

应用型本科生软件逆向工程课程建设研讨

杨 斌

四川大学锦江学院计算机学院, 四川 眉山

收稿日期: 2026年5月22日; 录用日期: 2026年7月21日; 发布日期: 2026年7月31日

摘 要

随着信息技术的纵深发展, 以及对企业遗留(legacy)系统维护、再生工程、功能拓展与跨架构迁移、混淆恶意代码分析及提升威胁响应效率等的需求持续提高, 软件逆向工程作为高质量软件开发和系统分析的重要工具, 在应用型本科教育体系中, 其重要性及紧迫性日益凸显。文章基于建构主义学习理论与能力本位教育理论, 对目前应用型本科高校软件逆向工程课程建设所面临的问题进行了分析, 在科研及教学实践的基础上总结出课程设置不合理、教学内容与实际应用脱节、学生学习积极性不高、软件开发过度依赖于AI大模型是主要问题。针对以上问题设计以应用为导向的课程内容、教学方法、实践环节等。同时, 建立多元化的教学效果评价机制, 从理论考试、实践操作以及项目答辩等方面对学生的学习情况进行全方位考核。此外, 还对课程的先修要求和相关前沿技术进行了讨论, 指出了先修课程的重要性, 以及新兴技术对课程建设带来的影响。实践证明, 经过一系列课程改革后, 学生的原生软件开发能力、软件逆向分析能力及再生工程研发能力得到了很大提高, 有利于培养符合时代发展需要的应用型人才。

关键词

应用型本科教学, 软件逆向工程, 课程建设, 教学改革, 建构主义学习理论, 逆向分析前沿技术

Discussion on Curriculum Construction of Software Reverse Engineering for Applied Undergraduate Students

Bin Yang

School of Computer Science, Sichuan University Jinjiang College, Meishan Sichuan

Received: May 22, 2026; accepted: July 21, 2026; published: July 31, 2026

Abstract

With the deepening development of information technology, the demands for enterprise legacy

system maintenance, regeneration engineering, functional expansion, cross-architecture migration, obfuscated malicious code analysis, and improved threat response efficiency continue to grow. As an important tool for high-quality software development and system analysis, software reverse engineering has become increasingly significant and urgent in the applied undergraduate education system. Grounded in constructivist learning theory and competency-based education theory, this paper analyzed the problems currently faced in the construction of software reverse engineering courses in applied undergraduate institutions. Based on scientific research and teaching practice, the main issues identified include unreasonable curriculum settings, disconnection between teaching content and practical applications, low student learning motivation, and excessive reliance on AI large models in software development. To address these problems, application-oriented course content, teaching methods, and practical components have been designed. Meanwhile, a diversified teaching effectiveness evaluation mechanism has been established to comprehensively assess student learning through theoretical examinations, practical operations, and project defenses. Additionally, the prerequisite requirements and related cutting-edge technologies of the course are discussed, highlighting the importance of prerequisite courses and the impact of emerging technologies on curriculum construction. Practice has proven that after a series of curriculum reforms, students' native software development capabilities, software reverse analysis capabilities, and regeneration engineering research and development capabilities have been significantly improved, which is beneficial for cultivating applied talents that meet the needs of contemporary development.

Keywords

Applied Undergraduate Education, Software Reverse Engineering, Curriculum Construction, Teaching Reform, Constructivist Learning Theory, Cutting-Edge Technologies in Reverse Analysis

Copyright © 2026 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

软件逆向工程(Software Reverse Engineering, SRE)作为软件工程与信息安全领域的核心技术之一,在企业遗留系统维护、再生工程、功能拓展与跨架构迁移、混淆恶意代码分析及提升威胁响应效率等场景中发挥着不可替代的作用[1][2]。然而当前应用型本科高校在推进软件逆向工程课程建设的过程中,仍面临诸多瓶颈。主要表现在:课程体系设置滞后、教学内容与产业需求脱节、学生专业认知内驱力不足,以及生成式 AI 大模型滥用导致的核心代码思维退化等[3]-[5]。为此本文旨在基于教育学的理论视角,通过引入建构主义学习理论(Constructivist Learning Theory)与能力本位教育理论(Competency-Based Education Theory)作为学理支撑,探讨了面向应用型本科生软件逆向工程课程建设,开设软件逆向工程课程内容设置和课程教学方面的一些问题及特点;探讨如何正确传授课程内容,引导学生正确地应用方向、如何正确驾驭讲授的内容;分析了信息安全技术面临快速更新迭代的冲击、移动互联网和智能终端发展对信息安全学科及逆向工程课程带来的新挑战等。以建立合理有效的教学模式,对于培养符合时代要求的应用型高质量软件开发人才有着重要的意义。

