文章编号：1672-5913(2021)02-0149-04
中图分类号：G642

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

牛淑芬，于　斐，杨平平，方丽芝
（西北师范大学 计算机科学与工程学院，甘肃 兰州 730070）

摘　要：针对信息安全数学基础课程教学存在的问题，结合本科生网络安全专业课程设置特点、创新人才培养需求以及交叉学科课程建设需求，提出将传统的教学手段与现代化教学方法、教学手段相结合，将数学理论教学、计算机编程能力和密码算法应用能力相结合，探讨信息安全数学基础课程的新型教学方法。

关键词：教学方法；信息安全数学基础；交叉学科
DOI:10.16512/j.cnki.jsjjy.2021.02.035

1　研究背景

随着信息技术的高速发展，人们对信息安全的关注越来越深入。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安全和信息化工作。习近平在中央网络安全和信息化领导小组第一次会议上强调，网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题 [1]。信息安全的概念在 20 世纪提出后历经了漫长的发展，20 世纪末才被人们深入研究。我国为了发展信息技术产业，在 21 世纪初先后于高校和科研院所的计算机与软件学院、信息科学学院、数学学院等院系设立信息安全专业，至今已有 100 多所高校开设信息安全专业，众多高校设立信息安全方向 [2]。经过长时间的探索和发展，信息安全的内涵及教育培养模式逐步成熟。信息安全作为一门交叉性学科，具有很强的综合性，其涉及诸多学科，如数学、密码学、计算机科学、信息学等，其目的是保障信息在存储和传输过程中的保密性、完整性、不可否认性等特性 [3]。信息安全数学基础以密码学为核心内容，建立在数学理论的基础之上并且涉及到多个数学分支 [4]，该课程也是一门应用背景比较强的信息安全专业的数学基础课程。

2　课程现状

作为一门新兴的课程，信息安全数学基础在学生培养过程中具有重要地位，研究密码学时以该课程作为数学基础，信息安全专业以该课程作为核心课程。信息安全数学基础课程具有同一般数学课程的理论性，同时具有与信息安全相关的实践性，为计算机编程和密码学中算法的实现提供理论依据，更接近于实际应用，解决现实问题。众所周知，理工类的学习和研究都需要一定的数学知识作支撑，因此信息安全数学基础课程对信息安全专业学生的今后学习具有基础性作用。由于信息安全数学基础课程课时紧、内容多、难度较大并且课程知识点松散，因此学生不容易接受 [5]。虽然信息安全数学基础课程经历了一段时间的发展，但是课程的教学方法仍有不足之处 [6]。

1）教学方式缺乏多样性。

大多数教师在教授信息安全数学基础课程的教学方式同一般数学课程的教学方式一样，往往以教师在课堂讲授为主。授课手段比较单一，一

基金项目：国家自然科学基金项目 (61562077, 61662069, 61662071, 61772022) 。
第一作者简介：牛淑芬，女，副教授，研究方向为密码学、云计算、大数据网络的隐私保护，sfniu76@ nwnu.edu.cn。

般都是传统的板书，或利用多媒体工具 PPT 放映，授课手段缺乏多样性和创新性。学生在这种满堂灌输的教学方式中处于被动地位，无法提高学习兴趣，调动积极性 [7]，其结果就是学生对课程产生厌倦甚至抵触心理，显然不会有良好的教学结果。

2）教学设计上缺少与密码学课程以及计算机编程的结合。

虽然信息安全数学基础的课程内容都是一些定义、定理等理论知识，但是学习该课程的目的不仅仅是了解理论知识，更重要的是能够利用其中的理论解决信息安全领域的问题 [8-9]。现实情况是学生在学习该课程时仅仅学到了课程的理论知识，却没能够利用其中的理论作为密码学的算法和计算机编程的依据来解决实际问题。对于信息安全专业的学生，这也就失去了学习的意义。

上述问题的存在大大影响了信息安全数学基础课程的教学质量。因此，在交叉学科的背景下，如何改善教学方法培养出满足当下需求的信息安全人才，值得探讨。

3 理论与实践结合的教学方法探讨

根据信息安全数据基础课程的特点，从数学理论学习到学生编程能力锻炼，再到实践教学的教学方法，教学设计将沿着“数学理论教学设计—基本编程能力教学设计—实践教学设计”的总体路线，总体教学设计路线见图 1。

