陕西交通职业技术学院
“思政课程”、“课程思政”示范课程
专项课题

典型案例

课题名称《密码学基础》“课程思政”示范课程研究与实践

申请部门 交通信息学院

课题负责人 薛倩

起止日期 2021 年 4 月至 2021 年 11 月

目录

陕西交通职业技术学院
SHAANXI COLLEGE OF COMMUNICATIONS TECHNOLOGY

模块三 保护信息安全
——《密码学基础》课程思政案例

一、案例综述

（一）课程简介

密码学是实现保密通信和信息系统安全的主要技术手段和工具,信息安全的保密性、认证性、完整性和不可否认性等属性都需要密码学的工具来完成。密码学有着悠久的发展历史,在二十世纪七十年代以前,密码学的应用主要限于军事和政治领域。随着计算机和计算机网络的普及,特别是网络安全的需要,加之自身理论与技术的发展,密码学逐渐走进更为广阔的民用领域,成为越来越受重视的学科。如今,各种密码学的加密和认证技术是实现网络安全、电子商务、电子政务等系统的必要手段。

《密码学基础》是信息安全技术应用专业的专业基础课，主要目的是让学生掌握密码学的基本理论、概念与方法，认识密码学、认识经典密码学、保护信息安全、保护应用安全、保护主机安全，通过了解和掌握企业信息安全中应用到的密码技术和产品，培养学生在企业信息安全管理与实践中应用密码技术解决信息安全问题的能力。

（二）案例背景

1.课程思政的目的和意义

随着我国改革开放的不断深入，中国特色社会主义进入了新时代。新时代的中国既是经济与社会走向高质量发展的转型阶段，也是各种矛

盾各种问题各种思潮更加纷繁的历史时期。而对于置身其中的相当数量的大学生来说要想正确解决此类问题并非易事，因为他们正处在一个重要的成长阶段，其世界观、人生观、价值观还未稳定成型，自身经历浅薄、文化积淀不够、鉴别和认知能力较弱，所以当他们面对多种价值观冲突和交锋的时候，在短时间内甚至在相当长的一段时间内都很难辨别清晰，并做出正确选择与取舍。

2016 年 12 月，习近平总书记在全国高校思想政治工作会议上强调指出，“高校思想政治工作关系高校培养什么样的人、如何培养人以及为谁培养人这个根本问题”。所以，做好高校思想政治工作，要因事而化、因时而进、因势而新。要用好课堂教学这个主渠道，思想政治理论课要坚持在改进中加强，提升思想政治教育亲和力和针对性，满足学生成长发展需求和期待，其他各门课都要守好一段渠、种好责任田，使各类课程与思想政治理论课同向同行，形成协同效应。

在 2017 年 12 月，中共教育部党组印发了关于《高校思想政治工作质量提升工程实施纲要》的通知。纲要中明确提出“要坚持育人导向，突出价值引领，建立健全系统化育人长效机制，特别是统筹推进课程育人，以此推动以‘课程思政’为目标的课堂教学改革，优化课程设置，修订专业教材，完善课堂教学设计，加强教学管理，充分挖掘和运用各门课程所蕴含的思想政治教育元素和所承载的思想政治教育功能，融入课堂教学各环节，实现思想政治教育与知识体系教育的有机统一”。

新时代，高校思想政治教育工作面临的环境愈加复杂，单纯依靠思想政治理论课或是课程德育，已很难适应思想政治教育的现实发展需求，也不利于“立德树人”目标的实现，所以“课程思政”的理念与实践应运而生。

2.课程思政教育现状

思想政治教育一直是教育界和理论界高度关注的领域。现有的研究较多地关注思想政治理论课、综合素养课程等层面，而对占学生培养课程量第一位的专业课程则关注较少，且当前高校的思政教育工作发展还是相对薄弱，高校大学生思想政治教育“孤岛化”困境尚未根本扭转，仍然存在着思政教育与通识教育、专业教学“两张皮”现象，导致教师对“知识传授”和“价值引领”关系的理解有误区，学生对课程的认同度和获得感不均、自我的政治认同和价值认同不高。因此，作为一名专业教师，抓住高校“育人”的本质要求，充分认识到由思想政治理论课、综合素养课程、专业教育课程构成的三位一体的高校思想政治教育课程体系中专业教育课程的重要地位，探索如何在专业课程教育中根植思政理念，将思政教育与专业课程学习自然融合，把正确的价值追求和理想信念传达给学生的路径方法为当下亟需解决的课程思政问题。