2. 文献综述与理论基础

2.1. 软件逆向工程教育研究现状

近年来,国内外学者围绕软件逆向工程教育展开了多维度探索。在课程体系设计方面,袁庆军等[4]

提出了思维驱动的密码软件逆向工程教学设计,强调以认知建构为导向的教学内容组织;范文庆等[3]从通信学科视角探讨了软件逆向工程课程的内容设置,指出跨学科融合的必要性。在教学方法论层面,项目驱动教学法(Project-Based Learning, PBL)已被广泛应用于计算机类专业课程,其核心在于通过真实或仿真的工程情境促进学生的主动知识建构[6] [7]。

然而既有研究仍存在以下不足:其一是多数研究停留在经验总结层面,缺乏基于实证数据的教学效果验证;其二是对教育理论的援引较为零散,未能形成系统的理论分析框架;其三是对前沿技术模块的教学定位尚不明确,存在过度实操化或完全虚化的两极化倾向。因此,本文试图在整合建构主义学习理论与能力本位教育理论的基础上,构建一个兼具理论深度与实践效度的课程建设方案。

2.2. 理论基础

建构主义学习理论由 Piaget [8]的认知发展理论和 Vygotsky [9]的社会文化理论发展而来,其核心命题主张知识并非通过被动接受获得,而是学习者在特定情境中借助他人协助与必要学习资源,通过意义建构的方式主动生成。该理论强调情境、协作、会话与意义建构四大要素,与软件逆向工程课程所要求的复杂问题解决能力、团队协作素养及真实工程情境适应能力高度契合。建构主义学习理论为软件逆向工程教学提供了适切的理论框架。逆向分析任务的情境性、小组协作与会话机制,以及学生通过反编译与调试实现的意义建构,共同构成该理论的核心适用维度,故本文将其作为项目驱动式教学与翻转课堂设计的理论基石。

能力本位教育理论(Competency-Based Education, CBE)是起源于 20 世纪 60 年代的职业教育领域,其核心主张是以学习者获得特定职业能力为教育目标,而非以知识传授的时间长度作为衡量标准[10]。该理论强调:教育目标应明确界定可观察、可测量的能力指标;教学内容应围绕能力目标进行模块化组织;教学评价应以能力达成为核心导向。能力本位教育理论为软件逆向工程课程建设提供了系统化的设计框架,课程目标须分解为可量化的能力维度,教学内容应依循能力进阶逻辑进行分层组织,教学评价则需构建涵盖过程性与终结性指标的多元化评估体系。

3. 当前应用型本科生软件逆向工程课程教学现状

3.1. 课程设置方面

应用型本科高校在软件逆向工程课程设置上存在较大问题。目前不过半数的应用型本科高校开设了软件逆向工程课程,而大部分高校只是在网络安全概论或者恶意代码分析等课程中简单介绍了一些逆向工程的内容。课程学时安排不合理,理论课时过多,占总课时的一半以上,实践课时过少。而且课程开设时间不合理,有的高校把这门课程放在低年级,学生没有足够的计算机基础,影响学习效果。

课程内容缺乏前沿性和时效性是另一个问题。传统的课程设置是以静态分析和动态分析的基本概念为主,对于移动应用逆向分析、云安全逆向分析、物联网设备逆向分析等新兴领域较少涉及。目前企业对掌握现代化逆向工程技能的人才需求急剧增加,但是高校课程设置落后于行业发展需要。课程先修关系安排不合理,没有很好地与程序设计、数据结构、计算机组成原理等专业基础课程相联系,不利于学生形成良好的知识结构。

3.2. 课程教学方面

教学方法单一化是目前软件逆向工程课程教学所面临的问题之一。传统的以教师讲授为主的教学方式仍然占主流地位,缺少必要的实践教学环节。大多数教师还是用 PPT 来上课,学生处于被动接受知识的状态,缺少思考以及动手的机会。教学工具及平台有限,搭建实验环境困难,在课后很难进行自主学

习与实践。而且案例教学资源匮乏，目前的教学案例大多都是过时的经典案例，不能满足当今形势的需求。

师资队伍建设的亟待加强。具有丰富实践经验的逆向工程专业教师较为匮乏，大多数任课教师有较好的理论知识但是缺少企业工作经验。有逆向工程经验的高校教师占比较少，远不能满足教学需求。教学评价机制不健全，主要是通过期末考试来评价学生的学习成果，而忽视对学生动手能力和创新意识等方面的考核。课程设置与社会需求脱节，教学内容更新缓慢，跟不上技术进步的速度，不利于培养出符合社会需要的人才。

