面向新工科的信息安全数学基础课程教学探索*

郑培嘉 卢伟

中山大学计算机学院，广州，510006

摘 要 在疫情期间，信息安全数学基础课程的传统教学模式已无法满足新工科下培养复合技术人才的要求。针对此问题，本文以促进学生学习的主观能动性为出发点，提出理论知识和编程实践相验证的教学设计以及线下授课与线上教学相结合的教学模式。本文还提供了将此方法应用在信息安全数学基础课程的思考探索和效果分析。

关键字 新冠疫情，信息安全数学基础，新工科

Teaching Exploration of Mathematics Foundations of Information Security for Emerging Engineering

Peijia Zheng Lu Wei

Guangdong Key Laboratory of Information Security Technology
Sun Yat-Sen University
Guangzhou 510006, China
zhpj@mail.sysu.edu.cn, luwei3@mail.sysu.edu.cn

Abstract—The traditional teaching mode of the mathematics foundation of information security can no longer meet the Emerging engineering requirements for cultivating compound technical talents in the COVID-19 epidemic. To address this problem, we propose a teaching design model that combines theoretical knowledge verification with programming practice and offline lectures with online teaching. This method can effectively promote students' learning initiatives. This paper also provides an in-depth exploration and effect analysis of applying this method to the mathematics foundation of information security.

Key words—COVID-19, mathematics foundations of information security, emerging engineering;

1 引 言

随着我国 “一带一路”、“中国制造 2025 ”等重大战略的不断推进[1][2]，新经济、新产业、新技术的快速发展，对网络空间安全技术人员的能力和素质提出了更高的时代要求。网络空间已成为现代生活不可或缺的一部分。没有网络安全就没有国家安全，网络空间安全已经上升到国家安全战略的高度，成为国家安全的重要组成部分[3]。党的十八大以来，以习近平同志为总书记的党中央高度重视网络空间安全工作。

近 10 年来，网络空间安全技术发展迅速，并在国家安全、智慧城市、物联网、大数据、云计算等众多领域得到了广泛的应用。“信息安全数学基础”是网络空间安全专业（信息安全专业）一门重要的专业基础课[4][5]。课程目标是使学生理解和掌握网络空间安全学科的数论和抽象代数等基本数学理论，能用严格的数学语言对网络空间安全所涉及的数学理论进行正确的推理和证明，并能够利用计算机对大素数生成、模重复平方法、不可约多项式等重要的算法进行编程实现。通过信息安全数学基础的学习，我们可以为学生进一步学习密码学、网络安全、信息隐藏、计算机取证等后续课程以及从事网络空间安全相关技术工作奠定基础。然而，当前教学方式侧重于授课老师单向传授知识，而忽略发挥学生主观能动性。现有的单一教学模式并不适应疫情期间建设新工科的目标[6][7]，因此新的教学探索迫在眉睫。

* **基金资助**：广东省自然科学基金（2022A1515011897, 2019A1515010746）；广州市科技计划项目（202102080354）

**通信作者：卢伟教授，邮箱 luwei3@mail.sysu.edu.cn

2 课程教学现状

虽然信息安全数学基础课程经历了一段时间的发展，但是其课程的教学方法在新的形势下仍有进一步改善的空间。信息安全数学基础知识点松散、理论性强、抽象度高、难度较大，且课程课时紧。这些特点导致学生在前期难以适应本课程的学习，并经常有在课程中后期跟不上课程进度的表现[8][9][10]。具体现状分析如下：

（1） 课程知识点繁多。

与一般的数学专业课不同，信息安全数学基础涉及概率论、数论基础、计算数论、抽象代数和计算机科学等内容，难度较大，且不同环节彼此间关联不紧密，知识点比较松散。这使得学生学习起来，消化吸收的困难度较大。

（2） 教学方式缺乏多样性。

目前信息安全数学基础的大多数课堂教学仍以教师讲授内容为主。教师们往往利用投影仪播放电子课件或是传统的板书，单向灌输知识。在此过程中，学生参与课堂的活跃度较低，无法充分发挥主观能动性。而且，现有教学中并没有针对疫情下的线上教学模式做研究和预案。另外，现有课程中抽象理论与公式很多，学生对课程容易产生厌倦甚至抵触心理，学习效果不理想。

