 DOI: https://doi.org/10.26549/jxffcxysj.v3i16.6252

Exploration on the Construction of Hybrid Course of Cryptography

Yihua Zhou[1] Weimin Shi[1] Yuguang Yang[1] Bo Zhang[2]

1.Institute of Information Security, Faculty of Information Technology, Beijing University of Technology, Beijing, 100124, China
2.Information Media Institute, Beijing College of Politics and Law, Beijing, 100023, China

Abstract

In view of the problems existing in the teaching process of cryptography, such as lack of value guidance, rigid teaching methods, lack of practical teaching, unclear language expression, lack of self-control and so on, this paper analyzes the current situation of the construction of cryptography curriculum, and puts forward a mixed teaching mode of cryptography with multiple integration, which realizes the mixing of knowledge and values, online and offline mixing, theory and practice the combination of Chinese and English teaching methods, international vision and domestic standards can improve students' learning interest and learning efficiency.

Keywords

cyberspace security; cryptography; hybrid teaching; flipped classroom

密码学混合式课程建设探索

周艺华[1] 侍伟敏[1] 杨宇光[1] 张博[2]

1. 北京工业大学信息学部信息安全研究所，中国·北京 100124
2. 北京政法职业学院信息媒体学院，中国·北京 100023

摘　要

针对密码学教学过程中存在缺少价值引领、教学手段僵化、实践教学缺失、语言表达不清、缺少自主可控等问题，论文分析了当今密码学课程建设现状，提出了多元融合的密码学混合式教学模式，实现了知识与价值观的混合、线上与线下的混合、理论与实践的混合、中英文教学方式的混合、国际视野与中国标准的混合，提高了学生的学习兴趣和学习效率。

关键词

网络空间安全；密码学；混合式教学；翻转课堂

1 密码学课程建设现状

随着网络技术的飞速发展和广泛应用，网络空间安全被提升到国家安全战略高度。习近平总书记指出：“没有网络安全就没有国家安全”，网络安全事关经济发展、社会稳定和国家安全。《密码学》课程是网络空间安全一级学科的核心专业课程，信息安全专业通常以密码学为基准，辅以计算机技术、通信网络技术等课程，构建课程体系，可以说没有密码学，就没有信息安全专业。建设好《密码学》课程对深入学习网络空间安全其他课程、网络空间安全一级学科的发展以及提升信息学科的核心竞争力具有显著的作用。

由于密码学是一门交叉学科，涉及理论性较强、学科多、知识体系繁杂、学生基础薄弱、教学体验差等一系列问题，中国和国际上的高校教师对密码学课程的教学模式与方法进行了不断的探索和改革。秦艳琳等 [1] 将“以学为中心”的探究式教学理念与方法引入密码学课堂，改进了灌输式教学模式的弊端；陈华瑾等 [2] 针对高层次人才需求，提出了区分教学内容、教授与讨论相结合以及双向教学总结的教学模式；吴万青等 [3] 基于网络平台，设计了混合式教学方法，优化了教学内容和教学方法，提高了课程的掌控能力；魏悦川等 [4] 将混合式、参与式教学理念运用到教学之中，提高了学生的参与程度及自主学习能力；蒋静等 [5] 采用翻转课堂教学模式设计了密钥分享方案的教学过程；吴旭光等 [6] 建立了包含基础实验平台、实训平台和创新应用平台的三层次密码实践环境，提升了学生的密码学实践技能；这些研究成果强调学生和教师的互动、提高了学生的实践能力、一定程度上优化了教学内容。由于密码学课程的理论性、前沿性、交叉性、实

 DOI: https://doi.org/10.26549/jxffcxysj.v3i16.6252

践性和国际性等特性，很难用一种或简单的几种教学模式达到优化的教学效果，有必要对密码学课程的深度混合教学模式进行研究和探索。

2 传统密码学教学中存在的问题

由于密码学是以信息安全数学、信息论、概率论、线性代数等为基础建立的信息安全保障体系，其安全性建立在计算复杂性理论之上，且主流的密码算法多数由国际首先提出并引入，造成传统的密码学课程教学存在如下突出问题。

2.1 侧重知识传授，缺少价值引领

传统密码学课程的教学过程中，侧重知识的传授。例如，算法的数学基础、算法的安全性分析以及算法的应用领域等，普遍认为科学无国界，缺少对思政元素的挖掘和价值的引领。

2.2 教学手段僵化，教学模式落后

传统密码学课程的教学手段普遍采用讲授方式，教学模式也基本采用线下课堂教学辅以提问、作业等方式。随着网络技术的发展，慕课、微课等教育模式的兴起，很多学校以线上教学方式取代了线下教学，但线上教学是针对大量群体制作的精品课程，考虑到接收群体的可接受性，基础性强，难以适应各个学校的专业特色。另外，线上教学教师一般都比较拘束，风趣性、互动性不足，需要线下教学对教学内容进行混合补充。