3.3. 学生学情方面

学生对软件逆向工程课程重要性的认识不够。只有少部分学生认为这门课程对自己以后的职业生涯有帮助，而大部分学生则把该课程当作可有可无的选修课。这样的观念影响了学生的学习热情与主动性，从而造成学生对该课程的关注度不高，学习效果不佳。学生对逆向工程技术的应用范围知之甚少，这不利于学生制定自己的学习目标。

基础知识储备不足是影响学生学习效果的重要原因。软件逆向工程课程对学生的基础知识有较高要求，包括汇编语言、操作系统原理等。约 3/4 的学生在学习这门课之前没有很好地汇编语言基础，对于操作系统内核的理解不够深刻。这些基础性的欠缺导致学生很难跟上课程进度以及进一步的学习，学生动手能力较弱，不能独立思考并解决一些较难的问题，在实际操作中遇到困难时不知所措。此外，生成式人工智能技术的普及引发了双刃剑效应。学生在软件开发中对大模型的过度依赖，正潜移默化地导致其底层逻辑推演能力与思维深度的退化，严重削弱了独立排查与修复复杂系统缺陷的原创性工程思维。

4. 研究方法

4.1. 研究设计

实验组干预措施涵盖五个维度：其一是课程体系重构，将传统理论讲授为主的结构调整为“基础 - 核心 - 高级 - 前沿 - 综合实验”的递进式能力培养路径，理论 - 实验学时比由 6:4 调整为 4:6；其二是教学模式革新，引入项目驱动教学法与翻转课堂模式，实现课前预习、课中协作探究与课后自主拓展的有机衔接；其三是教学资源建设，构建涵盖在线学习平台、虚拟实验环境及分级案例资源库的多元化支持系统；其四是评价机制改革，采用过程考核与结果考核相结合的多元化评估体系，强化实践能力与创新意识的考核权重；其五是专业认知强化，通过行业专家讲座、企业参观及成果展示等方式提升学生对技术产业价值与职业前景的认知。对照组维持以教师讲授为主、PPT 演示为辅助手段、期末闭卷考试为主要评价方式的传统教学模式。

4.2. 数据收集与分析

本研究采用多源数据收集策略以确保研究结论的验证。标准化测试问卷方面，课程前后分别施测软件逆向工程基础知识测验与反汇编代码阅读理解能力测验。项目评分标准方面，涵盖需求理解(20%)、工具应用(25%)、逻辑还原(30%)、报告质量(15%)及团队协作(10%)五个维度，采用 4 级李克特量表(1 = 不合格, 2 = 合格, 3 = 良好, 4 = 优秀)进行评分。动态调试能力测评方面，采用标准化实验任务要求学生独立完成指定二进制文件的动态调试、断点设置、内存扫描及运行时代码修改，依据操作完成度与准确性进行评分。课程结束后，对实验组学生施测学习体验与自我效能感问卷，涵盖学习投入度(5 题)、自我效能感(5 题)、团队协作满意度(3 题)及课程价值认同(4 题)，采用 5 级李克特量表计分。

定量数据采用 SPSS 26 进行统计分析。组间比较采用独立样本 t 检验(Independent Samples t-Test)，组

内前后测比较采用配对样本 t 检验(Paired Samples t-Test), 效应量以 Cohen's d 值表示。问卷数据采用描述性统计与探索性因子分析。显著性水平设定为 $\alpha = 0.05$ 。

5. 导向应用型人才的课程体系重构与教学创新

5.1. 面向应用的软件逆向工程课程建设

面向应用的软件逆向工程课程建设要以满足行业发展需要为导向, 建立适应应用型人才培养需求的课程体系。课程内容要注重实用性与先进性, 把传统的静态分析、动态分析方法与当前流行的逆向工程工具结合起来。课程内容包括 Linux 和 Windows 平台可执行文件分析、移动应用逆向分析、Web 应用安全分析等方面内容。同时, 由于云计算、物联网等新技术的发展, 课程还要涉及云服务逆向分析、嵌入式设备固件逆向分析等内容。表 1 展示了一种应用型本科生软件逆向工程课程教学内容设计, 各高校可基于自身教学实际, 对课程进行适应性调整与优化。教学案例亦应随技术发展与时代需求进行动态更新, 以保障教学内容的时效性与前瞻性。

Table 1. Course content design for application-oriented undergraduate software reverse engineering
表 1. 应用型本科生软件逆向工程课程教学内容设计