（3） 实践和衔接环节薄弱。

信息安全数学基础课程包含了大量的数学定义、定理和证明等理论知识，同时也包含了许多基于这些概念和定理的重要算法。如果前期的数学定义和概念没有掌握好，则相关的算法和后续的高阶内容就难以理解。学生在学习时，经常会陷于理解复杂的数学知识的过程中，而忽略掉自己动手写代码实现算法的实践。教师在教学过程中往往也不够学时和精力展开解释信息安全数学基础课程与后续课程的联系，这也使得学生缺乏对此课程重要性的了解，一定程度上也降低了学生学习的积极性。

（4） 疫情期间多渠道教学预案不足。

在现今疫情的新形势下，经常会面临着线上线下课程交替进行的挑战。大多数线上课程的教学是以多媒体电子课件（如幻灯片）播放辅助以背景旁白的形式进行。事实上，这些幻灯片是针对线下教学而准备的，并未针对线上教学做特别的优化设计。而且，单单只是背景旁白会让学生上课时感觉到更加单调，缺乏学习兴趣，容易走神。由于线上教学时教师很难观察到学生的反应，感受到学生对授课内容的接受程度，因此很难做出有效的师生互动。

上述问题让疫情期间信息安全数学基础课程的教学质量受到了很大的影响。面向新工科的高水平创新人才需求，迫切需要教师针对信息安全数学基础课程教学设计和教学模式等方面做出新的探索，以便充分发挥学生的主观能动性，提高学习效率，为培养出高质量的网络空间安全人才打下牢固的基础。

3 理论实践相验证教学设计

信息安全数学基础是一门需要理论学习与编程实践相互印证结合的课程，不仅要求学生学习信息安全数学与理论基础，还要求学生能熟悉利用计算机完成基础算法的实现，为后续网络空间安全相关课程的学习作铺垫。针对新工科下对网络空间安全专业学生的要求，我们要设计合理高效的教学计划，使学生理解与掌握信息安全数学基础的基本概念和理论，同时培养学生使用不同编程语言实现信息安全相关重要算法的技能，并锻炼学生解决信息安全工程实际问题的能力[11]。

笔者讲授的信息安全数学基础课程内容主要由两部分构成，即数论基础和抽象代数。这两部分的内容的数学基础有较强的逻辑性和抽象性，学习曲线比较陡峭。因此，在教学过程中，教师需要与学生充分沟通以了解其数学分析、线性代数、概率论等前期数学专业课的学习基础，并在授课期间有针对性的帮助学生回忆关键概念和定理。信息安全数学基础课程中的部分内容与密码算法的实现联系紧密，教师在讲授课程的同时应引入信息安全数学基础在密码学、网络安全、信息隐藏等相关网络空间安全课程中的应用实例，解释这些知识点与后继课程知识点的联系及重要性。单纯理论知识讲授会让学生难以透彻理解信息安全数学基础的知识，教师应指导学生动手编程实现部分实践性较强的算法，加深学生对算法实现及其数学原理的理解。总体教学设计框架路线见图 1。

（1） 数论基础。

对于简单且在之前数学专业课出现过的概念和定义，如集合、映射、函数等，教师可结合实际情况快速带过。对于较难理解的概念和定理，如中国剩余定理、欧拉定理、平方剩余、原根等,教师要重点解释和讲解，充分利用多种学科下的实例，用浅显易懂的例子让学生对这些抽象概念有形象化的认识。务必让学生熟练掌握数学公式的推导、透彻理解重点算法的数学原理，可以辅助举例讲解简单的密码算法来帮助学生理解这些抽象知识在密码学课程中的实际应用。而对于扩展的 Euclid 算法、模重复平方算法、二次剩余的判断和计算、素性检测等重要的信息安全算法，教师应当指导学生使用 C 语言、Python 语言、或 Mathematica 等多种语言实现编程，让学生充分掌握同一算法在不同编程语言下实现时应掌握的技巧，也了解不同编程语言下应具有的思维方式，并熟悉其不同实现的优缺点，从而更加深入了解算法的实现过程，并与相关数学理论进行相互验证，提升对这些抽象知识的认知程度。

（2） 抽象代数。

抽象代数主要研究对象是代数结构，包括了群、环、域、Galois 理论等内容。这部分内容是信息安全数学基础课程的核心，但其逻辑性强、抽象度高的特点也使其成为学习的难点。教师应强化对数学概念的解释和数学定理的证明，如正规子群、商群、环同态、

域的扩张等，着重培养学生的数学思维和逻辑能力，并积极地询问学生的接受情况。在讲授的同时应当引入其他网络空间安全课程的实例来拓展学生的思维，为学生今后学习相关知识以及了解学科前沿打下基础。对于循环群、多项式环、有限域等可编程实践的内容，教师也可指导学生用多种编程语言实现，以加深对这些知识的掌握程度。学生在编程过程中可以参考互联网上的文献资料或参考代码，但最终需要以自己的方式实现，提交详细的实验报告，并给出相关实验过程以及说明与哪些数学概念有关。这种理论与实践相互验证的方式既强化学生对所学数学概念的理解和推导能力，又锻炼了学生的自主学习能力和编程实践的应用能力。

