# AI 赋能《现代密码学》课程的数据驱动教学改革探索

刘冰[1] 范翠玲[2] 刘克剑[1] 牛宪华[1*]

（1.西华大学 计算机与软件工程学院，四川省成都市 邮编 610039；
2.西南交通大学 数学学院，四川省成都市 邮编 611756）

**摘 要** 针对《现代密码学》课程理论抽象、实验碎片化、学习反馈滞后及竞赛训练衔接不足等问题，面向 AI 时代密码人才培养需求，提出“AI 模型辅助认知—竞赛项目牵引实践—数据闭环评价改进”的课程改革框架。通过重构课程目标与教学内容，将 AI 辅助学习、密码算法实现、CTF 改编任务、合规案例和过程性评价融入教学全过程，并利用学生在线学习行为数据构建 BiLSTM 成绩三分类预测模型，为学情诊断和教学干预提供依据。测试结果表明，在 3115 个样本上，模型分类准确率和加权 F1 值均为 0.62，对 Fail 类学生的召回率达到 0.78，能够有效识别学习困难学生。研究表明，该模式能够将课程目标、实践任务与学习数据衔接，为教师实施针对性教学干预、持续改进课程设计及提升学生密码算法理解、工程实践、安全分析和合规意识提供支持。

**关键词** AI 模型，现代密码学，竞赛融合，数据驱动，OBE

# AI-Empowered Data-driven Teaching Reform of Modern Cryptography Course

Bing Liu[1], Cuiling Fan[2], Kejian Liu[1], Xianhua Niu[1*]

(1.School of Computer and Software Engineering, Xihua University, Chengdu 610039, China;
2. School of Mathematics, Southwest Jiaotong University, Chengdu 611756, China)
niuxh@mail.xhu.edu.cn

**Abstract—To address the problems of abstract theory, fragmented experiments, delayed learning feedback, and insufficient linkage with competition training in the Modern Cryptography course, this paper proposes a reform framework integrating AI-assisted cognition, competition-driven practice, and data-based closed-loop evaluation and improvement. By reconstructing course objectives and content, AI-assisted learning, cryptographic algorithm implementation, adapted CTF tasks, compliance cases, and process-based assessment are incorporated throughout the teaching process. Student online learning behavior data are further used to build a BiLSTM-based three-class performance prediction model to support learning diagnosis and instructional intervention. Test results show that, on 3,115 samples, the model achieves an accuracy of 0.62 and a weighted F1-score of 0.62, while the recall for the Fail class reaches 0.78, enabling effective identification of students with learning difficulties. The proposed approach links course objectives, practical tasks, and learning data, providing a data-driven basis and an implementation path for targeted intervention, continuous course improvement, and the cultivation of students' competencies in cryptographic understanding, engineering implementation, security analysis, and compliance responsibility.**

**Keywords—AI models, Modern Cryptography, competition integration, data-driven teaching, OBE**

## 1 引 言

随着信息技术的快速发展，信息安全引发人们的高度重视。密码技术是保障数据安全、网络安全和国家安全的重要基础。随着云计算、大数据、人工智能和量子计算等技术发展，密码算法的设计、实现、测评和迁移正在从单一理论问题转向涉及系统工程、法律合规和产业应用的综合问题。系统化建设信息安全专业学科以及大力发展密码技术的革新是促进信息安全技术发展的核心方案，是保障国家网络安全的重要手段。当前，我国正处于“十五五”规划开局和实施关键期。《中共中央关于制定国民经济和社会发展第十五个五年规划的建议》明确提出“加快建设网络强国”“加强网络、数据、人工智能等新兴领域国家安全能力建设”，为密码事业发展提供了战略指引。规划强调推进“教育科技人才一体化发展”，面向集成电路、人工智

