基于大模型的密码学课程改革探索*

韩萌

北方民族大学计算机科学与工程学院，银川 750021

摘　要　随着网络安全行业对专业人才需求的不断增长，密码学作为相关专业的核心课程，其教学质量的提升至关重要。针对应用型本科院校密码学课程面临的困境，如知识更新滞后、理论与实践脱节、学生参与度不高等问题，探讨了大模型技术在密码学教学中的融合创新思路。通过补充课程内容、增强课堂互动、个性化推荐复习资料，创新实验教学等方面的改革，构建智能化教学闭环。目的是提高学生的知识掌握程度和工程实践能力，为密码学教学改革提供新的思路和方法。经过多轮课程验证，课程内容的设计过程使用大模型能够提高学生上课的积极性从而得到更好的学习效果。

关键字　密码学，大模型，教学创新

Teaching Innovation of Cryptography Course Based on Large Models

Han Meng

School of Computer Science and Engineering,
North Minzu University,
Yinchuan 750021

Abstract—With the continuous growth of the demand for professional talents in the network security industry, as a core course for related majors, improving the teaching quality of cryptography is of great significance. Aiming at the dilemmas faced by the cryptography course in application-oriented undergraduate universities, such as the lagging update of knowledge, the disconnection between theory and practice, and the low student participation, this paper explores the innovative ideas of integrating large model technology into cryptography teaching. Through reforms in aspects such as supplementing the course content, enhancing classroom interaction, providing personalized recommendation of review materials, and innovating experimental teaching, an intelligent teaching closed loop is constructed. The purpose is to improve students' mastery of knowledge and engineering practice ability, and provide new ideas and methods for the teaching reform of cryptography.After multiple rounds of course validation, it has been found that incorporating large language models into the design process of course content can enhance students' enthusiasm in class, thereby leading to better learning outcomes.

Keywords—Cryptography, Large Model, Teaching Innovation

1　引　言

以大语言模型为代表的生成式人工智能正在迅速改变大学教学关于“人”及其教育的生产方式，在全球高等教育领域塑造出一种全新的人才培养模式[1]。基于大模型的智能体已经逐步具备了多模态感知、检索增强生成、推理与规划、交互与进化等能力[2]。已有研究表明，大模型在语言课[3]、生态课[4]、计算机实践课[5]等学展现出了很强的能力，在辅助外语教学与研究方面更有不俗的表现。

数字化时代，网络安全已成为国家和社会稳定发展的重要保障。密码学作为网络安全领域的核心支撑技术，其重要性不言而喻。对于应用型本科院校的网络安全专业而言，培养具备扎实密码学知识和实践能力的专业人才是教学的重要目标。然而，传统的密码学教学模式在当前快速发展的技术环境下，逐渐暴露出诸多弊端，难以满足行业对人才的需求。为此，研究者提出将人工智能作为一项前沿热门的科学技术应用到当前高校的网络安全相关课程中[6]。

密码学为信息的保密性、完整性、可用性以及身份认证等提供了关键的技术保障。学生通过学习密码学，不仅要掌握各类密码算法的数学原理，还要理解密码协议的设计思想。此外，能够将这些理论知识应用于实际的工程实践，如开发加密软件、设计安全的通信系统等。传统密码学教学面临不足在于：

（1）知识更新滞后于技术发展。在当前科技飞速发展的背景下，新的密码技术不断涌现。抗量子密码旨在抵御量子计算机对传统密码算法的潜在威胁，同态加密则允许在密文上进行特定的计算而无需解密，

*基金资助：北方民族大学校级混合式教学示范课程建设项目（bmdhsk202215），宁夏回族自治区普通本科高校本科教育教学改革研究与实践项目（bjg2021064）

**通讯作者：韩萌 compute2006_2@126.com 。

这些前沿技术在实际应用中逐渐崭露头角。然而，现行的密码学教学内容往往局限于经典的密码算法和协议，对这些新兴技术的介绍较少，导致学生所学知识与行业实际需求存在差距。

