文章类型：论文 | 刊号（ISSN）：2630-4686 /（中图刊号）：380GL020

理论与实践教学相结合提升课程育人效果——以工科《计算机密码学》课程教学为例

刘小跃* 李旅军
韩山师范学院
DOI:10.12238/er.v8i4.5991

摘　要：随着《计算机密码学》教学的不断发展，教学目标已经从以往的理论教学转向了理论和实践的融合。此外，我们还关注学生学习的成长。因此，本篇文章将针对《计算机密码学》这门课的独特性，研究案例教学法的应用。这种创新的教学方法，它融合了富有活力的密码学抽象的理论知识和实例，不仅有助于学生更好地理解和掌握所学的密码学知识，也能显著增强学生应用理论知识的技巧。
关键词：理论；实践；计算机密码学；教学改革
中图分类号：G420 **文献标识码：**A

The Combination of Theory and Practice Teaching Improves the Effect of Curriculum Education——Taking the Teaching of "Computer Cryptography" as an Example

Xiaoyue Liu*, Lvjun Li
Hanshan Normal University

Abstract: With the continuous development of computer cryptography teaching, the teaching goal has shifted from the previous theoretical teaching to the integration of theory and practice. In addition, we also pay attention to the growth of students' learning. Therefore, this article will focus on the uniqueness of the course 'Computer Cryptography' and study the application of case teaching method. This innovative teaching method, which combines the abstract theoretical knowledge and examples of cryptography, not only helps students better understand and master the knowledge of cryptography, but also significantly enhances students' skills in applying theoretical knowledge.
Keywords: Theory; Practice; Computer Cryptography; Teaching reform

引言

目前计算机、网络、电子支付等极度发达的社会环境中，窃取他人密码、非法侵入他人的密码保障系统的事情每天大量发生，现代大学生，特别是学习计算机密码学课程的大学生应承担相应的社会责任和历史使命。

一、传统教学中存在的问题

（一）学生主体缺位、参与性不强

在传统的教育模式中，教师的授课是核心，而学生则是被动接受知识，他们的角色更像是旁听者，这种模式的特性就是缺乏参与感，过分强调理论知识，而忽视实际经历。讲授密码学涉及近世代数基础和初等数论等数学概念，定理和数学公式的枯燥性使得学生在理解上感到困难。如果无法跟上老师的教学步伐，他们可能在未来的学习过程中陷入模糊不清的状态，这会降低他们的学习热情。学生往往将注意力不集中在学习上，而是转向了考试，常常只是机械的记忆知识点。在课程里，学生的核心角色并未得到充分地重视，他们无法全身心投入到教育活动，导致了教育成果的欠缺。

（二）教学手段单一、教学模式落后

在传统的教育方法里，教师只是使用黑板和幻灯片来进行讲解，这样的灌输式教育方法并不能有效地识别出每个学生的独特性。由于教育者与学生之间的互动和沟通不足，使得学生很难把握课程的核心，教师也无法准确掌握学生的学习进度，这样就降低了教学的效果，并阻碍了学生思考能力的提升。

（三）教学止于课堂，学生创新能力不足

目前的密码学课程涵盖了大量的知识点，并且需要在有限的时间里进行教学，这使得学生往往只是肤浅地理解，缺乏深入的研究。这使得那些对此感兴趣的学生感到无聊，无法全身心投入，也无法有效地提高他们的创新和实践能力。尽管我们在密码学领域进行了一系列的科研工作，包括数据压缩、编码设计以及密码学设计原理，科研实验环境也已经初步形成。然而，这些方法在解决“网络与信息安全”的实

际问题上还未得到应用，还没有建立一个完备的教学实验环境，无法满足学生课后进行相关实验的需求。学生们的知识掌握，主要是通过阅读教科书、查找资料和做好课后的练习题来实现的。