3.《密码学基础》课程申报我校“思政课程”、“课程思政”示范课程专项课题

在高校开展思想政治教育工作一系列政策大背景下，我校设立了“思政课程”、“课程思政”示范课程专项课题，《密码学基础》课程成功立项，课题组展开《密码学基础》“课程思政”相关内容研究，并完成课程标准、课程教案、典型案例等文档的撰写和示范课堂教学视频的录制。

（三）案例简述

《密码学基础》课程由认识密码学、认识经典加密算法、保护信息安全、保护应用安全、保护主机安全共 5 个模块、13 个子任务组成。典型案例内容选自模块三保护信息安全（见图 1-1），其中包含哈希函数、数字签名、密钥协商、认证技术 4 个子任务，分为 14 课时讲解（见表

1-1）。

图 1-1 课程内容及案例选取

表 1-1 案例讲解课时分配表

模块	任务	教学内容	课次	课时
模块三：保护信息安全	任务 1：哈希函数	哈希函数	第 15 次课	2
	任务 2：数字签名	数字签名-RSA	第 16 次课	2
		数字签名-SM2	第 17 次课	2
	任务 3：密钥协商	D-H 密钥交换协议	第 18 次课	2
		密钥管理	第 19 次课	2
		密钥管理实验	第 21 次课	2
	任务 4：认证技术	身份认证	第 22 次课	2
合计：				14

案例通过对课程思政理念研究、课程思政内涵分析、案例教学总体设计、学情分析、案例教学目标梳理、案例重点难点及解决策略归纳、案例课程思政挖掘、课程思政融入专业课教学方法研究，从案例包含的密码学知识中挖掘出(1)哲学教育、(2)美学教育、(3)数学思维、(4)家国情怀、爱国主义、民族自信心教育、(5)安全意识教育、(6)党史教育、(7)职业精神教育、(8)诚信守法教育、(9)知识产权保护学习、(10)中国优秀

传统文化学习，共10个方面的思政切入点；形成《密码学基础》课程95个思政融入课程教学的实例，其中案例部分的课程思政实例为34个；并以信息安全技术应用专业人才培养方案为依据，按照课程标准的要求，根据案例内容提炼涵盖职业岗位知识、技能、素质培养和思政育人“双线并举”教学目标；提出8个课程思政融入专业课教学的方法；设计“课前课中课后”三段线上线下混合式教学过程；最后总结了教学成效、反思了案例存在的问题。

二、案例分析

（一）思路与理念

1.课程思政理念

学校是国家培养人才的重要基地，其立身之本是立德树人，所有课堂都有育人功能，要充分挖掘专业课中的思政资源，在知识和能力培养中做好学生思想引领和价值观的塑造工作，把课程中的文化基因和价值范式转化为弘扬社会主义核心价值观的教学载体，将社会主义核心价值观融入学生思想政治教育全过程，帮助大学生校准理想信念、价值取向的坐标，自觉克服在价值认知、价值判断、价值选择等方面存在的困惑与偏差，努力增强学生的政治认识和认同、文化自觉和自信，实现推进大学生的价值观教育与行为内化的双轮驱动，唤醒青年一代的责任意识和担当精神，提升大学生的思想道德、精神品格和人文素养。

在做到全课程育人的同时，教师履行育人职责，实现专业课程与思想政治理论课同向同行。这就是架构“课程思政”体系的目标与核心理念，在教育教学中将社会主义核心价值观内化于心，外化于行，既注重在价值传播中凝聚知识底蕴，又注重在知识传授中强调主流价值引领，突出显性教育与隐性教育相融通，实现立德树人润物无声。

2.课程思政构建思路

基于案例内容的教学目标，研究案例涉及的专业知识体系，根据课程案例内容特点、学情分析，结合思想政治教育的内容和专业前沿知识，设计教学重点难点解决策略、挖掘思政切入点，形成课程思政实例和课程思政融入教学方法，并将其自然地运用到专业知识的讲授、技能的培养、素质的提升过程中，进行完整的教学过程设计。

（二）设计与实施

1.总体设计

案例实施主要从(1)课程思政内涵分析、(2)学情分析、(3)案例教学目标梳理、(4)案例重点难点及解决策略分析、(5)案例课程思政挖掘、(6)课程思政融入专业课教学方法研究、(7)“课前课中课后”三段线上线下混合式教学过程设计 7 个步骤展开进行。