（2）理论教学与实验验证脱节。在传统的密码学教学中，教师通常侧重于理论知识的讲解，学生虽然能够理解各种密码算法的原理，但在将其转化为实际代码实现时，却面临诸多困难。例如，学生在课堂上学习了 RSA 密码体制的密钥生成、加密、解密的数学原理。但在实际编写代码实现 RSA 时，需要考虑诸如密钥生成、数据格式处理、安全性增强等诸多实际问题，这与课堂上单纯的理论讲解存在较大差异。由于缺乏足够的实践指导和项目经验，学生往往难以将所学的理论知识应用到实际的编程实践中，导致理论与实践脱节。

（3）学生参与度降低。密码学课程涉及大量数学推导，对于数学基础较好、逻辑思维能力较强的学生来说，他们能够较好地理解和掌握课程内容，积极参与课堂讨论和学习。然而，对于部分数学基础薄弱的学生而言，这些抽象的数学知识成为了学习的障碍，易使他们课程失去兴趣，进而导致学生参与度两极分化严重。这种情况不利于整体教学质量的提升，也难以实现全员培养网络安全专业人才的目标。

应用型本科院校的学生具有较强的实践动手能力和应用意识，他们对实际项目的参与热情较高。与研究型大学的学生相比，他们在理论基础和抽象思维能力方面相对薄弱。在密码学课程学习中，过于抽象的理论知识和复杂的数学推导容易让他们感到困惑和吃力。因此，需要一种教学模式能够降低学习门槛，从学生易于理解和接受的实践入手，逐步引导学生深入理解理论知识。

为此，本文研究构建大模型参与的教学设计。第一阶段，使用大模型提高课程的备课效率，并与时俱进的补充与课程内容相关的前沿知识。大模型提高课程准备效率与课程内容前沿性。第二阶段，大模型提高课程学习效果与实践能力。通过简单、直观的实践项目，让学生对密码学的应用有初步的认识和体验，激发学生的学习兴趣。并且在实践过程中逐步引入相关的理论知识，帮助学生理解实践背后的原理，实现理论与实践的有机结合。大模型技术为实现这一教学方法提供了技术支持，通过生成丰富的实践案例、提供个性化的学习指导等方式，帮助学生顺利地从实践过渡到理论学习提高教学效果。

2 大模型在密码学教学中的融合创新思路

2.1 大模型提高课程准备效率与课程内容前沿性

大模型具备较强的知识整合能力，能够实时爬取密码学相关专业资源，如 OWASP 漏洞库等。通过对这些资源的深入分析和处理，大模型可以自动生成包含时序关系的密码技术演化图谱。通过可视化对比，帮助学生更好地理解密码技术的发展脉络和演进原因。同时，大模型还能根据教师的需求，整合最新密码算法和相关竞赛的实战案例，为教师备课提供前沿的知识素材，使教学内容紧跟行业发展。

（1）通过大模型构建知识图谱，提高学生对整个关联知识理解能力。

利用大模型的网络爬虫和数据分析能力，可以获取最新的密码学研究成果、相关的漏洞案例等多源信息，大模型自动生成密码技术演化图谱。该图谱不仅展示了不同密码技术的发展历程，如从早期的古典密码到现代的对称加密、非对称加密技术的演变，还包含了各技术之间的时序关系和技术关联。例如，在展示从 DES 到 AES 的发展过程中，图谱可以详细呈现 AES 在克服 DES 密钥长度短、安全性低等问题上所做的改进，以及这些改进背后的技术原理。通过可视化的图谱展示，学生能够更加直观地理解密码技术的发展脉络，教师也可以根据图谱更新教学内容，确保教学的时效性和前沿性。本文使用 Deepseek 生成的知识图谱如图 1 所示。