*基金资助：本文得到西华大学 AI 赋能本科教育教学改革专项（xjjg2026014）；四川省高等教育人才培养质量和教学改革项目(JG2024-0772); 第二批高等学校课程思政标杆院系和典型案例(川教函〔2025〕87 号)-《现代密码学》课程思政典型案例;西华大学教学教学改革项目(Xjjg2023012)支持。

*通讯作者：牛宪华 niuxh@mail.xhu.edu.cn。

能等战略急需领域加快创新型人才培养；同时提出全链条推进关键核心技术攻关，在抗量子密码、轻量级密码协议、人工智能与密码融合等前沿方向实现突破，筑牢数字安全“根技术”基石。此外，“十五五”规划起步之年，国家密码管理部门明确要求“统筹密码发展和安全，护航‘十五五’新征程”，将密码应用安全性评估、商用密码合规体系建设和产教协同育人作为重点方向，为高校密码课程改革注入了新的时代内涵与工程导向[1-2]。《中华人民共和国密码法》以及《商用密码应用安全性评估管理办法》为高校密码课程建设提出了更明确的规范意识和工程导向要求[3-4]。

《现代密码学》课程通常开设于网络空间安全、信息安全、计算机科学与技术等专业，是学生理解信息安全机制的重要专业基础课。该课程兼具数学抽象性、算法工程性和应用安全性，既要求学生掌握分组密码、公钥密码、哈希函数、数字签名、密钥管理等理论，又要求学生能够把算法原理落实为可验证的程序、协议或系统模块[5]。已有研究指出，《现代密码学》课程改革需要围绕教学目标、教学内容、教学方式和评价机制展开，并将“以学生为中心、多元融合、以赛促学”的混合式改革方案引入课程实践[6]。

由此可见，《现代密码学》课程改革需要从单一知识讲授转向“目标设置—任务驱动—证据闭环—技术改进”一体化设计：以课程目标统领知识组织，以项目任务连接理论与实践，以过程数据支持教学干预，以合规责任引导价值形成。鉴于此，本文结合双向长短期记忆模型（Bidirectional Long Shot Term，BiLSTM），基于数据驱动探索 AI 赋能《现代密码学》课程改革的可行路径。

## 2 《现代密码学》课程教学面临的问题

《现代密码学》课程的教学难点并不只来自算法本身，更来自“知识—实践—评价”之间的脱节。与一般程序设计课程相比，密码课程对数学基础、形式化推理、代码实现和安全思维都有较高要求，若仍采用以教师讲授和期末考试为主的方式，容易形成“听懂概念、不会实现；会写代码、不会分析安全性；能完成实验、不能迁移到竞赛和工程”的问题。

### 2．1 理论抽象与学习路径碎片化

《现代密码学》涉及数论、代数、概率论、复杂性理论等基础知识。学生在学习 RSA、椭圆曲线密码、哈希函数安全性和数字签名时，常常把课程内容理解为分散公式和算法步骤，难以建立从安全目标到密码原语、从密码原语到协议应用的整体知识结构。生成式 AI 模型虽然能够快速解释概念、生成示例代码，但若缺乏教师设计的任务边界和验证机制，也可能造成“看似理解、实则依赖”的浅层学习。

### 2．2 实验实践与竞赛训练衔接不足

当前不少课程实验仍停留在古典密码、AES、RSA、哈希函数等算法的单点实现层面，学生完成实验报告后，对算法为何安全、如何攻击、怎样在真实协议中使用缺乏进一步训练。另一方面，密码竞赛、CTF、网络安全竞赛通常强调综合问题求解，涉及编码、协议分析、脚本编写、漏洞利用和安全合规等能力，若课程上机实验没有逐步过渡到竞赛式任务，学生很难在短时间内形成迁移能力。

### 2．3 评价反馈滞后与教学干预不足

传统考核以平时作业、实验报告和期末考试为主，评价多集中于学习结束之后，难以及时发现学生在哪个知识单元、哪类算法、哪种实践任务中出现困难。上传次数、视频观看时长、作业得分等平台数据虽然易于获得，但如果缺少与课程目标对应的指标解释，数据就难以转化为有效教学干预。学习成效导向的改革强调以可视、可管、可控的过程数据支撑教师调整教学方案，这为《现代密码学》课程评价提供了重要启示[8]。