2.课程思政内涵分析

通过学习国家相关思政育人的政策文件精神，研读专家有关课程思政的内涵分析，根据先进的课程思政育人观点，总结得出“课程思政”就是在马克思主义基本立场观点方法的指导下，以学校所有课程为育人载体，把思想政治教育贯穿于教育教学活动全过程的育人理念和实践活动，即课程承载思政、思政寓于课程。

3.学情分析

（1）知识基础

《密码学基础》是信息安全技术应用专业的一门专业基础课。学生经过前期的部分课程学习，对于信息安全知识有一定的了解，具有一定的学习基础。

（2）《密码学基础》课程特点

密码学涉及消息机密性、完整性、身份认证、数字签名、访问控制等诸多领域，拥有密码编码学和密码分析学两个分支，很多理论算法都以数学为基础，是信息安全的基础与核心。总体而言《密码学基础》课程内容繁杂、知识面广、交叉性强、数学基本理论应用多。

（3）学生特点

1）数学基础较薄弱，缺乏迎难而上、学习报国的家国情怀

高职学生对于密码知识的要求是了解各算法原理，熟悉算法特点以及掌握算法的应用，对学生的数学基础知识要求较高，大多数学生的数学基础较薄弱，没有掌握数学思考的意识和掌握数学思考的方法，学习有畏难情绪，缺乏迎难而上、奋发学习、报效祖国的家国情怀。

2）对推导论证过程不感兴趣，缺乏运用科学理论指导实践能力

高职学生大多数对推导论证过程不感兴趣，重视的只是结论及其应用，只对例题、习题、作业的讲解感兴趣，因此，使得对课程算法原理知识框架的理解不够透彻，缺乏运用科学理论指导实践的能力。

3）缺乏学习热情和主动进取职业精神

部分学生进入大学后，学习动力来源已不存在，学习目标不明确，缺乏主动进取的精神状态。课堂表现整体比较被动，学习积极性不高，缺乏学习热情和职业岗位精神。

4）自学能力较差，缺乏独立思考的意识

对老师存有较强的依赖心理，没有反思学习过程的习惯，更不具备归纳、总结知识内容和思想方法的习惯。他们往往忽略了科学有效的学习方法是获取知识的重要条件。另一方面，在学习过程中没能有效进行自我监控，缺少及时反馈，这对于培养自己的抽象思维能力和迁移能力树立了一道难以跨越的障碍。