（2）通过大模型可以智能生成教案，提高备课效率，且能快速补充前沿知识。

教师只需输入具体的教学目标，如“讲解 SHA-3 海绵结构”，大模型即可自动生成全面的教案内容。并且可以设置分层教学案例，如针对基础层和进阶层学生，设计难易不同的内容。基础层的学生，大模型提供简单易懂的海绵结构示意图，清晰地展示其基本组成部分和工作流程。对于进阶层的学生，则给出与 SHA-2 的性能对比实验，包括实验环境搭建、数据采集与分析方法等，帮助学生深入理解 SHA-3 海绵结构的优势和特点。使用 Deepseek 生成的生成的 SHA-3 与 SHA-2 的性能对比如表 1 所示。通过比较密码设计基础，安全性，软硬件实现速度，输出长度和应用领域等方面给出了详细不同之处。

同时，大模型还能根据过往教学经验和学生常见问题，预警常见误区，如学生在学习过程中容易混淆的消息填充与比特位排序规则。此外，大模型会提示跨课程关联内容，如结合计算机网络中的 MAC 地址欺骗案例，帮助学生将密码学知识与其他相关课程知识建立联系，形成完整的知识体系。

图 1　DES-AES 发展知识图谱

表 1　SHA-3 与 SHA-2 的性能对比

性能指标	SHA-2	SHA-3
算法版本	SHA-224，SHA-256，SHA-384，SHA-512，SHA-512/224，SHA-512/256	SHA3-224，SHA3-256，SHA3-384，SHA3-512
设计基础	复杂的数学结构和计算难度	海绵函数结构，包括 θ (theta)、ρ (rho)、π (pi)、χ (chi)、ι (iota)五个步骤
安全性	较高，但 SHA-1 因安全问题被逐渐替代	提供更高的安全性和效率
软件实现速度	通常较快	在某些情况下可能稍慢于 SHA-2
硬件实现速度	–	通常能提供更好的性能
输出长度	多种选择，满足不同需求	支持任意长度的哈希输出，但常用固定长度为 224、256、384 和 512 位
应用领域	数据完整性校验、数字签名、安全协议等	数字签名、数据完整性验证、密码哈希等