二、《计算机密码学》融入理论与实践相结合的新要求

（一）兼顾数学、编程技术基础来重塑课程

网络安全涉及数学、计算机技术、通讯等多个学科的综合性研究，其人才的塑造必须依赖于专门的学术理论与实际操作技巧的完美结合。原先的计算机密码学课程主要侧重于数学基础的训练，然而，对于网络空间安全学科的深入发展，学生的各种能力必须得到充分的整合。因此，我们决定采取一种以数学与编程技术的相结合、加强实际工作的课程方案：首先，我们需要扎实的数学理论基础，深入研究密码算法、密码协议、密码应用、密码系统等方面的数学基本概念，从而科学地调整数学与编程课程的逻辑联系及其比例的分布[1]。构建了如代数和分析、概率和统计、组合和保护、密码理念以及密码运用等多个教学部分。其次，我们需要强化编程技术的基本功。我们倡导学生们和其他专业的同学们一起参与各类比赛，以此来持续提升他们对密码学的认识。其三，我们需要加强对计算编程的理解，激发学生的算法思考能力，训练他们把数学知识转换为编程算法的技巧。

（二）增加课程的实践比重

针对网络安全领域的人才需要，我们对教学设施进行了改良，并将课程的实践部分的学习量从过去的 16 学时提升至 32 学时，这一部分的学习量大概是整个计算机密码学课程的二分之一。增加课程的实践比重的目标是提高密码的运用技巧。首先，我们需要扩大密码学信息知识面，强调密码算法的实践性，以此来推动教学活动，提升技术素质。我们需要持续地丰富和完善教学内容，让学生能够熟练运用密码技术，并且在实践中不断积累知识。二是我们需要改革实践环境，增强实践意识，通过模拟和仿真真实的环境，使学生能够亲身体验到真实的工作气氛和工作流程。这样，他们不仅能迅速掌握网络空间安全实践的技巧和素养，还能在一个包含全部场景、全部步骤、全部感知的综合性实践环境中进行有效的训练[2]。三是实施小组的实践项目，致力于提升小组的实际操作技巧，并主动推行以主题、应用型产品的开发为主线的教育模式。我们根据学生的学业水平，把他们分配到 3~5 个小组中，引导他们进行与现实生活中有关的网络安全产品的主题探讨。我们还会通过完成各种综合素质项目和学生的创新策略，并通过举办一系列的网络安全比赛来提升他们的工程实践综合技能。

（三）面向产业、课程吻合实际需求

我们的最终目标是满足产业的需求，并且能够适应网络空间安全相关的行业。通过实际应用如区块链，确定实践科目的主题为工作量证明机制的实验，强化密码算法的实际运用，理解密码算法在区块链系统安全中的重要性。关于如何进行具体的策略：首先，我们需要让所有人都有所进步，并且根据训练的目的，创造出更加实用的实战课程。我们需要规划和执行训练过程，并根据不同的级别来决定训练的方式。我们还需要改进和优化专门的教育和训练设备，以便打造出一个包含“教育、训练和协作”的密码学控制和协同开发的课程[3]。其次，我们需要增强基础技术的培养，在代码解读、数据解读、算法解读和系统解读这四个方面都安排相应的课程训练，以此来提高有针对性的培养，并进一步提升学生的学业技术水平。这主要是因为我们需要应对密码攻击和防御的信息不平衡问题，以此来提高学生们的密码信息分析和处理能力。同时，我们也需要让他们掌握如何在实际操作中应用这些技巧，以此来提升他们的创新和执行能力。