5）迟到现象时有发生，缺乏诚信守信意识和遵守职业道德规范意识

上课迟到早退、作业完成不及时，一定程度上在当前学生中存在。说明学生缺乏对诚信的认知，没有遵守职业道德规范的意识。

6）容易受到社会不良风气影响，缺乏辨别能力和责任意识

大学生正处在一个重要的成长阶段，其世界观、人生观、价值观还未稳定成型，容易受到社会上一些错误的价值观的左右，从而迷失自我，缺乏辨别能力和责任意识。

7）获取知识途径灵活多样，有利于线上线下混合式教学开展

学生对信息的获取途径丰富多样。可以有效解决学生对课程重难点的学习。可以正确引导学生择优选取各类学习资源，为线上线下混合式教学的开展打下基础。

以上是根据学生特点，亟需解决的几个问题，案例将结合课程特点将课程思政融入课程教学，通过思政育人，解决学情存在的问题，引导学生健康发展。

4.案例教学目标分析

以信息安全技术应用专业人才培养方案为依据，按照课程标准的要求，根据案例内容提炼涵盖职业岗位知识、技能、素质培养和思政育人“双线并举”教学目标（见图 2-1）。

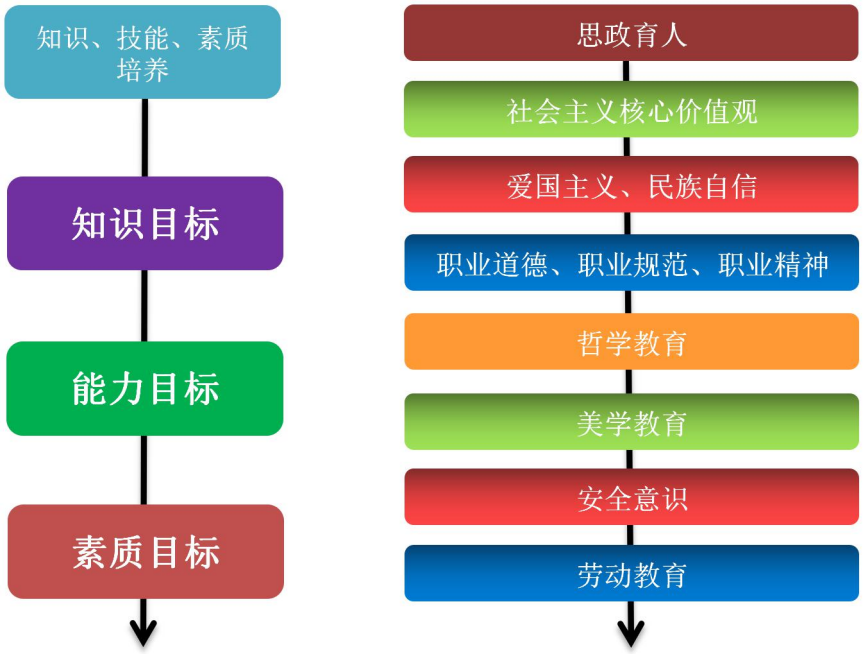


图 2-1 “双线并举”教学目标

（1）知识目标

1）了解哈希函数，掌握MD5算法、SHA算法；

2）了解数字签名概念；

3）掌握基于公钥加密的数字签名模型；

4）掌握 RSA 数字签名方案、SM2 算法、数字签名标准、盲签名；

5）掌握 Diffie-Hellman 密码交换协议；

6）了解密钥、密钥管理的概念；掌握密钥管理的内容、密钥分配技术、密钥的分层和分散管理策略；

7）掌握完整性认证和数字证书等密码技术。

（2）能力目标

1）能够应用密码技术实现企业数据的保密性和完整性；

2）能够应用哈希函数；

3）能够应用密码技术实现身份认证和管理；

4）能够完成企业各类型密钥安全管理与分发。

（3）素质目标

1）具有持续学习和终身学习、分析问题和解决问题的能力；

2）具有敬业精神，吃苦耐劳、团结合作、严谨细致的工作态度；

3）增强学生职业荣誉感和责任感，具有健康的体魄和良好的身体素质，拥有积极的人生态度。

（4）思政育人目标

1）培养深厚的爱国情感和中华民族自豪感，弘扬家国情怀；

2）践行社会主义核心价值观；

3）激发党史学习的积极性和实效性；

4）弘扬中华民族传统文化，提升科技创新能力；

5）树立国家安全意识和网络安全意识，遵守网络安全法律法规，提高辨别能力，增强责任意识、法治意识，捍卫个人信息安全；

6）培养爱岗敬业精神，倡导诚实守信、健康文明的网络行为，增强团队协作意识、职业荣誉感和责任感；

7）体会哲学思想，感受曲折的美、数学的美、公式的美，培养学生处世智慧;

8）教育学生知法、懂法、守法，牢固树立“保护知识产权”意识。

5.案例重难点和解决策略分析

基于案例选取内容为模块三保护信息安全的 4 个子任务，分为 14 课时、7 次课讲授，根据教学目标和内容，设计 7 次授课内容重点难点的解决策略（见表 2-1）。

表 2-1 教学重难点及解决策略

任务 1：哈希函数（2 课时）		
教学重点	**内容**	**理解 MD5 算法的原理**
	解决策略	课前布置任务，了解 MD5 的概念和作用，在课堂通过动画演示熟知 MD5 算法的过程，教师将难点进行讲解，最后通过实验操作掌握 MD5 的应用。
教学难点	**内容**	**哈希函数安全性分析**
	解决策略	课前布置线上学习，了解哈希算法的定义，课堂通过学生分组讨论哈希函数安全性，教师总结，再以数学推导，具体的数字显示改善和安全性。
任务 2：数字签名——数字签名 RSA（2 课时）		
教学重点	**内容**	**RSA 数字签名算法**
	解决策略	通过动画演示、案例讲解，了解 RSA 数字签名算法，课堂上通过练习，分组完成 RSA 数字签名算法实验，掌握 RSA 数字签名算法。
教学难点	**内容**	**RSA 数字签名的安全性分析**
	解决策略	要分析 RSA 体系的安全性，必须对 RSA 攻击方面进行分析，分组讨论，对模数 n 因子分解攻击分析；对 RSA 的选择密文攻击分析；教师总结，并完成相应的实验，利用智慧树平台记录学生表现，实时显示积分，激发学生积极性。
任务 2：数字签名——数字签名 SM2（2 课时）		
教学重点	**内容**	**基于椭圆曲线实现数字签名**
	解决策略	提前布置椭圆曲线的概念，课堂提问，摸清学生基础，教师讲解 SM2 数字签名算法和验证算法，分组讨论区块链中的数学-SM2 的签名和验证过程，最后引导学生对椭圆曲线数字签名进行总结，认识更多的应用场景，提高学习的