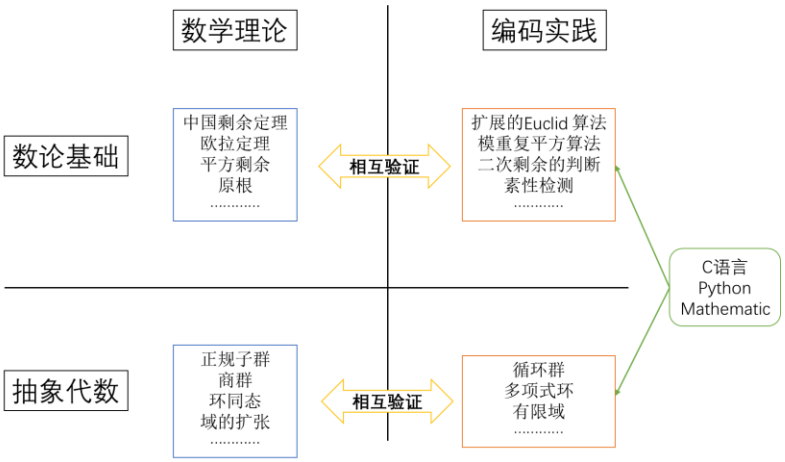

图 1　理论实践相验证教学设计框架

4　线上线下相结合教学模式

目前线下教学大多以多媒体教学为依托，再辅助以板书的形式进行。但多媒体课件包含的教学信息量偏多，使得学生无法定位重点内容，增加了消化理解的难度[12-14]。教师应该要根据听课学生的反应，实时地进行授课语气、内容的调整，降低学生课堂倦怠感，提升其注意力集中度。疫情期间，部分课时转为在线上进行。

线上教学不能把线下的教学方式都生搬硬套到线上进行，应该要根据线上教学的特点作灵活地适配。线上教学时，教师很难准确地观察到学生的听课反应，故不能做到及时且积极的反馈。因此，教师要力争做到线上网络授课与线下课堂教学有等质的教学质量。除此之外，教师还要做好线下到线上，以及线上回到线下教学的前后衔接。这样可以使得学生不会在学习信息安全数学基础课程时，因为线上线下教学的交替进行而产生困惑和不适应感。总体教学模式框架见图2。

（1） 线下课堂教学。

教师课前做好详细备课工作，对课程知识体系烂熟于心。在授课时教师要条理清晰地表达授课内容，讲述重点与难点问题，引领学生跟随课程进度，讲解重要习题，梳理编程思路，引导学生解决编程实践问题，激发学生的学习兴趣和热情。还要及时注意学生的听课反应，适时给出有趣生动的示例，吸引学生的注意力，并根据学生提出的问题，做进一步的示例解释，或者根据学生的需要再讲解一次难点内容。

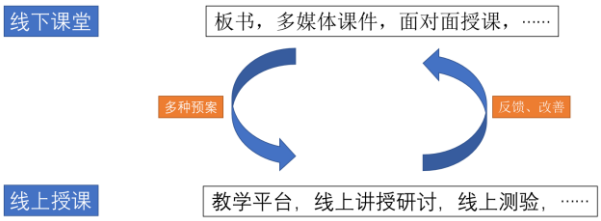

图 2　线上线下相结合教学模式

（2） 线上网络授课。

教师需要充分利用多媒体资源，根据不同教学知识点录制电子课件、视频动画等多样化内容。在授课时，教师要以饱满的精神状态进行线上授课，注意做到授课话速适中。授课中间需要询问网络语音是否通畅和课件播放是否同步。线上教学是在教师和学生教学空间分离的情况下实现的，学生需要长时间对着显示屏。

为了引导学生将注意力集中在课堂上，教师要适时的提出问题引导学生在课堂中发言交流，并根据学

生的回答，给予鼓励和赞赏。这样可以有效地让学生主动加入课堂教学中，从被动的听课者的身份转变成课堂教学的积极参与者。

（3） 线下线下交替。

疫情期间，可能会因紧急疫情导致从线下转到线上授课。教师应该做好预案，从多渠道的在线授课平台中选择出最合适的，如腾讯会议、腾讯课堂、钉钉平台、超星学习通平台等。

为了避免由于网络问题而导致的拥堵、卡顿现象对线上授课的影响，教师可以提前把资料发给学生。为了解决声音不同步，视频不能播放等问题，还可以在课后将线上授课的过程转成视频，供学生再观看复习。当从线上恢复到线下正常教学时，教师可以通过课程小测试，了解学生线上学习的状态和成效，并解答学生疑问。此外，还可以通过适当的设计教学问卷收集学生课后反馈，从而能及时根据建议做相应调整，改善学生听课和学习质量。