三、理论与实践相结合在《计算机密码学》的运用

（一）实施多元化的参与式教学，提供各种学习的机会。

采用互动型的教育方法进行授课，可以让学生积极投入到课堂中，感受到知识的建立。据研究显示，优秀的教育工作者会把 15%的精力用于调整他们的授课方式，同样的，他们也会投入 50%的精力去参与各类交流活动。我主要通过两种方式来增强学生的参与度。首先，我们需要增加教育方法的多样性，通过各类方法让学生积极投入课堂活动之中。教室里，我们能够融合诸如提问、探讨、争议、思维激荡、双向互动等活动，旨在给予学生丰富多样的学习体验。比如，当我们讨论序列密码算法的随机性这一主题时，我会展示一系列二进制序列，让学生们互相探讨序列的特征，接着根据随机性的强弱对其进行排序，并通过小组间的辩论等方式来确定评估序列随机性的标准[4]。其二，进行更深入的思考过程，激发学生共同研究和寻找答案。依照 Bloom 的思考方式，仅靠记忆或者理解是无法推动学生的高层次思考的提升的，必须通过分析、整合、评价、规划等方式的培养。所以，我们可以构建一个任务导向的教育环节，让学生们通过协同工作来实现目标，从而达到学习的效果。最终，我们会在课程中进行详细的讲述与讨论，同时，老师也会作出相应的指导与概括。比如，当我们研究数据加密标准 DES 的过程中，我会把 DES 轮函数的四个部分分配给四个小组的学生进行预习和讨论。接着，每个小组都会选出一名代表来向其他的学生详细解释，并对其设计特性进行评价，同时也会回答其他学生的疑问。此策略能够最大限度地激发学生的独立学习和分析技巧，并且倡导他们彼此之间的交流，最大化同伴的影响力，从而有效地提升学生的热情，挖掘他们的潜力。实施参与性的学习方法，凸显了学生在学习过程中的核心角色，

增进了老师和学生以及学生和老师的交流，颠覆了传统的单向教育方法，构建了复杂的反馈系统。

（二）深度运用各类教学平台，探索理论与实践相结合模式

为了适应信息化时代对人才培养的新挑战，我们需要摒弃传统的班级授课模式，转向将课堂讲解、综合设计、创新实践和网络教学紧密融合的多元化教学方式。这样，学生就能在学习中应用知识，真正实现学以致用，全面提升他们的综合素质。首先，利用互联网信息以及多媒体工具来整合教育材料。利用各类教育资源，使教学更具生动性和吸引力，激发学生的求知欲和学习热忱。比如，当讨论 AES 加密的问题时，简单的理论教学往往无法引发学生的热情，他们本身也对加密流程感到困惑。然而，当我们制作了 AES 加密的动画，并通过动画展示，这不仅能激发学生的兴趣，还能帮助他们更深入地理解每个加密步骤的效果。针对古代 SK、RSASK、Diffile-HellmanSK 交换协议等相关主题，创建了一套精心设计的微型课程[5]。利用先进的多媒体科技，我们的教学方式不只是增强了课堂的效益，拓宽了教育的范围，同时也让学生们的学习变得更加愉快和富有乐趣，实现了事半功倍的成果。其次，通过利用信息技术和教学平台，实现了传统教育与信息化教育的融合。比如，在课程开始前，学生可以通过平台获取预习资料，然后利用终端进行自我学习。在课程中，我们利用平台进行思维激荡和实时监测。课后进行深度讨论和复习解答等活动。利用这个平台，教师与学生能够进行实时的交流，这对于教师理解学生的掌握情况以及多种方式获取教学反馈大有裨益。此外，借助信息技术工具，学生可以在零散的时间里随时随地进行学习，从而扩大了他们的学习时间和范围。最后通过 MOOC 来融合传统的教学方式与 e-learning。MOOC 的存在为传统的教学方式带来了强大的支持[6]，比如，斯坦福大学的 DanBoneh 教授所讲解的密码学得到了广泛的赞誉。我们可以利用这些资源，对密码学的课堂内容进行适当的改造，让学生在课后独立观察并完成相关的学习任务，包括提出问题、完成个别任务、团队任务及整理课后的学习内容，从而增强学生的学习积极性和参与感。