总体教学设计采取从理论学习到实践教学的路线，层层递进。教学设计环节各有特点，各有明确的培养目的。在“数学理论教学设计”的环节中，要求教师在课堂上精简核心内容和重点内容，注意重难点突出，详略得当。在课堂教学中，教师作为知识引导者和梳理者，学生作为学习主导者，充分发挥学生的积极性和主观能动性，提升学生自主学习的能力。在“基本编程能力教学设计”的环节中，挑选几个本课程代表性的算法，让学生用 C 语言编程实现算法。学生自主完成教师布置的实验教学内容，鼓励各式各样的讨论形式，创造轻松的学习氛围。在整个过程中，教师可进行适当引导，并把握学习讨论进度。在“实践教学设计”的环节中，采用任课教师、硕士研究生和本科生组成的课题小组，每组 12 人（每组配一名教师和一名硕士研究生），教师负责教授密码算法设计，研究生作为助教指导编程设计，本科生作为主体实现编程。

3.1 数学理论教学设计

信息安全数学基础课程内容主要有 3 部分构成，分别是数论基础、代数学基础和椭圆曲线理论 [10]。其中数论基础、代数学基础有较强的逻辑性和抽象性，具有一定的学习难度，因此需要学生在前期的高等数学、线性代数、概率论以及离散数学学习基础上，进行理论分析学习。

（1）对于数论部分，让学生熟练掌握公式的推导、透彻理解算法的数学原理，通过举例讲解简单的密码算法来理解其在密码学课程中的实际应用。

（2）对于代数学部分，其作为信息安全数学基础课程的核心，应强化对数学概念的理解和数学定理的证明，着重培养学生的数学思维和逻辑能力。

（3）对于椭圆曲线理论部分，首先结合椭圆曲线上的公钥密码算法进行讲解，其次在讲授的同时引入其他信息安全课程的实例来拓展学生的思维，加强其对算法的理解，点明此课程与后续网络安全课程的关系及课程地位，为学生今后学习相关知识以及了解学科前沿打下基础。因此，这部分内容的学习首先要强化学生的计算力和推导能力。

3.2 基本编程能力教学设计

信息安全数学基础课程中的部分内容与密码学中密码算法的实现联系紧密，单纯理论知识的讲解会让学生感到枯燥。对实践性较强的内容设置实验环节，让学生通过动手操作或编程实现，加深对具体算法及其数学原理的理解。因此，在授课中开设部分简单实验，具体实验内容见表 1。在这部分的教学环节中，由于所列算法数学推理比较简单，学生可用学过的 C 语言编程实现算法。表 1 中的前 3 个实验可由学生独立完成，以提交作业的形式上交，教师批阅讲解，优化算法的代码。第 4 个实验是中国剩余定理，这是一个综合性实验，编程实现稍有难度，可由 6 名学生组成小组共同完成。学生在编程过程中可以参考各类文献资料或部分源代码，但必须通过消化整