2.3 偏向理论教学，忽视实践培养

传统密码学教学普遍偏重于理论知识的教学。例如，阐述加 / 解密、签名算法基于的困难问题、密文不可取分性原理、攻击者模型等，受学时不足、算法实现复杂、算法结果可视性差等特性的限制，教师一般基于开源的 OpenSSL、CryptoPP 等开源密码库调用现成的算法进行实现，起不到应有的实践效果。

2.4 内容描述不准，语言表达不清

传统密码学的教材一般选用中国教师编写的教材，很少选用国际上的教材，授课语言绝大多数采用中文教学。受限于密码算法产生的背景、文化差异等，有些国际上的算法翻译成中文之后就失去了原有正确语义，准确性不足。而直接选用英文教学，受母语的限制，学生的可接受性较差，有必要探索中文、英文混合教学机制，而不是简单的中文、英文或双语教学。

2.5 偏重国际算法，缺失国密标准

传统密码学教学普遍选用国际流行的密码算法。例如，对称密码算法中的 DES、AES 算法，非对称密码算法中的 RSA、离散对数算法，数字签名算法中的 ElGamal 算法等，对中国密码算法 SM2、SM3、SM4 及 ZUC 往往一带而过或由学生自学完成，造成学生国密算法认知的缺失。

3 密码学混合式课程教学模式的探索

针对密码学课程的特点及传统教学过程中存在的不足，探索了多元融合的密码学混合式教学模式，包括知识与价值观的混合、线上与线下教学模式的混合、理论与实践教学的混合、中英文教学方式的混合和国际视野与中国标准的混合等。

3.1 知识传授与价值塑造相结合

深入挖掘密码学课程的专业知识内容与其中蕴含的思政育人素材，选取接地气的时事热点和经典案例教育引导学生，鼓励学生发愤图强、努力开发和掌握核心技术，突出学生品格塑造，实现知识传授与价值引领的有机统一。例如，通过 1993 年的“银河号事件”，美国借助 GPS 卫星导航系统围困“银河号”，迫使中国自主发展自己的北斗导航卫星系统。而北斗导航系统的有效运行很大程度上依赖数据传输的保密性、完整性和认证性等密码技术，通过将案例自然融入专业课程教学中，达到润物细无声的境界，激发学生的研究兴趣和责任担当。

3.2 线上与线下教学相结合

随着慕课、微课这类全新教育模式的兴起，以翻转课堂、

【作者简介】周艺华（1969–），男，博士研究生，副教授，现任北京工业大学信息学部信息安全研究所副所长，从事信息安全研究。

侍伟敏（1978–），女，博士研究生，副教授，现就职于北京工业大学信息学部信息安全研究所，从事信息安全研究。

杨宇光（1976–），女，博士研究生，教授，现就职于北京工业大学信息学部信息安全研究所，从事信息安全研究。

张博（1976–），男，硕士研究生，副教授，现任北京政法职业学院信息媒体学院副院长，从事网络安全研究。

【基金项目】北京工业大学密码学混合式课程建设项目（项目编号：KC2018MT008）；北京工业大学研究生精品课程建设项目（项目编号：CR201906）；2020 年北京工业大学信息学部计算机学院院级教育教学项目（项目编号：2020JSJJX007）；2020 年北京政法职业学院科研课题《职业院校技能大赛促进教学机制研究——以计算机网络技术为例》（项目编号：KY202001）。

 DOI: https://doi.org/10.26549/jxffcxysj.v3i16.6252

学生为中心的混合式教学应运而生。但如何混合、混合程度如何、混合内容如何，没有统一标准，使用不当，往往会增加学生负担、浪费教学资源。针对密码学课程的特点，服务端采用日新学堂网络教学平台，客户端采用学习通的混合式教学模式，将签到、通知、作业、讨论这类比较费时的内容改为线上模式，大部分教学内容仍采用线下教学，同时采用学习通的同步课堂或腾讯会议的实现远程同步教学，利用录像功能实现课程回放。为了解决学生对困难问题的理解，制作了专门的难点答疑视频、算法动画演示、国际上的视频中文配音讲解等。充分利用了线下教学的互动性、参与性、可监督性、趣味性和线上内容的丰富性、选择性、自学习的特点，取得了理想的教学效果。