### 2.4 合规意识与职业责任培养不足

密码技术兼具防护性和攻击性。学生能够编写加密程序、破解弱口令或分析协议缺陷，并不意味着已经形成正确的安全边界意识。课程若只讲技术，不讲法律、伦理和应用规范，易把密码学习窄化为“解题技巧”。在密码应用安全性评估、商用密码合规和关键信息基础设施保护成为行业重要任务的背景下，将法律法规、标准规范和工程责任融入教学全过程，是《现代密码学》课程改革的重要内容[3-4]。

## 3 改革思路与课程目标重构

本文借鉴 OBE 理念中“培养目标—毕业要求—课程目标”的支撑逻辑，把课程产出从知识掌握扩展到算法实现、攻击分析、合规表达和竞赛迁移。已有研究表明，课程内容分析不应只停留在课程名称或知识标签上，还应关注课程所指向的认知、情感和技能产出[7]。因此，本文将《现代密码学》课程产出划分为 3 个层次：认知层面理解密码机制，技能层面完成算法和协议实践，价值层面形成密码应用合规意识与职业责任。

### 3．1 “AI 辅助—竞赛牵引—数据改进”的改革理念

改革的基本思路是：以 AI 模型为认知助手，解决课程抽象、概念密集和学习差异大的问题；以竞赛项目为实践牵引，把算法实现、攻击分析、协议应用和团队协作融入课程任务；以学习数据为持续改进依据，形成课前预诊断、课中干预、课后反馈和阶段复盘的

闭环。AI 模型的角色不是替代教师或学生，而是成为教师组织学习资源、学生进行概念澄清、实验调试和反思表达的工具。竞赛任务的角色不是单纯追求获奖，而是把真实问题的复杂性引入课程学习过程。

围绕《现代密码学》课程的基础性和应用性，可设置 4 类课程目标，分别支撑密码算法理解能力、工程实现能力、安全分析能力和职业规范能力，具体见表 1。

## 3．2　课程目标与能力支撑关系

表 1　课程目标与能力支撑关系

| 课程目标 | 支撑能力 | 教学证据 |
| --- | --- | --- |
| 目标1：理解密码学基本概念、典型算法与安全目标 | 算法原理理解、形式化表达 | 随堂测验、概念图、算法推导记录 |
| 目标2：实现并测试典型密码算法和协议模块 | 程序实现、实验验证、错误排查 | 代码仓库、实验报告、单元测试结果 |
| 目标3：分析弱实现、弱协议和典型攻击场景 | 安全分析、问题建模、竞赛迁移 | CTF任务复盘、攻防报告、团队展示 |
| 目标4：理解密码应用合规要求与职业责任 | 合规意识、伦理判断、工程表达 | 案例讨论记录、评估清单、反思报告 |

## 3．3　教学内容的模块化重构

课程内容按“基础理论—算法实现—协议应用—竞赛拓展—合规评价”进行模块化重构（如图 1 所示），既保留《现代密码学》的核心理论，又增加 AI 辅助学习、国密算法应用、后量子密码前沿、密码应用安全性评估等内容。后量子密码标准化进程也说明，密码课程不能只停留在经典算法讲授，而应适度引入面向未来安全需求的知识更新[10]。