阶段	主要内容	核心知识点	能力重点	案例名称	实践目标
基础	逆向分析、软件逆向分析与密码软件逆向分析的概念内涵	逆向工程定义与伦理边界; 正向工程与逆向工程的辩证关系; 密码软件逆向的特殊性	明确课程学习目标; 建立逆向思维基本框架	如何仿制一枚原子弹	了解逆向工程基本思想[4]; 理解已知结果反推过程的方法论本质
	IDA Pro、x64dbg 工具安装与使用	反汇编器工作原理; 调试器架构(用户态/内核态); 断点类型(软件断点、硬件断点、内存断点)	工具基本操作方法; 断点设置与条件断点配置方法	TraceMe.exe 跟踪调试	掌握工具的基本操作和程序断点设置方法[4]; 能够独立完成单步跟踪与寄存器状态观察
核心	函数调用约定、栈帧结构与数据传递分析	x86/x64 调用约定(cdecl, stdcall, fastcall, thiscall, System V AMD64 ABI); 栈帧布局(EBP/RBP 基址指针、ESP/RSP 栈指针); 局部变量与参数在栈中的分布规律	分析程序控制流与参数传递方式; 识别编译器优化策略	SimpleFlows.exe 控制流验证分析	能追踪输入验证逻辑并定位关键判断语句; 能够绘制函数调用关系图
	软件保护机制识别、软件保护技术突破方法	序列号保护算法(对称加密/哈希校验); 时间限制机制(系统 API Hook 检测); KeyFile 保护结构; 网络验证协议逆向	序列号保护、时间限制、KeyFile 保护、网络验证的识别与突破方法	disable-Menu.exe Patch 关键字去除菜单功能限制	了解软件保护函数的参数设置以及修改方法, 掌握软件保护技术爆破方法[4]; 理解 Patch 技术的伦理边界
	内存扫描与动态修改技术(Cheat Engine 原理)	进程内存空间布局(堆、栈、代码段、数据段); 内存扫描算法(精确扫描、模糊扫描、变化量扫描); 代码注入与 DLL 注入原理	掌握运行时数据定位与修改方法; 理解内存保护机制(DEP/ASLR)	单机游戏金币值修改实验	实现指定变量的定位与数值修改; 能够编写简单的内存修改脚本
高级	脱壳技术: 识别 UPX、ASPack 等常见壳	可执行文件加壳原理(压缩壳/加密壳); 入口点(OEP)识别方法; Import Address Table (IAT) 重建技术; Dump 与修复技术	掌握手动与自动脱壳流程; 理解 PE 文件结构深层机制	PackedCrack Me.exe 脱壳技术实践	完成内存 Dump 与重建输入表操作; 能够区分不同壳类型并选择对应脱壳策略
	漏洞挖掘基础: 栈溢出原理与 ROP 链构造	缓冲区溢出机制(栈溢出/堆溢出); 返回导向编程(ROP)原理; Gadget 搜索与链构造; NX/DEP 绕过技术; ASLR 信息泄露利用	理解内存漏洞机制; 掌握 Exploit 开发基本流程	StackOverflowDemo.exe 漏洞实验	实现 EIP 控制并执行简单 Shellcode; 能够构造基础 ROP 链完成漏洞利用

续表

移动端逆向入门： APK 逆向分析与 Frida Hook	Android 应用结构 (DEX/ART/Smali)；APK 反编译 流程(apktool/dex2jar/JADX)； Frida 动态插桩框架原理；Java Native Interface (JNI)分析	掌握 Android 应用 逆向流程；理解运 行时 Hook 与静态 Patch 的区别	Simple LoginApp.apk 登录验证	使用 Frida 动态修改 返回值实现认证 Bypass；能够定位关 键校验函数并编写 Hook 脚本
前沿 技术	并行计算在代码相似性检测中的 应用；深度学习模型(如 BERT、 Transformer)在二进制函数识别 中的应用；后量子密码学基础与 抗量子逆向分析概念	掌握代码库并行处 理架构设计基本概 念；熟悉深度学习 模型二进制检测的 基本原理；理解后 量子算法逻辑及逆 向分析难点	面向车联网 固件的智能 化漏洞挖掘 系统(文献 研讨)	面向具备科研潜质的 学生，通过文献阅读 与专题研讨，主动探 索并行计算、人工智 能与量子计算在软件 逆向工程中的交叉融 合与前沿应用
综合 实验	独立完成 PC 端通信 协议逆向分析：解析 协议结构、逆向还原 算法逻辑、编写脚本 模拟请求与登录	网络流量捕获与分析 (Wireshark/tcpdump)；协议字段 识别(长度字段、校验和、加密 标志)；常见加密算法(AES/RSA) 逆向识别；Python/Go 脚本编写	掌握流量分析与算 法追踪；能将汇编 逻辑转化为高级语 言代码；理解授权 验证机制	协议破壁 者：通信协 议还原与模 拟登录
小组合作完成高级持 续性威胁样本深度分 析：脱壳逆向、行为 提取与威胁情报图谱 构建及检测规则开发	恶意代码脱壳与反混淆；动态行 为监控(API Hook/沙箱分析)； ATT&CK 框架映射；威胁情报 STIX/TAXII 标准；YARA/Suri- cata 规则编写	掌握高级恶意代码 反分析技术；熟悉 威胁情报图谱构建 与标准化报告及检 测规则编写	溯源追踪： 高级威胁样 本分析与可 视化情报图 谱构建	深度解析恶意软件攻 击链，构建可视化图 谱，产出威胁情报报 告与检测规则，实现 溯源闭环