3.3 理论与实践相结合

密码学课程普遍存在实践学时不足现象，因而很多学校采用了国际通用的开源平台，只是使用一下函数接口，获得对密码算法的验证性实验，起不到对算法原理的理解和进一步设计优化的目的。如果将整个算法交给学生去完成，学生往往短时间内难以完成复杂的密码算法。为此，本课程设计了模块化实验平台，将密码算法划分成多个模块，如将 DES 算法划分为：文本输入 / 输出模块、图像输入 / 输出模块、置换模块、S 盒替代模块、ECB 及 CBC 分组模块等，每一模块定义完好的输入输出接口，这样学生就可以把主要精力花在核心功能设计上，减轻了学生的负担，提高了程序完成的正确率，实现了理论与实践算法的有效结合。

3.4 中文与英文双语教学方式相结合

针对中英文文化和描述的差异，在密码学的教学过程中不应该统一采用某一种语言进行教学，也没有必要采用双语方式讲一遍英文，然后再用中文进行解释，这样反而会浪费更多的学习时间，而应该在恰当的时机对恰当的内容选择不同的语言。例如，Random Oracle Model 就可以使用中文“随机预言机模型”，而不会影响其对语义的理解，而 Oracle 公司翻译成甲骨文公司，就失去了其本来的意义，个人认为这种类型的英文可以直接使用英文。再如，Hash 函数，该词的本意是杂乱信息、无用信息，翻译成哈希函数，反而不如直接用 Hash 更准确，因为通俗的中文中并没有“哈希”这个词，同样有些算法的解释如果用中文翻译不如直接用英文表达的意思更准确，则直接用英文进行解释和讲解，通过挖掘中英文表达的差异，提高了理论与算法解释的准确性。

3.5 自主可控与国际视野相结合

针对传统密码教学普遍采用国际密码的问题，有些院校要求将国密算法替换为国家商密算法。受限于商密算法资料的困乏，一般的商密算法基本上介绍算法的过程，缺少对原理的精细解释和分析，造成学生理解上的困难。为此，采用了对比教学的方法，首先讲解主流的国际密码算法，然后在讲解商密算法时让学生对比分析国际算法与商密算法异同点，吸收了哪些优点，又抛弃了哪些不足，吸收与抛弃的原因等。以商密算法 SM4 为例，对比发现 SM4 采用了类似 DES 的非平衡 Feistel 结构，而非 AES 的 SP 结构，优点是加解密具有相似性，加密与解密算法相同，这样加密机和解密机可以用相同的设备，而 AES 加密和解密就必须用不同的算法和设备。但 SM4 的非线性 S 盒却吸收了 AES 算法的字节替代方案而非 DES 算法中的非对称压缩替代，消除了 DES 算法中 S 盒设计不公开、存在后门或漏洞的疑惑，增强了安全性，通过对比分析，学生不但能轻松地学会了复杂的 SM4 算法，还提高了设计密码算法的能力，最终达到青出于蓝而胜于蓝的境界，实现了国际视野与自主可控密码教学的有机统一。

4 结语

论文针对密码学课程教学过程中存在的不足，深入研究了混合式教学过程中的融合内容、融合模式、融合方法、融合技术、融合文化等，对多元融合的密码学混合式教学模式进行了研讨，提出了课程的改进思路，提高了课程的互动性、参与性、趣味性及内容的准确性、丰富性、选择性等，取得了满意的教学效果。

参考文献

[1] 秦艳琳 , 胡卫 . 密码学探究式课堂教学设计实例与分析 [J]. 计算机教育 ,2020(01):112-115.

[2] 陈华瑾 , 张昊 , 王中孝 . 高层次密码学课程实践探索 [J], 计算机教育 ,2020(16):16-18.

[3] 吴万青 , 杜瑞忠 . 基于网络平台的混合式教学法在密码学教学中的效果评价 [J]. 网络与信息安全学报 ,2019(03):96-101.

[4] 魏悦川 , 韩益亮 . 计算机密码学课程的混合式、参与式教学研究与实践 [J]. 计算机教育 ,2019(03):27-29.

[5] 蒋静 , 李高仕 . 翻转课堂在密钥分享方案教学中的应用 [J]. 福建电脑 ,2020(02):118-119.

[6] 吴旭光 , 韩益亮 , 朱率率 , 等 . 密码应用与实践课程建设探索 [J]. 计算机教育 ,2020(03):8-11.