5 教学效果分析

笔者自 2019 年来在从事信息安全数学基础这门课的教学工作。经过连续 4 年的探索和实践，信息安全数学基础的教学质量有了明显提高。

（1） 学生学习的主观能性得到强化。

线上线下相结合的教学模式使得学生可以从多种信息渠道学习信息安全数学的知识，从关注授课的形式转变成注重授课内容。授课模式的灵活性激发了学生主动学习的能动性，学生更能感受到自己是学习的主体这一道理，从而更能充分地发挥自己的主观学习意愿。从连续 4 年的信息安全数学基础的教学感受来看，上课时课堂气氛逐年地活跃起来，学生们更加愿意与老师交流，学习动力更强。

（2） 学生的学习效果得到有效提高。

理论实践相验证的教学设计，使得学生在课堂学习到理论定义、定理和算法之后，还能及时地通过项目方案设计、编程实现等实践环节印证这些理论知识，建立起理论和实践的联系，从而将老师教授的课程内容内化成自己的知识。

在信息安全数学基础课程结课后，有许多同学参与了全国网络安全挑战赛、广东大学生网络安全攻防大赛等竞赛，并获得了一系列奖励。由于对信息安全数学知识的良好掌握，学生们更加坚定了做好网络空间安全研究的信心。有多名学生本科毕业后，保研或考研到网络空间安全等相关专业继续深造。

6 结束语

新工科建设为网络空间安全人才培养起提供了新的推动力，疫情期间的线上线下教学给高校教师带来了新的挑战和要求，因此探索新形势下信息安全数学基础的教学非常有意义。笔者从连续多年的信息安全数学基础授课实践出发，提出了理论实践相验证的教学设计和线上线下相结合的教学模式。这些探索思考有望充分发挥学生的主观能动性，综合多种有效的教学工具，提升学生学习信息安全数学基础的效率。

参 考 文 献

[1] 卢晶琦,邓春健,师向群,等.新工科视域下的电子信息创新人才培养实践[J].实验技术与管理， 2020,37(5):156-159.

[2] 于秀娟.新工科背景下高校研究生科研创新能力提升策略研究[J].教育教学论坛， 2020(14):111-113.

[3] 赵瑞琦.中国网络安全战略:基于总体国家安全观的特色建构[J].学习与探索,2019(12):57-65.

[4] 郎荣玲,刘建伟,金天.信息安全数学基础理论教学方法研究[J].计算机教育,2012(17):33-35.

[5] 汪楚娇,张艳群.基于抽象代数的“信息安全数学基础”教学模式研究[J].教育现代化,2019,6(34):159-160.

[6] 林健.面向未来的中国新工科建设[J].清华大学教育研究,2017， 38(2):26-35.

[7] 董奇颖,高敏芬,贾春福.“讲一练二考三”在信息安全数学基础中的实践[J].计算机教育,2017,(12):59-62.

[8] 牛淑芬,于斐,杨平平,方丽芝.交叉学科背景下信息安全数学基础理论与实践教学方法研究[J].计算机教育,2021,(02):149-152.

[9] 贾春福,李瑞琪,高敏芬.任务驱动法在信息安全数学基础教学中的应用[J].计算机教育,2022,(03):85-88+93.

[10] 周潭平,潘峰,张薇,刘文超.密码学课程中分离数学思维与密码思维教学方法探讨[J].计算机教育,2022,(03):49-52.

[11] 凌志刚,温和,李华丽.面向新工科的数字图像处理课程线上线下一体化教学改革[J].计算机教育,2022,(03):139-142.

[12] 彭鑫,瞿述,谢文武,朱鹏.疫情防控期间线上教学的混合式实现途径[J].计算机教育,2021,(02):44-48.

[13] 姜延,张巨俭,陈春丽.疫情期间高校线上教学三部曲——以数据库基础课程的教学组织为例[J].计算机教育,2020,(08):37-41.

[14] 吕美香,董永强,洪小丽,黄晓菁.疫情时期高校在线教学管理实践与思考[J].计算机教育,2021,(03):20.