		积极性。
教学难点	内容	**数字签名标准**
	解决策略	课前布置预习，课中学生分享数字签名标准的发展脉络，通过视频了解数字签名标准，学生讨论数字签名标准目的，教师讲解数字签名 DSS 背景知识和 DSS 算法，由于该算法比较复杂，采用框图形式展示该算法，最后通过举例加深学生对算法的理解。
任务 3：密钥协商——D-H 密钥交换协议（2 课时）		
教学重点	内容	**Diffie-Hellman 密码交换协议原理**
	解决策略	关于邮局双方在没有任何密钥的情况下，能否协商出一个秘密的共享密钥为导向，引发学生讨论，角色扮演，进而得出无需交换密钥就可以传递秘密信息，教师通过动画讲解 D-H 密钥交换协议过程，分析该协议优点和缺点，通过算法举例、总结，加深输出方法的理解与记忆，进而突破教学重点。
教学难点	内容	**中间人攻击**
	解决策略	根据 D-H 密钥交换协议原理，结合课前预习数学基础，分组讨论 D-H 密钥交换协议的安全性，从而模拟中间人攻击，最终教师分析重要环节，通过如何设计一个安全的 Diffie-Hellman 密钥交换协议，突破教学难点。
任务 3：密钥协商——密钥管理（2 课时）		
教学重点	内容	**密钥的生成**
	解决策略	课前布置任务,搜集密钥的故事,通过沈安娜的字母表、熊向晖的密电典型故事，课堂上展开讨论，了解密钥、密钥管理的概念和重要性，通过动画演示加深密钥生命周期的理解。
教学难点	内容	**SSH 远程登录**

	解决策略	最后使用密钥验证方式完成远程登录任务,教师讲解原理,学生加深 Telnet 和 SSH 远程登录的区别,进一步掌握 SSH 远程登录的原理。
任务 3：密钥协商——密钥管理实验（2 课时）		
教学重点	**内容**	**密钥的生命周期**
	解决策略	课前布置任务,搜集密钥的故事,通过沈安娜的字母表、熊向晖的密电典型故事，课堂上展开讨论，了解密钥、密钥管理的概念和重要性，通过动画演示加深密钥生命周期的理解。
教学难点	**内容**	**CA 证书以及 SSL 连接**
	解决策略	课前预习 CA 证书以及 SSL 连接,在课堂上分组完成实验,学生分析完成任务的收获,教师总结,使学生进一步理解 CA 证书与 SSL 连接相关应用。
任务 4：认证技术——身份认证（2 课时）		
教学重点	**内容**	**认证和消息摘要的概念**
	解决策略	从小品《开锁》的视频中，引入了身份识别的教学内容，课堂上通过互动，了解身份识别的实现方式和应用场合。通过动画演示，以类比思维加深认证、加密、与数字签名的区别。
教学难点	**内容**	**报文认证和完整性认证**
	解决策略	课前布置任务,介绍防伪技术，并完成防伪技术用到的知识，在课堂上通过小组汇报和课堂互评,教师总结,最后通过线上测评，使得学生进一步理解认证的原理和相关应用,在智慧职教平台记录学生表现，实时显示积分，激发学生积极性。

6.教学实施过程

（1）分析《密码学基础》课程内容，挖掘与之紧密相关的课程思

政切入点

1）密码学知识中的哲学教育

辩证法三大规律，即对立统一规律、量变质变规律、否定之否定规律，在密码学课程中处处得到体现。

a.密码学中的对立统一

世界上任何事物的内部和事物之间都包含矛盾的两个方面，矛盾的双方既对立又统一，事物的运动发展在于自身的矛盾运动。密码学自诞生起就体现了对立统一性，密码学作为一门学科包含密码编码学和密码分析学，也就是“攻”与“防”两个对立的方面，这对矛盾不断促进了密码学的发展。量子计算机可以攻破现实中正被使用的 RSA 等公钥加密方案，为此，当前一些密码学家正研究能抵抗量子计算机的密码方案。这推动了密码学领域的一个新分支即后量子密码学的出现。世上没有单一性质的、绝对的事物。这一规律也体现于密码学中，比如，现实使用的密码方案没有是绝对安全的，只有相对安全的。