课程设置要符合由浅入深的原则，要有层次感的知识脉络。基础部分主要让学生明确课程学习目标、了解逆向工程基本思想、掌握工具的基本操作和程序断点设置方法等。核心部分详细讲解栈帧结构分析、软件保护技术突破方法、内存扫描等。高级部分包括脱壳技术、漏洞发现、移动端逆向分析等内容。前沿部分探索并行计算、人工智能及量子计算在软件逆向工程领域的交叉融合与应用。综合实验依托项目驱动，培养学生综合技能整合、复杂问题独立求解及团队协作素养。每个部分都要有配套的实验环境以及相应的实验案例/项目，使学生能够将所学知识运用到实际中去。同时还要注意与其他相关课程之间的联系，形成一套完整的知识框架。

5.2. 教学内容的取舍与教学模式的革新

教学内容合理取舍是课程建设成败的关键，在有限教学时间里要抓住重点知识、技能点，不要贪多嚼不烂。基础理论部分要讲清楚二进制文件结构、CPU 指令集架构、内存管理机制等基本概念，为后面动手操作打下良好基础。工具使用要选用主流逆向工具，比如 IDA Pro、x64dbg 等，使学生了解并能熟练使用这些工具。案例分析要选取有代表性、符合时代要求的真实案例，包括各种软件以及不同难度的分析任务。

教学模式改革要突出应用型人才特点。项目驱动式教学是很好的一种方式，在此基础上设计一系列由浅入深的逆向工程项目让学生在中学。翻转课堂可以让学生更积极地参与到学习中来，学生课前自学相关知识，课堂上进行交流、实验、答疑等。团队合作有利于增强学生的沟通能力和团队意识，以小组的形式来完成一个相对较复杂的逆向工程项目。同时，构建多样化的教学资源支持系统，如在线学习平台、虚拟实验环境、案例资源库等，给学生提供更多学习资源和便利的学习条件。

5.3. 强化专业认知与学习内驱力的培养

提升学生对软件逆向工程课程重要性的认识可以从以下几个方面着手。产业需求导向的认识教育是

基础工作，可以请来行业人士做报告、带学生去企业参观、查看软件逆向工程人才需求情况等，使学生认识到逆向工程技术在软件开发行业的重要地位。逆向工程相关职位平均工资比一般程序员高约 1/3，这对学生来说是一个很大的吸引力。另外还可以给学生讲一些近年来软件逆向工程技术的案例，比如企业遗留系统维护、再生工程、功能拓展与跨架构迁移，混淆恶意代码分析等，让学生明白逆向工程技术的社会意义及其重要性。

课程的价值要贯穿始终，在课程开始时用一些有趣的例子来展示逆向工程的魅力，激发学生的兴趣。在教学中，设置一些阶段性的小成果展示，让学生感受到自己所学的知识是有用的。将课程的学习与未来的职业发展联系起来，比如学校与企业合作的项目、实习实训等，让学生在实际的工作环境中感受逆向工程的魅力。另外，树立榜样，让优秀的学长学姐讲述自己的故事，起到榜样作用，营造一种良好的学习氛围。而课程的考核也应该以能力为导向，用实践项目、创新作品等形式来检验学生的学习效果，让学生在学的过程中得到积极的反馈。

