密码专硕驱动下高等代数课程的教学改革探索

高艳艳，张康群
南京工程学院 数理学院，江苏 南京 211167
DOI: 10.61369/ETR.2025500033

摘　　要： 随着国务院学位委员会和教育部批准设立密码专业学位，高层次密码应用型人才的培养得到了高度重视。本科阶段的高等代数课程作为重要的基础课程，对于密码专业硕士研究生的培养起着关键的支撑作用。然而，当前该课程在教学内容、教学方法、课程衔接等方面存在与密码专硕需求脱节的问题。本文旨在深入剖析这些问题，并从优化教学内容、创新教学方法、完善课程衔接等多个维度提出针对性的改革探索，以实现高等代数本科课程与密码专硕需求的有效对接，提升密码专业人才培养质量。

关 键 词： 密码专硕；高等代数；教学改革；案例教学

Exploration on the Teaching Reform of Advanced Algebra Course Driven by Master of Cryptography Specialty

Gao Yanyan, Zhang Kangqun
School of Mathematics and Physics, Nanjing Institute of Technology, Nanjing, Jiangsu 211167

Abstract: With the approval of the Academic Degrees Committee of the State Council and the Ministry of Education for the establishment of the professional degree in cryptography, great attention has been paid to the cultivation of high-level applied cryptography talents. As an important basic course at the undergraduate level, the Advanced Algebra course plays a key supporting role in the cultivation of postgraduates majoring in cryptography. However, there are problems in the current course, such as disconnection from the needs of the Master of Cryptography Specialty in terms of teaching content, teaching methods, and curriculum connection. This paper aims to deeply analyze these problems and propose targeted reform explorations from multiple dimensions, including optimizing teaching content, innovating teaching methods, and improving curriculum connection. The purpose is to realize the effective connection between the undergraduate Advanced Algebra course and the needs of the Master of Cryptography Specialty, and enhance the quality of cryptography talent cultivation.

Keywords: master of cryptography specialty; advanced algebra; teaching reform; case teaching

网络与信息安全是国家安全的基石，而密码是保障网络与信息安全的核心技术和基础支撑，是国家重要的战略资源。2022年第2期《求是》杂志刊发习近平总书记重要文章《不断做强做优做大我国数字经济》，明确指出将发展数字经济上升为国家战略。随着信息技术的飞速发展，密码技术的应用领域不断拓展，对高层次密码应用型人才的需求也日益迫切。为了满足这一需求，国务院学位委员会和教育部于2022年印发通知，从2023年起在交叉门类设立密码专业学位。

高等代数作为一门重要的数学基础课程，为密码学的学习和研究提供了不可或缺的工具和方法。在本科阶段扎实掌握高等代数的知识和技能，对于学生后续攻读密码专业硕士学位以及从事密码相关工作具有深远的影响。然而，目前本科高等代数课程的教学现状不容乐观，存在诸多与密码专硕需求不匹配的问题。因此，探索面向密码专硕需求的高等代数本科课程教学改革路径具有重要的现实意义。

一、高等代数课程对密码专硕的重要性

（一）密码学中的代数基础

在密码学领域，许多核心算法和理论都深深扎根于代数学的知识体系。例如，希尔密码（Hill Cipher）就是运用基本矩阵运算的替换密码。希尔加密算法的基本思想是，将d个明文字母通过线性变换将它们转换为d个密文字母，而解密只要作一次逆变换就可以了，密钥就是变换矩阵本身。又如，在现代密码学中广泛应用的公钥密码体制，如RSA算法，其安全性基于数论中的大整数分解难题以及模运算。而模运算与高等代数中的同余类环密切

基金项目：本文得到国家自然科学基金面上项目(No. 12271249)，南京工程学院“课程思政”示范项目(No. KCSZ2025KC60)，南京工程学院教学改革和建设项目(No. JXGG2025ZX05)，江苏省本科高校“高质量数理类课程教材改革研究”专项课题(NO. 2025SL004)的支持。
作者简介：
高艳艳(1983—)，女，汉族，山西晋中人，博士，南京工程学院教授。主要从事编码密码理论、群代数研究。
张康群(1981—)，男，汉族，山东莒南人，博士，南京工程学院教授。主要从事数学教育、偏微分方程研究。