b.密码学中的量变质变

任何事物的变化都是由量变到质变的过程，量变到一定程度引起质变，产生新质，然后在新质的基础上又开始新的量变。密码学中关于加密方案的安全性定义的不断完善就很好地体现了这一规律。在公钥密码学诞生后，密码学界关于什么是安全的加密方案并没有清晰的概念。起先，人们认为在一个方案中，只要由公钥推不出私钥，则这个方案就是安全的；渐渐地，人们发现这样并不能保证方案是安全的，因为当一个方案是确定性加密的时候，即一个明文只确定性地对应一个密文时，通过密文比对就有可能恢复小明文空间的明文。1984 年，Goldwasser 和 Micali 首次提出了概率加密的概念，在该思想的启发下，密码学家给出

了关于加密方案的 IND-CCA（Indistinguishability under chosen ciphertext attack,选择密文攻击下的密文不可区分性）安全性定义。

c.密码学的否定之否定

任何事物的发展变化都是新事物对旧事物的否定，是事物内部的肯定和否定两方面矛盾斗争的结果，是事物自我发展的过程，但是否定并不是全盘抛弃，是克服和保留的统一。新事物否定旧事物然后被更新的事物否定，一切事物都“螺旋式”向前发展。密码学的发展脉络始终体现这一“螺旋式”发展的客观规律。在 1976 年之前，人们使用的密码学都是对称加密方案，即加密密钥和解密密钥一样的加密方案。然而随着计算机网络的发展，人们发现对称加密方案有一个很大的缺陷，即在多节点网络中需要大密钥量。1976 年，Diffie 和 Hellman 提出了公钥加密的思想，即加密密钥可公开，而解密密钥不公开的加密思想。在多节点网络中，公钥加密方案可大大减少密钥量。公钥加密方案也有一个缺陷，就是加解密速度比对称加密方案低几个数量级。公钥密码的出现是密码学发展的一个里程碑，但它的出现并没有导致对称加密方案的退出。现实中，人们将这两者结合实现混合加密方案，在混合加密中公钥方案用来加密对称密码的钥匙，而对称方案用来加密数据。

2）密码学知识中的美学教育

美的事物是人们喜欢的事物。一个全面发展的人应该是善于发现美、乐于发现美的人。作为教师应该努力发掘，并让学生领略到课程中蕴含的美。密码学课程（包括课程中用到的数学）中美学教育可以体现在以下方面。

a.研究对象的美

对称的事物往往是美的。中国的古典建筑美轮美奂，它们大都是中轴对称的，比如北京的故宫单个宫殿和整个宫殿群都是对称的，甚至整个老北京城也是对称的。群论是密码学一个重要的数学工具。“群”是一个很抽象的概念，教师告诉学生“群”就是研究事物的对称性，1885 年化学家利用“群”证明了自然界中只有 230 个结晶群，从而把自然界的所有结晶体予以分类后，学生就会对“群”这个理性概念有了感性的认识，发现“群”就在他们的身边。

b.思维的抽象美

密码学课程中所用到的一些数学无疑是抽象的，有的学生害怕抽象，摸不透抽象。教师在讲相关知识块的时候，可结合具体的例子，讲一些抽象概念的产生背景，使学生明白一个哲理：抽象也是具体的，抽象是更一般的具体。比如在讲图论的产生背景时，可以给学生抛出历史上著名难题哥尼斯堡七桥问题，让学生先解决，当学生束手无策时，可以提醒学生可把陆地看成点，桥看成线，之后一部分学生自己就可以解决哥尼斯堡七桥难题。这样学生就有成就感，也能感知抽象是具体的，进而领略了数学抽象思维的魅力。

c.发现的曲折美

密码学很多发现都是跌宕起伏，有痛苦更有快乐，有失败更有胜利，可以说密码学的一些发现就像一个个动人的故事。在讲授密码学知识的时候，可以给学生讲授与之有关的故事。这方面的例子很多。比如，在讲公钥密码学创建时，可以告诉学生如下背景。当时还是大学本科生的 Merkle 创造性地提出了公钥密码学的思想，而他的思想和论文残忍地被他的教师和相关杂志拒绝；等 Diffie 和 Hellman 率先发表了公钥密码学思想后，人们才慢慢地承认 Merkle 作为公钥密码的创始人之一。