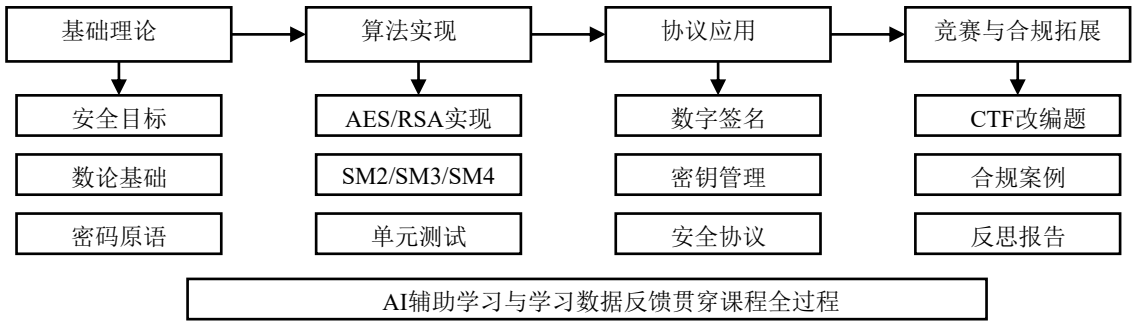



图 1　《现代密码学》课程内容模块化结构

# 4　“AI+竞赛+数据”闭环教学模式

在教学组织上，如图 2 所示，本课程构建“课前 AI 导学—课中问题讲解—课后实验实践—竞赛任务提升—数据反馈改进”的教学模式。该模式吸收混合式闭环教学强调的“学生为中心的学与做、教师主导的教、复杂工程能力培养”的思路[8]，并将其迁移到《现代密码学》课程改革中。

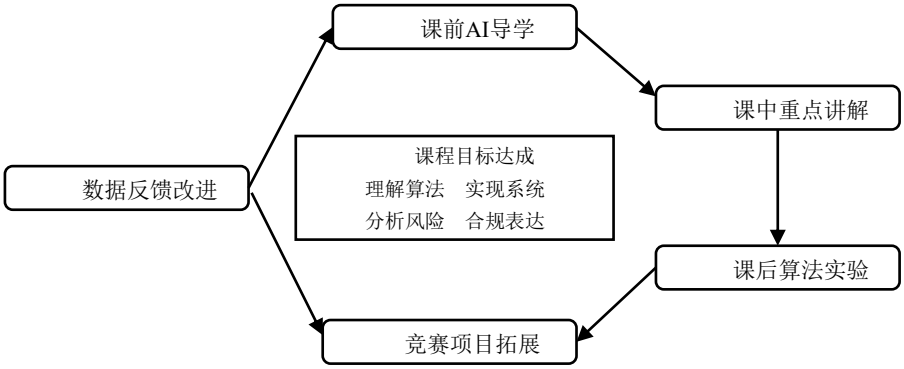



图 2　AI 模型赋能竞赛融合闭环教学模式

### 4．1 AI 模型辅助认知：从概念解释到错误诊断

课前，教师围绕每个知识单元提供 AI 使用提示词、阅读材料和预习问题，引导学生使用 AI 模型进行概念澄清，但要求学生提交“AI 回答—个人修正—证据来源”三段式学习记录。课中，教师选择学生记录中高频出现的误解开展讲解，如“混淆扩散与安全性之间的关系”“把哈希函数误解为加密算法”等。课后，学生可使用 AI 模型辅助调试代码，但必须保留关键错误、修正过程和测试截图，防止只提交可运行结果而不理解过程。

### 4．2 竞赛项目牵引实践：从单点实验到综合任务

课程实验不再只按算法目录布置，而是围绕“可验证、可攻击、可解释”的项目任务展开。例如，在对称密码单元中，学生先实现分组密码的基本加解密，再分析不同运行模式下的错误扩散和重放风险；在公钥密码单元中，学生不仅实现 RSA 的快速模幂和签名验证，还要分析弱随机数、短密钥和不规范填充带来的安全问题；在数字签名和认证协议单元中，学生需完成协议时序图和攻击路径复盘。竞赛题目用于拓展而非替代基础教学，难度从课堂案例、改编题、开放题逐步提升。