相关，同余类环的结构和性质为理解和分析 RSA 算法提供了坚实的理论基础。

（二）代数方法在密码算法设计与分析中的应用

高等代数中的矩阵理论在密码算法设计与分析中发挥着关键作用。以分组密码中的 AES 算法为例，该算法的轮变换过程中包含了字节代换、行移位、列混淆和轮密钥加等操作。其中，列混淆操作通过一个固定的可逆矩阵与状态矩阵相乘来实现，这一过程充分利用了矩阵乘法的运算规则和矩阵的可逆性。通过对矩阵运算的精确运用，AES 算法能够有效地混淆明文信息，增加密码分析的难度。在密码分析中，利用矩阵的特征值和特征向量等概念，可以对某些密码算法的安全性进行评估。例如，通过分析密码算法对应的矩阵的特征值分布情况，可以判断该算法是否容易受到特定类型的攻击。

（三）培养学生逻辑思维与问题解决能力

学习高等代数课程对于培养密码专硕学生的逻辑思维和问题解决能力具有不可替代的作用。高等代数课程具有高度的抽象性和严密的逻辑性，学生在学习过程中需要从具体的数学对象中抽象出一般的概念和性质，并通过严格的逻辑推理来证明定理和结论。这种思维训练有助于学生形成严谨的思维方式，使其在面对复杂的密码学问题时，能够迅速理清思路，运用所学知识进行深入分析。当学生遇到一个新的密码算法需要分析其安全性时，他们可以运用在高等代数学习中培养的逻辑思维能力，从算法的基本原理出发，逐步推导和验证其安全性属性。高等代数课程中的各种问题求解过程，如线性方程组的求解、矩阵的运算等，也为学生提供了丰富的实践机会，锻炼了他们运用数学方法解决实际问题的能力。

二、当前高等代数课程教学现状及问题

（一）教学内容与密码专硕需求脱节

目前，高等代数课程的教学内容主要围绕多项式理论、行列式、矩阵、线性方程组、线性空间、线性变换等展开，虽然这些内容是高等代数的基础，但在教学过程中，往往缺乏与密码相关实际应用的紧密结合[1]。例如，在讲解矩阵理论时，通常侧重于矩阵的基本运算、性质以及常见的矩阵分解方法，而对于矩阵在密码算法中的具体应用，可以给学生提供分组密码中的列混淆操作、公钥密码体制中的密钥生成等方面的应用。这种脱节导致学生在学习过程中难以理解高等代数知识与密码学之间的内在联系，无法将所学的代数知识有效地应用到密码专业的学习和研究中。

（二）教学方法单一

在高等代数课程的教学中，传统的讲授式教学方法仍然占据主导地位[2]。教师在课堂上主要以讲解理论知识和推导证明为主，学生被动地接受知识，缺乏主动参与和思考的机会。这种单一的教学方法使得课堂氛围沉闷，学生的学习积极性不高。而且，由于高等代数课程内容抽象，对于一些基础薄弱的学生来说，单纯的讲授式教学很难让他们理解和掌握知识点，容易导致学生对课程产生畏难情绪。在讲解线性空间的概念时，教师如果只是从抽象的定义出发进行讲解，学生很难直观地理解线性空间的本质特征，也难以将其与实际问题联系起来。