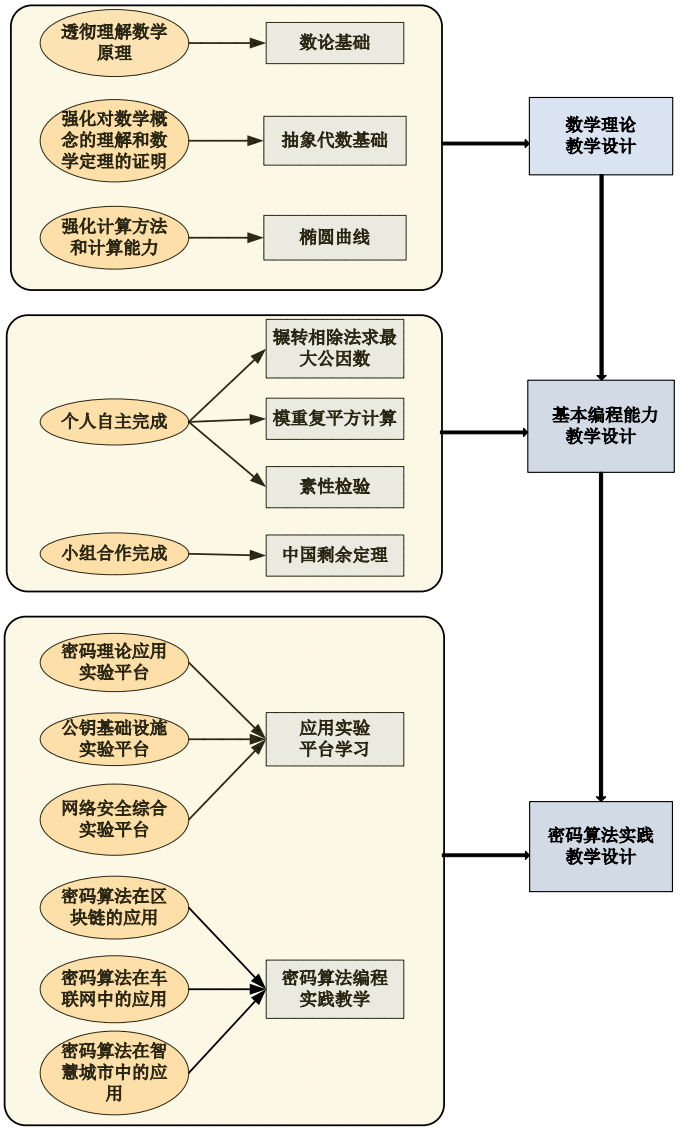

图 1　总体教学设计路线图

合，最终提供完整的加解密界面。对于小组共同完成的实验，需要通过答辩的形式来对学生的实验效果进行验收。这种实验方式既加深了学生对所学数学知识的理解，又锻炼了学生的自主学习能力和知识的综合应用能力。

3.3　实践教学设计

表 1　课程实验

知识点	实验设置
辗转相除法求最大公因数	编程求解 s，t，使得 $sa+tb=(a,\ b)$
模重复平方计算	编程实现模幂运算 $bm\ (\mathrm{mod}n)$
素性检验	编程实现 Miller–Rabin 素性检验算法
中国剩余定理	编程实现 Rabin 公钥算法

1）利用开发完善的实验平台学习。

利用现有的教学平台，在教师指导下完成实验。实验内容主要是以信息安全的理论为基础，以现有的网络安全教学平台为依托，让学生了解和理解 TCP/IP、防火墙、IDS、IPSec、计算机病毒、漏洞检测等基本的网络安全知识。主要实验平台有密码理论应用实验平台、公钥基础设施实验平台以及网络安全综合实验平台。在此部分的教学中，密码理论应用实验平台重在让学生了解经典的加解密算法；公钥基础设施实验平台和网络安全综合实验平台旨在让学生初步了解密码算法的实验环境和实际应用背景。

2）密码算法编程实践教学。

针对网络中的数据安全问题和具体的应用环境，根据实际问题的数据安全需求，提出密码算法进而通过编程实现算法，最后在仿真平台上或者通过数值模拟完成测试。

在算法网络背景环境的选用上，根据课题组教师的现阶段的科学研究项目，选择 3 个方向：电子病历数据共享加密算法、车联网身份认证算法和智慧城市中数据隐私加密算法。具体算法研究见表 2。这部分的教学重在于培养学生提出问题和解决问题的能力。在任课教师的指导下分析网络环境中数据的安全性需求，设计相应的密码算法。例如在电子病历中，为了实现对密文数据的搜索和对数据解密共享，设计基于可搜索加密和代理重加密的电子病历数据共享算法，同时可将前沿的区块链技术引入算法设计。

在算法编程实践教学的设计环节中，培养学生用 C 语言和密码学 PBC(Pairing-Based Cryptography) 双线性对包 [11] 编写较为复杂的密码学程序。经过专业课的学习，学生对 C 语言比较熟悉。针对较为复杂的密码算法，结合 C 语言和 PBC 双线性对包进行编程。表 3 是 PBC 双线性对包的一个参数案例。群 G_1、G_2 的长度为 1 024 位，利用 a 型椭圆曲线 $y^2=x^3+x\mathrm{mod}q$。实验环境配置见表 4。在编程实践环节，由 1 名研究生和 10 名本科生组成一个教学团队（创新团队）研究学习，部分研究成果可考虑在国内学术期刊发表，进而培养学生的科学研究能力。

