授课－实践－反馈”的闭环，教学团队推送线性分析领域前沿论文，引导学生自主拓展视野，培养研究型思维。

4.3. 完善过程性评价，检验教学成效

过程性评价涵盖知识掌握(课堂提问、雨课堂发布练习)、实践能力(自动化平台操作、实验报告、代码编写)、思政素养(责任意识、家国情怀)、协作能力(小组讨论表现)四个核心维度。

依托雨课堂和中国大学慕课等线上教学平台，采集学生学习数据，结合线下课堂观察、小组互评、教师点评，实现“线上 + 线下”“过程 + 能力”的综合评价。建立评价结果反馈机制，结合评价数据，持续优化三元融合教学模式、自动化平台应用及思政融入方式，确保教学质量持续提升。

5. 结语

面对网络空间安全领域攻防技术的快速迭代与前沿交叉学科的日新月异，《密码分析学》课程建设需紧跟国家战略，持续深化“知识图谱 + 能力图谱”双驱动的数智化教学平台应用，进一步拓宽产教融合与科教融汇的边界，依托高水平科研团队，将更多尖端密码科研成果与真实攻防案例转化为优质教学资源，推动“教、学、研、用”的无缝衔接。此外，还需不断完善课程思政的协同育人长效机制，引导学生在探索密码前沿技术中，厚植家国情怀，强化法治意识与职业伦理，以期为构筑国家网络空间安全坚固防线、护航数字中国建设，持续输送具备国际视野、扎实技术与创新精神的卓越密码学拔尖人才。

基金项目

山东省本科教学改革研究项目(密码分析学一流课程建设研究与实践(No.M2023243))；山东大学本科教育教学改革研究项目(密码分析学课程体系优化建设研究(No.2024Z23))；AI 赋能导向的《密码算法分析》课程体系重构与实践(No. SDYJSJGX2025041)。

参考文献

[1] 维护国家密码安全 促进密码事业发展——国家密码管理局负责人就《中华人民共和国密码法》答记者问[N]. 人民日报, 2019-10-28(11). http://politics.people.com.cn/n1/2019/1028/c1001-31422648.html

[2] 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, 11(8): 53-57.

[3] 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).

[4] 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.

[5] 林家全. 基于网络安全技术的攻防一体化教学设计与探究[J]. 现代信息科技, 2023, 7(10): 166-170.

[6] 陶宇斐. 我国本科基础学科拔尖人才培养改革的回眸、反思与建议[J]. 高校教育管理, 2023, 17(3): 88-99.

[7] 吴煌. AI 大模型在高校课程知识图谱构建中的实践探索[J]. 科技理论与实践, 2025, 6(12): 45-48.

[8] 赵建庆, 宋振世. 课程思政与信息素养教育隐性融合路径的研究与实践——以华东师范大学图书馆信息素养教育为例[J]. 图书馆杂志, 2023, 42(3): 107-113.