（三）与密码专硕课程缺乏有效衔接

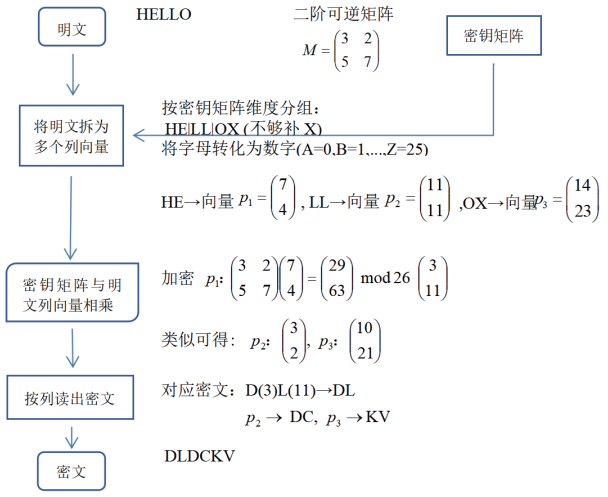
在课程体系设置上，高等代数课程与后续的密码专硕课程之间缺乏明确的衔接规划。2025年我校首次招生密码专硕的学生，因此本科阶段的教学没有充分考虑到为密码专硕课程打下坚实基础的重要性，会导致学生在进入密码专硕阶段学习时，发现本科所学的高等代数知识无法很好地满足密码需求。学生在学习这些密码专硕课程时会遇到较大的困难，需要花费大量的时间和精力来补充和巩固相关的代数知识。这种课程衔接不畅的问题不仅影响了学生的学习效果，也制约了密码专业人才培养的质量和效率。

三、面向密码专硕需求的教学改革策略

（一）优化教学内容

1. 融入密码学应用案例

在高等代数课程教学内容的设计中，可多次融入与密码学紧密相关的应用案例[3,4]。在讲解矩阵乘法时，可以引入 Hill 密码的加密和解密过程作为案例。Hill 密码是一种多字母替换密码，它通过将明文字母分组，并与一个密钥矩阵进行矩阵乘法运算来实现加密。通过这个案例，学生不仅可以深入理解矩阵乘法的运算规则，还能直观地看到矩阵在密码加密中的具体应用。下面通过加密的具体的例子（图1）来说明：



通过这些具体的应用案例，能够使抽象的高等代数知识变得更加生动形象，激发学生的学习兴趣，同时也帮助学生建立起高等代数与密码学之间的桥梁，让他们明白所学知识在实际中的应用价值。

2. 适当调整教学内容

根据密码专硕的需求，对高等代数课程的教学内容侧重点进行合理调整。在传统教学中，行列式和线性方程组的求解往往占据较大比重。虽然这些内容仍然重要，但是可以适当减少一些复杂行列式计算技巧的讲解，转而增加一些与密码相关的代数内容

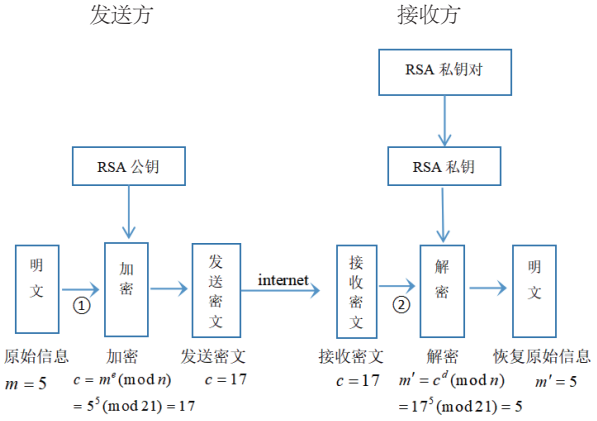
的深度和广度。在讲解矩阵理论时，除了基本的矩阵运算和性质外，可适当加强对矩阵的特征值、特征向量以及矩阵分解在密码学中的应用讲解。在密码分析中，通过分析密码算法对应的矩阵的特征值和特征向量，可以评估算法的安全性；在密码算法设计中，矩阵分解技术如奇异值分解可以用于数据加密和压缩。通过调整教学内容侧重点，使学生能够更有针对性地学习高等代数知识，更好地满足密码专硕学习和未来从事密码相关工作的需求。

（二）创新教学方法

1. 结合项目式教学

项目式教学是一种以学生为中心的教学方法，通过让学生完成一个具体的项目来学习和应用知识。在高等代数课程中，可以设计一些与密码学相关的项目。要求学生利用所学的高等代数知识，练习经典的密码算法（图2所示）[5,6]，并对其安全性进行分析。学生在完成项目的过程中，需要综合运用矩阵运算、线性变换等知识，学生可能会遇到各种问题，如算法效率低下、安全性漏洞等，这就促使他们主动查阅资料、与同学讨论，寻求解决方案。通过这种方式，不仅能够提高学生对高等代数知识的掌握程度和应用能力，还能培养他们的创新思维和团队协作能力，这些能力对于密码专业人才来说都是至关重要的。