针对当前软件开发过度依赖 AI 大模型引发的思维浅层化，软件逆向工程课程可提供一种强制回归本质的矫正机制。通过系统性的底层代码剖析与逻辑还原训练，迫使学生跳出 AI 生成的黑盒表象，深入探究控制流、数据流、组件拓扑，以及算法模型等核心技术内幕。这种自下而上的逆向思维训练，不仅可有效重建学生的思维主体性，更能教会学生将他们所学的计算机各专业课程知识体系有机串联，实现理论与实践的深度融合，从而在掌握开发技术的同时，具备独立排查缺陷与深度优化的能力。

6. 教学效果评估与反馈

6.1. 评估体系构建

软件逆向工程课程的教学效果评估体系的制定要考虑到该课程的特点，即实践性强、技术更新快、应用场景复杂等。传统的单一考试评价方式已经不能很好地反映学生对软件逆向工程的理解程度，所以建立一个多元化的、多层次的评价体系就非常必要。评价体系应该包括学生对所学知识的理解程度、动手实践的能力、解决问题的能力以及团队合作的能力等方面的内容，在这四个方面分别给以不同的比例进行打分，以便更准确地衡量学生的学习情况。

多元化评估方式的实施需要有相应的评价标准以及操作流程。理论考核主要是考察学生对逆向工程的基本概念、原理、方法掌握情况，以客观题和主观分析题为主。实验操作评估是通过现场演示、操作录屏等方式，考察学生对逆向工程工具的应用能力和问题分析能力。项目实践评估是让学生独立完成一个完整的逆向分析项目，从需求分析到结果展示都要参与其中，锻炼学生的实际操作能力和解决问题的能力。小组合作项目着重培养学生的团队协作素养。同时建立一个评估数据库，记录学生在各个阶段的学习情况，以便进行个性化教学，让每个学生都能在自己的基础上得到提高。

6.2. 反馈机制建立

有效的反馈机制是提高教学质量的重要保证，在软件逆向工程课程中，反馈机制的设计要具有及时性、针对性以及建设性。设置多种反馈方式，如课堂上的即时反馈、阶段性反馈、期末反馈等，以便及时发现并解决问题。课堂上的即时反馈可以通过提问、实验指导等方式进行，使学生及时改正错误认识。阶段性反馈可以通过定期的小测验、实验报告点评等方式，让学生了解自己学习情况以及存在的问题。期末反馈则是通过对学生成绩进行详细分析以及对学生的能力进行评价，给学生以后的学习指明方向。针对 64 学时的课程教学(理论 - 实验学时比为 5:5 或 4:6)，表 2 展示了一种成绩计算方法，各高校可依据自身教学实际进行适应性调整与优化。

Table 2. Course grade calculation method
表 2. 课程成绩计算方法

考核类别	考核项目	对应能力维度	权重	考核频次
过程考核	1. 课堂考勤(100 分)	学习投入维持与学术承诺能力	10%	每周一次
	2. 课堂练习/表现(100 分)	即时知识迁移与情境应用能力	20%	每周一次
	3. 书面作业(100 分), 理论作业	理论建构与逻辑推演能力	30%	两周一次
	4. 上机实验(100 分), 专项实验	算法实现与工程化实践能力	40%	每周一次
结果考核	1. 期中成绩(100 分)	阶段性知识整合与重构能力	15%	每学期一次
	2. 期末成绩(100 分)	系统性知识统摄与迁移能力	15%	
	3. 综合案例(100 分), 独立完成项目, 中小规模	独立问题求解与系统思维能力	30%	
	4. 综合案例(100 分), 小组合作项目, 中大规模	协同创新与复杂工程驾驭能力	20%	
总计	100%			

注：四项过程考核合计 100%，占总计的 20%。

反馈信息的获取及处理要有制度化的保障。利用学生评教、同行互评、企业导师评价等方式获取教学情况信息，利用大数据方法对这些信息进行分析和比较，找出教学中存在的问题以及可以改善的地方。然后对这些信息进行归纳总结、分析判断，提出具体的解决办法。同时也要有反馈信息的效果跟踪，对所采取措施的效果进行评价，形成一个反馈 - 改进 - 再反馈的过程，不断提高课程的教学质量以及学生的学习体验。

7. 软件逆向工程课程的先修课程及前沿知识探索

7.1. 先修课程体系设计

软件逆向工程是一门综合性、技术性很强的课程，要求学生有良好的计算机专业基础。先修课程包括程序设计基础、数据结构与算法、计算机组成原理、汇编语言程序设计、操作系统原理、软件工程等。程序设计基础课程使学生具备基本的编程能力和对代码的理解能力，是以后分析反编译代码的基础。数据结构与算法课程帮助学生理解程序的逻辑结构，提高代码分析效率。计算机组成原理、汇编语言课程使学生了解底层硬件知识以及低级语言特性[5]，是进行深入逆向分析的基础。操作系统原理课程使学生理解程序运行环境及系统调用方式。软件工程课程使学生具有工程化思想以及项目管理能力，这些都是软件逆向工程学习的基础。