3）密码学知识中的数学思维

密码学涉及较多的数学知识，如数论、图论、椭圆曲线、概率论、数理逻辑等，还涉及计算机、通信工程等多个学科，是数学学科的一个重要应用。《密码学基础》课程内容与数学理论环环相扣。密码学有些理论或方案用语言描述是复杂的，学生也不能掌握其本质。如将这些理论或方案凝练成公式，不光学生易记、易懂，也许更能揭示本质。在讲RSA公钥加密时，学生往往一头雾水，可是当教师告诉学生加密就是$c=m^e \bmod n$，解密就是$m=c^d \bmod n$ 时，学生不光一辈子不会忘记，也能感受到数学公式的深刻、简洁。

4）密码学知识中的家国情怀、爱国主义、民族自信心教育

爱国主义、民族自信心教育是我国重要的教育方针。大学课程教学也应当贯彻爱国主义、民族自信心教育。密码学基础（包括课程中用到的数学）的很多理论都是西方建立起来的，因此，在密码学课程教学中进行爱国主义、民族自信心教育尤为重要和紧迫，当然也有难度。例如，在授课过程中，针对国外密码体制在信息安全领域的垄断地位问题，为学生引入王小云教授成功破解MD5密码算法的事例，鼓励大家学习王小云教授潜心基础研究、不畏困难、敢于挑战、勇于创新的科研精神。加强对学生思想政治的教育可以从课内外两手抓起：应当注重在课堂教育中多多引用名人事例，使学生在学习专业知识的过程中体会人性的光辉；鼓励大家在课下多观看杰出人物的影视作品，在休闲娱乐中欣赏他们高尚的品质，以提升自己的思想境界。此外，教师在不断提升自我的思想道德素质和政治文化修养的同时，在生活和学习中以身作则，为学生树立良好的榜样。

5）密码学知识中的安全意识教育

习近平总书记说过：“没有网络安全就没有国家安全”，随着我国网络环境的不断发展，结合已经颁布并实施的《中华人民共和国网络空间安全法》、《中华人民共和国数据安全法》等相关法律法规，引导学生运用自身的专业特长为维护风清气正的网络空间环境而做出贡献，懂得建立健康安全的网络环境是每个网络参与人的义务。

根据信息安全与网络安全行业的法律法规，提醒学生重视密码学课程，认真学习，保证在以后的职业岗位中具有良好道德修养和法制意识，建立起必要的职业担当；课堂中提出：如何提升网络安全性以保护个人隐私问题，通过讨论反思网络安全隐私泄露事件，号召学生在使用网络过程中注重保护个人隐私，研究新的隐私保护技术。

6）密码学知识中的党史教育

引入沈安娜的字母表、熊向晖的密码典型故事，了解党领导下的保密工作发展历程，一代代共产党人服从党的纪律，严守党的秘密的初心故事。提高学生学习党史的积极性。从党的伟大征程中，从党的保密工作历史中，汲取前进的智慧和力量，珍惜来之不易的学习机会，从而为实现“中国梦”注入无限生机和活力。通过党史学习教育对中国共产党的百年历史进行回顾，帮助学生深刻理解我党建立、发展及奋进的历史，充分认识到党的领导下中国特色社会主义制度的优越性，增强民族自豪感，培养热爱祖国和人民的爱国情怀。

7）密码学知识中的职业精神教育

目前，互联网企业的技术人员存在职业素质良莠不齐的现象，在技术开发等工作岗位上经不住利益的诱惑，把职业道德、从业规范等要求抛在脑后，将不合规范或没有通过有效的实践和评估的产品推向市场，

给用户带来了不必要的损失。对于信息安全行业的从业人员来说，倘若没有良好的职业素养，他们就会给社会和个人带来很多麻烦，例如：侵入互联网用户系统，窃取大量的数据信息，更有甚者会危害国家网络安全。

通过具体案例，在项目实施之前，使学生明白“不要企图访问超过其权限的内容”，不得有意或无意泄露项目信息，轻者对单位造成不利影响，重者可能触犯法律。众所周知，信息安全没有绝对，只有相对。因此，在项目实施过程中，要让学生明白，安全是动态的，只要一个小小的漏洞都可能是对手攻击的目标。在项目实施过程中培养学生团队合作精神、沟通与团队的协作能力；注重职业素质和大国工匠精神，文档规范，严格数据分析过程，培养学生严格遵守操作标准的习惯，精益求精的工匠精神。