RSA 算法实现流程



①选择 $p=3,q=7,n=pq=21,\phi(n)=(p-1)(q-1)=12$，选加密密钥 e=5

②求解密密钥 $ed\equiv 1(\mathrm{mod}\,\phi(n)),5d\equiv 1(\mathrm{mod}\,12),d=5$

图2

2. 利用多媒体与在线教学资源

充分利用多媒体和在线教学资源，丰富教学手段，提高教学效果。在多媒体教学方面，可以制作精美的动画演示，将抽象的高等代数概念直观地展示给学生。在讲解线性空间的基变换和坐标变换时，可以通过动画演示向量在不同基下的坐标变化过程，让学生更清晰地理解这一抽象概念。利用视频资源展示高等代数在密码学中的实际应用案例，如介绍一些密码算法的实现过程和应用场景。还可以借助在线教学平台，如中国大学 MOOC、学堂在线等，引入相关的优质在线课程作为辅助教学资源，有助于学生进行预习和复习等。

3. 开展小组合作学习

小组合作学习是一种有效的教学方法，能够促进学生之间的交流与合作，培养学生的团队精神和沟通能力。在高等代数课程教学中，可以将学生分成小组，针对一些复杂的问题进行合作学习。在讲解矩阵的特征值和特征向量在密码分析中的应用时，可以布置小组任务，让学生分析不同密码算法中矩阵的特征值和特征向量与算法安全性之间的关系。小组成员需要分工协作，有的负责查阅相关文献资料，了解不同密码算法的原理；有的负责计算矩阵的特征值和特征向量；有的负责分析计算结果，并撰写小组报告。在小组合作过程中，学生们可以相互学习、相互启发，共同解决问题。通过小组合作学习，学生不仅能够更好地掌握高等代数知识，还能提高团队协作能力和解决实际问题的能力。

（三）加强课程衔接

适当加强高等代数课程与密码专硕课程的协同教学。例如在高等代数课程中讲解矩阵理论时，可以与密码中的分组密码算法相结合，理论上从矩阵运算和性质的角度讲解，应用上讲解分组密码算法中矩阵的应用，进一步从密码算法的设计原理和安全性分析方面进行补充和拓展。通过协同教学，让学生在学习高等代数知识的同时，能够及时了解其在密码学中的应用，加深对知识的理解和掌握，也为后续学习密码专硕课程奠定良好的基础。

四、结语

将密码中的相关案例引入高等代数教学是一种有效的教学方法，通过在不同教学环节引入合适的密码学案例，合理设计案例的难度梯度和多样性，把握案例引入的实施要点，能够显著提升学生的学习兴趣和知识应用能力，实现高等代数与密码知识的深度融合。这不仅有助于学生更好地掌握高等代数知识，还为他们后续在密码专硕的学习和研究奠定坚实的基础。在未来的教学实践中，教师应不断探索和完善密码学案例引入的方法，根据学生的反馈和教学实际情况进行调整和优化，以适应不断发展的教学需求和人才培养目标。

参考文献

[1] 段雪峰，段复建，李春梅 . 代数类课程的教学改革探索 [J]. 教育教学论坛，2011,(33):19-20.

[2] 李雪佳，郭爱丽 . 基于应用型人才培养的高等代数课程教学改革探索 [J]. 考试周刊，2018,(96):67-69.

[3] 刘光军 . 应用型本科高校应用密码学课程教学方法和教学内容改革探索 [J]. 当代教育实践与教学研究，2018,(09):62-63.

[4] 王平辉，赵俊舟，张迪 . 密码学课程教学改革探索 [J]. 高教学刊，2025,11(08):53-57.

[5] 丁南庆，刘公祥，纪庆忠，郭学军 . 高等代数 [M]. 科学出版社，2021.

[6] 张艳硕，李丽秋，袁煜淇，张健毅 . 密码学课程实践教学的思政教育探索与实践 [J]. 北京电子科技学院专科学校学报，2024,(3).