7.2. 前沿知识探索

随着计算机技术的发展，软件逆向工程也迎来了新的变化，新技术的应用给教学带来新的契机与挑战。并行逆向工程技术的发展大大提高了大规模软件系统的逆向分析效率，在把一个复杂的逆向问题拆分成若干个并行的小问题之后，用多核 CPU 或者集群来解决这些问题就可以大大节省时间并且更加准确[11]。这对于处理当今复杂的软件系统来说是非常有利的，尤其是对于包含几百万行代码的大型程序而言，传统的单线程方法已经不能满足需要了。并行逆向工程改变了逆向工具的设计思路，也对逆向工程师提出了更高的要求。

人工智能技术在软件逆向工程中发挥着越来越大的作用，正在改变这一领域的发展趋势。机器学习可以用来自动发现代码模式、预测程序的行为、发现恶意代码的特点等，使逆向分析更加自动化。深度

学习对于二进制代码的分析、函数的识别以及漏洞的发现都有很好的效果，在面对混淆或者加密的代码时，基于人工智能的逆向工程工具可以很快找到重要的代码部分，找出程序的主要功能。自然语言处理的应用让逆向工程工具可以自动生成代码注释和分析报告，提高学习效率。然而，人工智能技术的渗透亦构成双刃剑效应：一方面，对抗性机器学习的发展促使恶意软件采用逃逸攻击与对抗样本技术主动规避智能检测系统，对逆向工程师的 AI 素养提出更高要求；另一方面，需明确区分两类应用场景，在 3.3 节学生学情分析中批判的是学生利用大语言模型进行代码生成的偷懒式认知外包行为，而技术前沿所倡导的则是基于 AI 的自动化漏洞挖掘、二进制代码克隆检测以及反混淆分析等深度应用。唯有厘清此界限，方能准确把握人工智能赋能逆向工程的本质内涵。

量子计算的发展为软件逆向工程带来了范式层面的变革。量子计算机强大的并行计算能力可攻破基于传统数论难题(如大整数分解、离散对数)的密码体系，这将深刻改变软件保护与逆向分析的技术格局。量子逆向工程(Quantum Reverse Engineering)旨在利用量子算法的优势，在多项式时间内解决经典计算机上需指数时间求解的问题[12]。此外量子纠错技术与量子软件的发展亦为逆向分析提出了全新命题，传统的逆向工程手段对于量子程序几乎无能为力[12]。尽管量子计算尚处于早期发展阶段，但其潜在影响已引起学术界与产业界的高度重视，后量子安全的软件保护技术研究已逐步展开。在应用型本科教育层面，量子逆向分析技术应定位为前沿视野拓展模块，以理论通识讲座形式引入，如专题讲座或文献阅读研讨，侧重于概念理解和前沿追踪，不要求本科生掌握量子电路的底层逆向实操，旨在培养其面向未来的技术敏锐度与抗量子安全思维，为其后续深造及职业发展奠定前瞻性的知识基础。

8. 研究结果与讨论

教学改革实施后，对实验组与对照组的学习成效进行了系统评估，主要结果如表 3 所示。结果表明，实验组在基础知识测验成绩($t = 4.31, p < 0.001, d = 0.81$)、反汇编代码阅读理解准确率($t = 11.87, p < 0.001, d = 2.24$)、动态调试工具链综合应用能力($t = 10.96, p < 0.001, d = 2.05$)及逆向分析项目综合评价($t = 11.42, p < 0.001, d = 2.12$)等维度均显著优于对照组，且效应量均达到大效应水平(Cohen’s $d > 0.8$)。其中，反汇编代码阅读理解准确率的提升尤为突出，由对照组的 37.12%提升至实验组的 64.29%，增幅达 27.17 个百分点，验证了以应用为导向、以建构主义理论为指导的课程改革方案在提升学生底层代码分析能力方面的显著效能。

Table 3. Comparison of learning outcomes between the experimental and control groups (M ± SD)

表 3. 实验组与对照组学习成效对比(M ± SD)