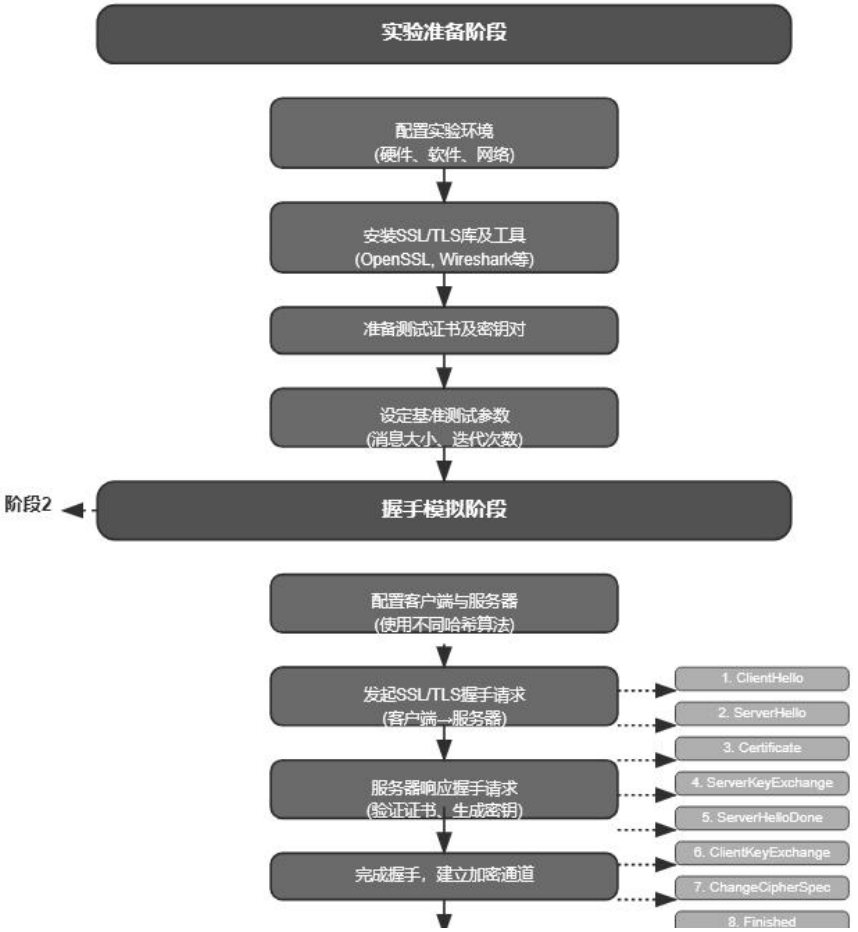


图2 SSL/TLS协议的握手过程的实验准备阶段和握手模拟阶段示意图

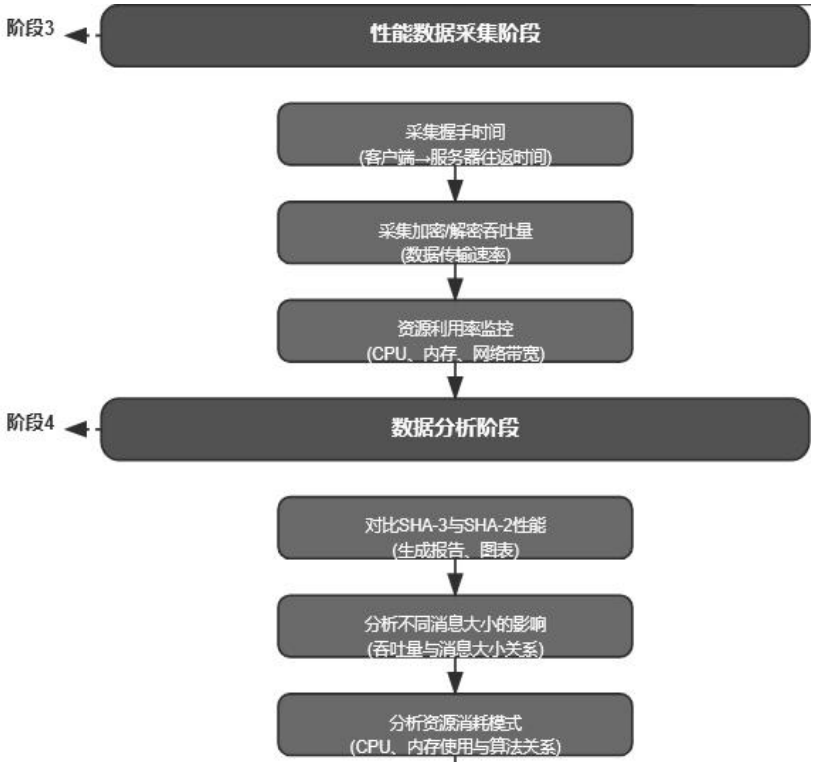


图 3 SSL/TLS 协议的握手过程的数据采集阶段和数据分析阶段示意图

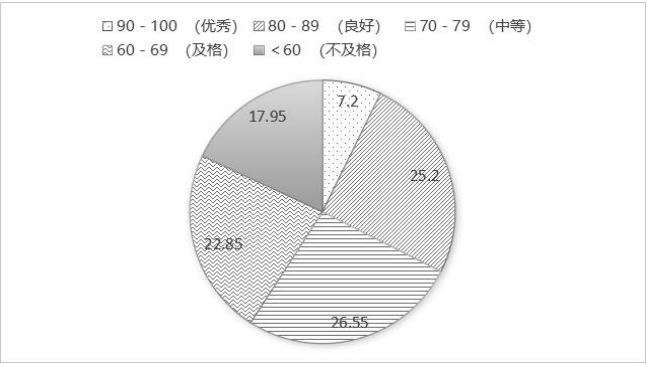
2.2 大模型提高课程学习效果与实践能力

（1）提高课堂学习效果

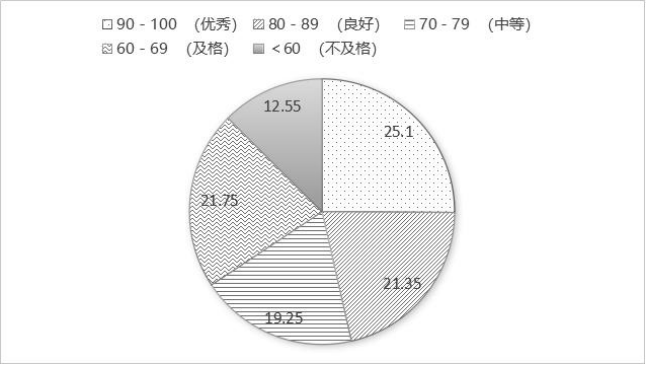
在密码学教学中，交互式场景的构建对于学生理解复杂的密码协议和攻击防御机制至关重要。大模型可以支持密码协议仿真，例如学生可以在大模型生成的虚拟环境中模拟 SSL/TLS 协议的握手过程，观察不同参数设置下协议的运行情况，深入理解协议的工作原理。使用 Deepseek+豆包设计的实验流程如图 2 和图 3 所示，给出了“实验准备阶段-握手模拟阶段-数据采集阶段-数据分析阶段”详细设计过程。此外，大模型还能构建攻击防御沙盒，学生可以在其中扮演攻击者或防御者的角色。攻击者尝试利用大模型生成的各种密文漏洞进行破解，防御者则需要运用所学知识设计混合加密方案来抵御攻击。这种交互式的学习场景能够极大地提高学生的学习兴趣和参与度，使学生在实践中更好地掌握密码学知识。