### 4．3 数据驱动教学干预：从结果统计到过程画像

课程建立学习数据采集与分析机制，主要采集预习测验、课堂互动、实验提交、单元测试、竞赛任务、同伴互评和反思报告等过程性数据。教师不直接以平台活跃度评价学习效果，而是把数据映射到课程目标，形成知识掌握、实验实现、攻击分析、合规表达 4 类学习画像。对于预习测验错误率高的知识点，教师在课中增加对比示例；对于实验提交多次失败的任务，教师发布针对性调试清单；对于竞赛复盘表达薄弱的小组，教师安排二次答辩和报告修订。

### 4．4 合规与课程思政融入：从技术应用到责任表达

在密码课程中开展价值引导，不宜简单增加口号式内容，而应将法律、标准和行业案例嵌入具体技术任务。例如，在商用密码算法教学中讨论国产密码算法的应用背景，在密钥管理单元讨论密钥全生命周期责任，在协议分析单元讨论漏洞披露边界和竞赛伦理。学生在完成攻击分析报告时，必须同时提交“风险说明、合规边界、修复建议”3 项内容，使其理解密码技术既是工程工具，也是安全责任。

## 5 课程实施设计与质量保障

### 5．1 分阶段教学实施

课程可按照 16 周安排 4 个阶段实施。第一阶段为基础导入，重点建立密码安全目标、攻击模型和 AI 使用规范；第二阶段为算法实现，围绕对称密码、公钥密码、哈希函数和数字签名开展实验；第三阶段为协议与竞赛任务，选择 2—3 个改编 CTF 题或行业案例进行小组项目；第四阶段为总结评价，学生提交学习档案袋，教师依据过程数据和作品质量进行课程目标达成分析。

### 5．2 教学资源与平台建设

课程资源包括 3 类：一是知识资源，如微视频、讲义、概念图、算法伪代码和法规标准材料；二是实践资源，如代码模板、单元测试脚本、在线判题环境和密码工具库；三是生成资源，如学生代码仓库、攻防复盘报告、AI 辅助学习记录和优秀作品案例。教师定期筛选学生生成资源，形成可复用案例库，服务后续教学。与职业师范院校计科专业教学改革中“课程群夯实基础—行业认证对标能力—产教协同深化实践”的思路类似，《现代密码学》课程也需要在校内课程、行业规范和竞赛实践之间建立相互支撑关系[9]。

### 5．3 学习成效评价与持续改进

评价采用“形成性评价+终结性评价+增值性评价”组合方式。形成性评价关注预习、课堂参与、实验提交和 AI 学习记录；终结性评价关注期末考试、课程项目和小组答辩；增值性评价关注学生从初始测验到后续竞赛任务中的能力变化。如图 3 所示，多维度评价综合评价学生学习能力与学习情况，避免单一的考核式评价不能完全达到课程目标。