评价维度	实验组(n = 56)	对照组(n = 52)	t 值	p 值	Cohen’s d
基础知识测验成绩(后测)	78.32 ± 8.47	71.15 ± 9.23	4.31	<0.001	0.81
反汇编代码阅读理解准确率	64.29% ± 11.36%	37.12% ± 12.84%	11.87	<0.001	2.24
动态调试工具链综合应用能力测评	82.16 ± 9.52	61.38 ± 10.71	10.96	<0.001	2.05
逆向分析项目评价量规(REPR)总分	3.42 ± 0.48	2.31 ± 0.56	11.42	<0.001	2.12
学习投入度(问卷)	4.12 ± 0.63	—	—	—	—
自我效能感(问卷)	3.89 ± 0.71	—	—	—	—

注：实验组问卷数据为组内描述统计，对照组未施测该问卷。

研究表明，基于建构主义与能力本位教育理论的课程改革方案在提升应用型本科生软件逆向工程能力方面具有显著优势。项目驱动式教学促进了学生的主动知识建构，翻转课堂模式优化了课堂时间配置，

多元化评价机制保障了实践能力考核权重。然而,准实验设计存在选择偏差等内部效度威胁,单一院校样本限制了外部效度,且缺乏长期追踪评估。未来研究宜扩大样本规模,采用随机对照试验设计并开展纵向追踪,以更严谨地验证课程改革的持续效应。

9. 结束语

应用型本科生软件逆向工程课程建设是一项系统工程,要从课程建设、教学内容、教学方法、师资力量等方面进行整体规划。目前课程建设存在的问题主要是缺乏系统性、实用性不够、与社会需求脱节等问题。而通过建立以应用为导向的课程体系、改革教学方式、加强实践环节等手段可以很好地解决这些问题。面向未来,软件逆向工程课程建设要与时俱进,把最新的技术、方法及时引入到教学中来,以保证所培养的人才具有一定的前瞻性以及适应性。另外,还需要进一步加强与企业的合作,形成校企联合培养的人才培养模式,给学生提供更多的实习机会以及就业方向。这样,应用型本科高校就可以培养出更多符合社会需求的高水平逆向工程技术人才。

最后需要特别强调的是,软件逆向工程与网络安全领域紧密相连,其技术应用并非总是合法合规的。因此,在软件逆向工程课程的建设中,必须高度重视并强化课程思政建设。在教学过程中,应着重加强对学生的法律意识与职业道德教育。唯有如此,才能培养出既具备精湛技术,又拥有高尚品德,真正对社会有用的软件逆向工程技术专业人才。

参考文献

- [1] 张平,李清宝. 反编译技术[M]. 北京: 科学出版社, 2023: 19-211.
- [2] 庞建民. 编译与反编译技术实战[M]. 北京: 机械工业出版社, 2017: 129-355.
- [3] 范文庆, 黄玮, 安靖. “软件逆向工程”课程内容设置的探讨[C]//中国通信学会, 辽宁省通信管理局. 第十届中国通信学会学术年会论文集. 北京: 中国传媒大学理工学部计算机学院, 2014: 119-121.
- [4] 袁庆军, 薛昊原, 陆思奇, 等. 思维驱动密码软件逆向工程教学设计[J]. 计算机教育, 2023(11): 135-139.
- [5] 郑天明. 二进制安全基础[M]. 北京: 清华大学出版社, 2025: 1-268.
- [6] Krajcik, J.S. and Shin, N. (2014) Project-Based Learning: A Promising Approach to Supporting Student Learning. In: Sawyer, R.K., Ed., *The Cambridge Handbook of the Learning Sciences*, Cambridge University Press, 275-297. <https://doi.org/10.1017/cbo9781139519526.018>
- [7] Blumenfeld, P.C., Soloway, E., Marx, R.W., Krajcik, J.S., Guzdial, M. and Palincsar, A. (1991) Motivating Project-Based Learning: Sustaining the Doing, Supporting the Learning. *Educational Psychologist*, **26**, 369-398. <https://doi.org/10.1080/00461520.1991.9653139>
- [8] Piaget, J. (1950) *The Psychology of Intelligence*. Routledge & Kegan Paul.
- [9] Vygotsky, L.S. (1978) *Mind in Society: The Development of Higher Psychological Processes*. Harvard University Press.
- [10] Spady, W.G. (1994) *Outcome-Based Education: Critical Issues and Answers*. American Association of School Administrators.
- [11] 贾明飞, 董渭清, 黄泳翔. 基于分布存储系统的并行编译关键技术[J]. 计算机工程与应用, 2003(22): 103-106+152.
- [12] 刘光明. 基于经典与量子混合架构的软件脆弱性分析技术研究[D]: [硕士学位论文]. 郑州: 郑州大学, 2023.