图 4 实施问答过程示意图

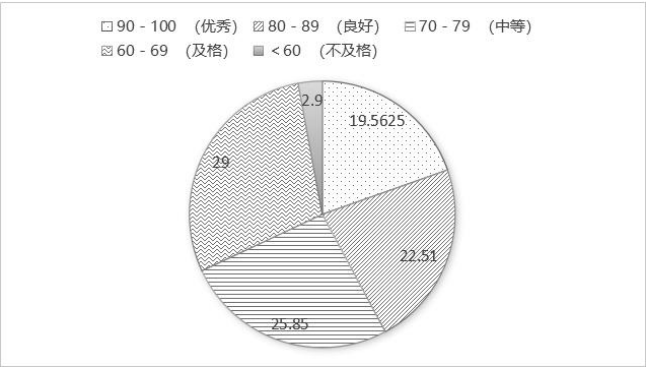
大模型还能实现情境化教学助手功能。如实时问答引擎是大模型在课堂教学中的重要应用之一。当学生在课堂上提出“为什么 RSA 加密不直接用于长明文？”这样的问题时，大模型能够迅速响应，给出详细解释。



2023 年整体成绩分布情况（%）



2024 年整体成绩分布情况（%）



2025 年成绩分布情况（%）

图 5　三年成绩分布情况

学生可以直观地看到长明文在使用 RSA 加密时存在的问题以及如何解决这些问题，从而加深对知识的理解。整个过程分为 5 步，如图 4 所示。此外，大模型还能创建博弈式学习场景。教师可以将学生分成小组，分别扮演攻击方和防御方。攻击方需要利用大模型生成的密文漏洞尝试破解密码，防御方则要根据所学知识设计混合加密方案来抵御攻击。在这个过程中，学生不仅能够巩固所学的密码学知识，还能提高团队协作能力和解决实际问题的能力，极大地增强了学习兴趣和参与度。