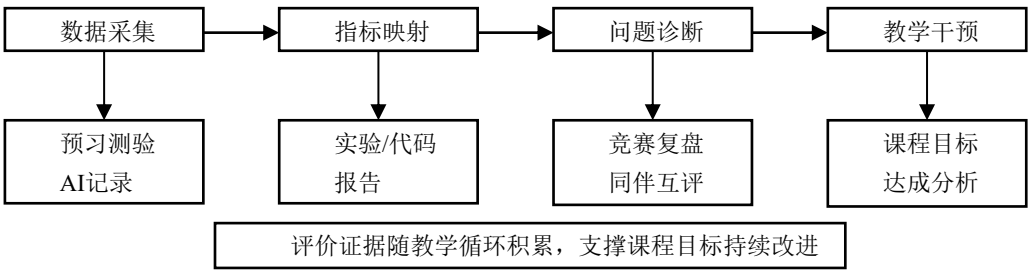



图 3 数据驱动的学习成效评价闭环

## 5．4 基于 BiLSTM 模型的数据驱动教学改革

本文利用学生在线学习行为数据构建深度学习模型，如图 4 所示，基于 BiLSTM 模型[11]预测学生最终成绩，教学期间介入学情，提升学生学习效率并持续改进。

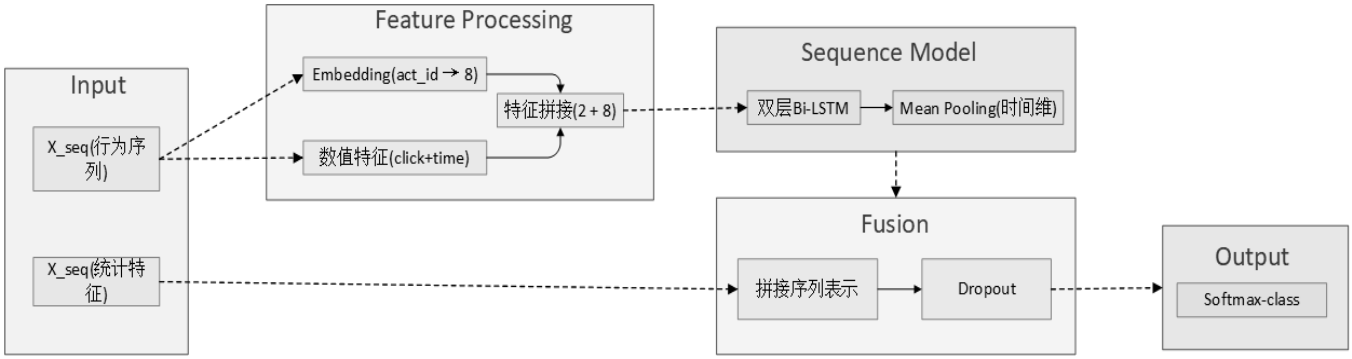



图 4 Bi-LSTM 模型结构图

本模型旨在通过融合序列行为数据与统计特征，对学生的最终成绩进行三分类预测。将学生在学习平台上的行为序列（如点击次数、时间间隔及活动类型）进行建模，其中类别特征通过嵌入层转化为低维稠密表示，并与数值特征进行拼接。随后，利用 BiLSTM 网络捕捉行为序列中的时序依赖关系，从而学习学生行为随时间变化的动态模式。

在序列特征提取后，采用平均池化对时间维度进行聚合，得到全局行为表示。同时，引入手工构造的统计特征（如总点击量、平均点击量等）作为补充信息，与序列表示进行融合。最后通过全连接网络进行特征映射，并输出三分类结果。

具体算法流程如下：

Step 1: 数据预处理

读取原始数据并进行表连接，保留学生行为记录及对应标签，对标签进行数值映射（Fail=0, Pass=1, Distinction=2），并清理无效数据。

Step 2: 特征编码

对行为类型进行离散编码，将其转换为整数索引，以便后续嵌入层处理。

Step 3: 序列构建

按学生分组，将每个学生的行为数据按时间排序，构建固定长度的行为序列。对于不足长度的序列进行零填充，超出长度的进行截断。

Step 4: 特征工程

提取序列中的数值特征以及类别特征，同时构造统计特征。

Step 5: 特征标准化

对数值特征进行标准化处理，使其具有相似的尺度，提高模型训练稳定性。

Step 6: 模型输入构建

将序列特征输入 Embedding 层并与数值特征拼接形成统一的序列表示，将统计特征作为辅助输入。

Step 7: 序列建模

通过双向 LSTM 网络对序列进行建模，提取时序依赖关系，并通过平均池化获取全局序列表示。

Step 8: 特征融合

将 LSTM 输出的序列表示与统计特征进行拼接，形成最终特征向量。

Step 9: 分类预测

通过全连接网络进行映射，输出三分类结果（Fail / Pass / Distinction）。

Step 10: 模型训练与优化

采用带类别权重的交叉熵损失函数，以缓解类别不平衡问题，并使用 Adam 优化器进行训练，同时通过验证集进行早停策略以防止过拟合。

Step 11: 模型评估

在测试集上进行预测，计算准确率、精确率、召回率和 F1-score 等指标，对模型性能进行评估。

最终评估结果如表 2 所示：

表 2 BiLSTM 模型评估结果

| 类别 | Precision | Recall | F1-score | Support |
|---|---|---|---|---|
| 0（Fail） | 0.62 | 0.78 | 0.69 | 950 |
| 1（Pass） | 0.71 | 0.62 | 0.66 | 1747 |
| 2（Distinction） | 0.30 | 0.28 | 0.29 | 418 |
| Accuracy | - | - | 0.62 | 3115 |
| Macro avg | 0.54 | 0.56 | 0.55 | 3115 |
| Weighted avg | 0.63 | 0.62 | 0.62 | 3115 |