实践教学环节通过循序渐进的学习过程开展。教学平台实验教学比较直观，容易激起学生的学习兴趣；利用计算机语言编程解决针对目前热门方向中数据安全问题，可以让学生将所学的理论知识应用到解决实际问题中，可以培养学生对知识的应用能力，在交叉学科背景下的学生，能够将其所学理论直接用于实践，对于学生未来的学业发展尤其重要。

表 2　密码算法编程实践教学表

算法网络背景环境	算法类型
电子病历数据共享加密算法	可搜索加密算法、代理重加密算法
车联网身份认证算法	聚合签名算法
智慧城市数据隐私加密算法	签密算法

表 3　参数的主要性质 [11]

参数类型	基域 (bit)	Dlog 安全 (bit)	椭圆曲线次数
Type a	512	1 024	2

表 4　环境配置参数

电脑型号	CPU	内存	操作系统	虚拟机
ASUS A455L	Inter(R) Core(TM)i5-4210U	4.00G	Win10	Linux

4　结　语

针对现阶段信息安全数学基础课程教学方式的不足提出的教学方式具有两大创新点：一是将数学算法理论的学习与计算机编程紧密结合起来，锻炼学生的逻辑推理能力、自主学习能力和知识综合应用能力；二是将本课程的学习和密码学知识结合起来，提出具体的密码算法，解决区块链、智慧城市和车联网中的数据安全问题，培养学生的实践创新能力。在今后的教学过程中，还要不断统计分析教学状况，根据实际情况调整优化教学方式，进一步提高教学质量。

参考文献：

[1] 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.
[2] 朱潜, 李昕, 徐剑, 等. 信息安全数学基础新型教学方法研究[J]. 计算机教育, 2014(1): 43-46.
[3] 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.
[4] 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.
[5] 秦艳琳, 吴晓平. “信息安全数学基础”案例教学[J]. 计算机教育, 2010(1): 141-144，137.
[6] 余琍, 付杰, 黄传河. 信息安全专业人才培养模式创新思路与实践教学改革[J]. 计算机教育, 2007(22): 151-153.
[7] 赵焕平, 古凯, 刘艳. 创新人才模式下信息安全数学基础课程教学改革与探索[J]. 电脑知识与技术, 2020, 16(6): 38-40.
[8] 潘世英, 马海滨. 基于能力培养的计算机技术专业实践教学改革研究[J]. 教育现代化, 2019, 6(43): 50-51，53.
[9] 方芳, 方洋. 信息安全专业人才需求: 基于互联网招聘市场的分析[J]. 教育现代化, 2019, 6(24): 236-239.
[10] 陈恭亮. 信息安全数学基础[M]. 2版. 北京: 清华大学出版社 , 2014: 58, 108, 198.
[11] Stanford. PBC Library-Pairing-Baesd cryptography [EB/OL]. (2015-03-16)[2020-05-06]. http: //crypto. stanford. edu/pbc/ .

（编辑：孙怡铭）

（上接第143页）

示出了在线上教学中的有效性。在今后的教学中必然是线上教学和线下教学的深度互动与融合，这些行之有效的方法，在将来的线上线下相结合的教学中必然也能发挥重要作用。

参考文献：

[1] 郑勤华, 秦婷, 等.疫情期间在线教学实施现状、问题与对策建议[J].中国电化教育, 2020(5):34-43.
[2] 叶崇凉.疫情下线上教学面临的挑战与对策[J].计算机教育, 2020(5):22-24.
[3] 刘润清, 赵荣棵.新冠疫情期间线上教学模式的适用性分析[J].中国多媒体与网络教学学报(上旬刊), 2020(7):50-52.
[4] 郭静.“互联网+教育”视域下网络传播课程线上教学探索与反思[J].新闻研究导刊, 2020, 11(13):30-31.
[5] 陆鑫, 张凤荔, 汤羽.以学生为中心的课程混合式教学模式研究与实践[J].计算机教育, 2020(5):147-151.

（编辑：孙怡铭）