（三）教学方法采用任务引导，并广泛进行实践活动

通过自我实践，学生可以亲身感受到实际操作的乐趣，并在此过程中积累经验，从而对自己的技能和专业知识有更深入的理解。通过实际操作，可以让学生最大限度地激活其主观能动性，并且增强他们利用所掌握的信息来探究和处理问题的技巧，从而进一步提升其创新思维和实际操作的技巧。在讲授密码学的过程里，我们专门为学生们制定了诸如密码算法的应用、古代密码的解析以及求逆的编程实验问题。这些问题允许他们随机地组队挑选，然后按照各自的职责和协同完成。最终，他们会在课堂上做出详细的回顾和总结，并得到老师的评价和反馈。此种策略能够极大地激发学生的实践技巧、自我学习技巧和创新思维，同时也培育出他们的团队合作精神，并且突破了传统教学中内容的局限性，从而提升了教育效果。此外，我们还可以通过信息安全比赛、密码数学竞赛、密码技术比赛等方式，让学生真正投入到密码算法、安全芯片、电子商务政务等安全技术的实践中，提升他们的密码技术能力和全面设计能力，同时也培育他们的创新思维和团队协作精神。

（四）注重实训与考核相结合的实践效果

在教学全过程中，尽可能地将计算机密码学的理论知识和教学经验融为一体。当学生熟练掌握了计算机密码学的技能和运用，他们也需要更深入地研究和理解国内有关计算机密码学的相关资料，包括计算机、互联网、密码等领域的法律条例，以此提升他们对中国的文化和理论的理解，并进一步提高他们的国家认同感。在此过程中，我们需要不断加深对学生的道德教育，提升他们的网络保护认知。尽可能地为学生提供积极的机会去参与密码算法和编程训练。通过实施本课程的实验教学，以增强学生的能力，提升计算机辅助教育的效果，培养学生的分析、整合、概括和总结的技能。

四、结语

《计算机密码学》这门课程在一些大学的计算机科目中最近几年才被引入。由于计算机专业的教育目的以及学生的专业素质，使得这个《计算机密码学》课程的教育模式与核心内容与其他专业的课程有所区别。只有当老师根据学生的具体需求，最大限度地利用他们的专长，全力以赴地唤醒和保持他们对学习的热爱，我们才有可能获得理想的教育成果。此外，通过对课程的发掘和利用来提升学生的专业技术，例如密码算法的编程能力，这样做，无论在帮助学生深化自身的专业知识，或者提升他们的全面专业素质上，都将产生积极的影响。

[参考文献]

[1]王瑞锦,吴劲,周世杰,等.新工科背景下“信息安全系统研发”实验课程的重构[J].实验技术与管理,2020,37(09):231-235.DOI:10.16791/j.cnki.sjg.2020.09.052.

[2]张建新,郭亮,刘燕娜,等.新工科背景下测控专业特色实验室构建[J].实验技术与管理,2020,37(12):265-269.DOI:10.16791/j.cnki.sjg.2020.12.058.

[3]周振雄,麻丹丹,辛平,等.工程教育视角下地方高校人才实践能力自我成长培养模式创新[J].实验技术与管理,2021,38(02):11-15.DOI:10.16791/j.cnki.sjg.2021.02.003.

[4]胡燕,孔凡哲,陈心浩.实验项目驱动式教学促进四大关键能力的实证研究[J].实验室研究与探索,2021,40(02):191-196+203.DOI:10.19927/j.cnki.syyt.2021.02.038.

[5]李波,覃俊,帖军.新工科及人工智能背景下计算机类专业创新创业教育研究[J].实验技术与管理,2021,38(03):18-22.DOI:10.16791/j.cnki.sjg.2021.03.005.

[6]王春燕,房芳.课程思政改革在高校化学实验教学中的探索[J].实验室研究与探索,2021,40(04):217-221.DOI: 10.19927/j.cnki.syyt.2021.04.049.

作者简介：

刘小跃（1973.09-），男，汉族，湖南临湘人，博士，韩山师范学院，计算机与信息工程学院，副教授，研究方向：信息安全，密码学，高等教育。

李旅军（1982.08—）男，汉族，湖南郴州人，博士，韩山师范学院，计算机与信息工程学院，副教授，研究方向：量子计算与量子信息，计算机软件与理论。

基金项目：

本文系韩山师范学院教学质量工程项目“软件工程课程群虚拟教研室”（HSJYS-XN231041）研究成果。