基于 BiLSTM 的预测模型有效识别低分学生，《现代密码学》课程组便可以在了解学情进展时介入学生学习活动，对于需要帮助的学生重点帮扶，提升学生学习兴趣并提高学习效果。

## 6 结 语

《现代密码学》课程改革的核心，不是简单把 AI 工具、竞赛题目和数据平台叠加到原有课堂中，而是围绕学生能够形成何种能力重新设计课程目标、学习任务和评价证据。本文面向 AI 时代密码人才培养需求，提出“AI 模型辅助认知—竞赛项目牵引实践—数据闭环评价改进”的课程改革框架，并从课程目标、内容模块、教学流程和质量保障等方面给出实施路径。该框架的特点在于：一是把 AI 模型定位为可验证的学习助手，强调学生的个人修正和证据意识；二是把竞赛任务嵌入课程实践过程，促进学生从算法实现走向攻击分析和综合应用；三是把学习数据与课程目标对应起来，基于 BiLSTM 深度强化学习模型预测学生行为，推动教师根据证据进行持续改进；四是把密码法规、合规评价和职业伦理融入技术任务，提升学生的安全责任意识。

后续课程改革将围绕 AI 使用规范、竞赛任务难度梯度、学习画像可信度和课程目标达成评价开展持续验证。同时，可与企业、密码测评机构和竞赛平台建立更稳定的协同机制，推动《现代密码学》课程从知识传授走向能力生成和价值内化。

## 参 考 文 献

[1] 中华人民共和国教育部. 教育部关于加快建设高水平本科教育全面提高人才培养能力的意见：教高〔2018〕2 号[EB/OL]. (2018-10-12)[2026-05-04].

[2] 教育部等五部门. 教育部等五部门关于加强普通高等学校在线开放课程教学管理的若干意见：教高〔2022〕1 号[EB/OL]. (2022-03-10)[2026-05-04].

[3] 全国人民代表大会常务委员会. 中华人民共和国密码法[EB/OL]. (2019-10-28)[2026-05-04].

[4] 国家密码管理局. 商用密码应用安全性评估管理办法：国家密码管理局令第 3 号[EB/OL]. (2023-10-07)[2026-05-04].

[5] 杨波. 现代密码学[M]. 5 版. 北京：清华大学出版社，2022.

[6] 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——以仲恺农业工程学院为例[J]. 创新教育研究，2024，12(9)：330-336.

[7] 陈陟，王雪鹤，印鉴. 基于 OBE 理念的人工智能专业课程聚类探索[J]. 计算机教育，2025(4)：65-69.

[8] 张小东，战德臣，初佃辉，等. 基于学习成效的混合式程序设计课程教学改革[J]. 计算机教育，2025(5)：110-116.

[9] 陈静，张建勋，杨慧. 职业师范院校计科专业教学改革：从内容体系到教学模式的重构[J]. 计算机教育，2026(4)：225-231.

[10] National Institute of Standards and Technology. NIST Releases First 3 Finalized Post-Quantum Encryption Standards[EB/OL]. (2024-08-13)[2026-05-04].

[11] Kalita E, Alfarwan A M, El Aouifi H, et al. Predicting Student Academic Performance Using Bi-LSTM: A Deep Learning Framework with SHAP-Based Interpretability and Statistical Validation[J]. Frontiers in Education, 2025, 10: 1581247.