（2）大模型实现实践教学创新

大模型实践教学创新，设计项目式学习案例，提高学生实践能力。例如，大模型设计全同态加密实训，基于 CSDN 案例中全同态加密（FHE）的云平台部署经验设计隐私计算工作坊。学生在工作坊中使用微软 SEAL 库完成加密数据查询任务，在此过程中，大模型实时评估学生对密文操作的计算开销，并与 Paillier 半同态方案的性能进行对比。通过这种实践，学生能够深入理解全同态加密的优势与实际应用中的挑战，切实提升在隐私计算领域的实践能力。

（3）教学成果比较

为了评价基于大模型的教学效果，将 2025 年成绩与未使用大模型的 2023 年和开始使用大模型的 2024 年相同专业的密码学成绩进行简单对比。图 5 显示了 3 年考试卷面成绩整体分布对比，显示优秀、良好、中等、及格和不及格的占比情况。

通过三年的成绩对比可以明显分析出，在保持试卷的考核内容、难度等差异度不大的前提下，通过借助大模型等 AI 工具，能够不断提高学生课上课下学习的主动性，明显提高了学生的及格占比。对于表现优秀的学生，整体分布也有明显的提升。整体增加了学生的学习积极性，得到了较好的教学效果。

3　结束语

大模型在全球掀起了新一轮人工智能产业的发展浪潮，势必推动计算机教育的改革和创新，同时使计算机教育面临一系列新的挑战[7]。通过将大模型技术融入密码学课程教学，构建了理论 - 实践 - 评估的全流程智能化教学闭环。在理论教学方面，利用大模型实现了课程内容的动态更新和智能教案生成，提高了教学内容的时效性和针对性。在实践教学环节，通过虚实融合实验平台和项目式学习案例，增强了学生的实践能力和创新能力。在评估方面，大模型支持的精准化复习体系能够根据学生的学习情况提供个性化的复习建议，有效提高了学生的学习效果。

尽管大模型在密码学教学中取得了显著成效，但仍存在一些问题和挑战需要进一步研究解决。例如，大模型生成的内容可能存在准确性和可靠性问题，需要进一步优化和验证；在教学过程中，如何更好地引导学生正确使用大模型，避免过度依赖，培养学生的独立思考能力和创新精神，也是未来研究的重要方向。此外，随着技术的不断发展，如何将最新的密码学研究成果和大模型技术应用到教学中，持续完善教学体

系，提高教学质量，也是教学过程中需要持续关注和探索的问题。

参 考 文 献

[1] 蒋贵友, 殷文轩. 变革抑或危机：大语言模型赋能大学教学及其限度——基于斯坦福大学的案例考察[J]. 电化教育研究, 2025, 46(01): 122-128.

[2] 卢宇, 余京蕾, 陈鹏鹤. 基于大模型的教学智能体构建与应用研究[J]. 中国电化教育, 2024, (07): 99-108.

[3] 冯庆华, 张开翼. 人工智能辅助外语教学与研究的能力探析——以 ChatGPT4.0 和文心大模型 4.0 为例[J]. 外语电化教学, 2024, (03):3-12+109.

[4] 张智顺. 引入认知大模型的“生态环境的保护”高三复习课教学[J]. 生物学教学, 2025, 50(02): 51-53.

[5] 李清勇, 耿阳李敖, 彭文娟, 等. “私教”还是“枪手”：基于大模型的计算机实践教学探索[J]. 实验技术与管理, 2024, 41(05): 1-8.

[6] 高秋燕. 人工智能技术在高校网络安全防御中的应用[J]. 网络安全技术与应用, 2025, (05): 75-77.

[7] 徐悦, 黄子文, 宋雨轩, 皮德常. 从 AI 大模型看高校计算机教育面临的机遇与挑战[J]. 计算机技术与教育学报, 2024, 12(03): 99-06.