8）密码学知识中的诚信守法教育

以《中华人民共和国网络安全法》、《中华人民共和国电子签名法》为依据,倡导诚实守信、健康文明的网络行为，践行社会主义核心价值观，做到知法懂法守法；通过访问控制概念的介绍，强调诚信守法、诚信考试，教育学生树牢“四个意识”，坚定“四个自信”，坚决做到“两个维护”，要把职业道德放在第一位，严守道德、法治规范，坚决抵制违法犯罪。

9）密码学知识中的知识产权保护学习

国务院印发的《“十四五”国家知识产权保护和运用规划》提出知识产权保护迈上新台阶、知识产权运用取得新成效、知识产权服务达到新

水平、知识产权国际合作取得新突破等四个主要目标，全面加强知识产权保护。

通过对网络犯罪、知识产权、隐私权及计算机相关道德问题的了解，教育学生遵纪守法；引入防伪技术案例，强化学生的知识产权保护意识，引导学生尊重知识产权，不能剽窃别人的论文和观点，不用盗版软件、不买盗版书籍、影像资料等。通过介绍隐私权的定义，号召学生在使用网络时，注意保护个人隐私，不被他人非法侵犯、知悉、复制、利用和公开，同时也注意不泄露或侵犯他人的敏感信息，包括事实、图像等。启发学生积极研究新的隐私保护技术。

10）密码学知识中的中国优秀传统文化学习

2017 年中共中央办公厅、国务院办公厅印发的《关于实施中华优秀传统文化传承发展工程的意见》，从政策层面推进中华优秀传统文化融入思政课教学。教师可以将中华传统文化融入到密码学基础课程中，培养学生对中华文化的高度认同，筑牢中华民族共同体意识。

在讲解身份识别时，可以告诉学生我们的老祖先早就使用身份识别的思想了，那就是“兵符”。在讲数论基础知识时，古典密码实验将十六进制的字符串转换成 base64 编码，为了便于学生理解，用中国的成语作为例子：“屈指可数”是十进制；“掐指一算”是六十进制；“半斤八两”是十六进制，并进一步介绍中国天干地支纪年法中的天干十进制、地支十二进制和中国易经中的二进制，帮助学生了解古人智慧、认识密码学基础中知识。

了解到这些素材后，学生会发觉中国传统文化的魅力，学生的民族自信心在得到加强的同时，更感责任重大，更加自觉地把优秀传统文化和民族精神继承和发扬下去。

（2）案例课程思政实例挖掘

按照涵盖职业岗位知识、技能、素质培养和思政育人“双线并举”教学目标，基于案例教学内容，结合学情分析，为了解决案例重点和难点，挖掘出 34 个案例部分的课程思政实例（见表 2-2）。

表 2-2 课程思政实例

序号	模块	任务	课程思政实例	思政元素
1	模块三：保护信息安全	任务 1：哈希函数	通过 md5 的反向查询网站，警示大家网络中以密文形式传输，个人口令设置安全可靠；	**安全意识**
2			通过王小云教授领导的团队做出的创新性贡献，增强学生的民族自豪感；	**民族自信** **科技创新**
3			通过全球网络安全事件，培养学生在网络行为中的网络安全意识和国家安全意识；	**科技创新**
4			通过了解“图片识别”原理，提高学生学习积极性，培养学生的知识迁移能力；	**职业精神**
5			讲解二进制和十六进制，了解中国文化的活水源头《易经》中的阴阳八卦及其所蕴含的辩证哲学和处世智慧；	**中国传统文化**
6		任务 2：数字签名	通过学习《中华人民共和国电子签名法》和《中华人民共和国个人信息保护法》，培养学生网络安全意识和国家安全意识，教育学生知法、懂法、守法；	**安全意识**
7			通过讲述比特币之父中本聪的故事，体会发现曲折的美；	**美学教育**
8			欧拉函数将复杂的理论或算法抽象为公式，容易记忆、容易理解，更能揭示事物的本质；	**美学教育**

9			了解我国商业密码算法SM2是一种较RSA算法更先进安全的算法，已成为ISO/IEC国际标准，培养学生的爱国主义精神，建立民族文化自信；	**民族自信**
10			通过对RSA数字签名的安全性分析，体会数字签名方案是螺旋上升的，注重知识的积累；	**哲学教育**
11			了解签名发展路线，体会哲学思想，感受安全是相对的，学习是螺旋式上升的；	**哲学教育**
12			解密与加密、签名与验证是攻与防对立的两个方面，这对矛盾不断促进密码学的发展；	**哲学教育**
13			通过完成RSA数字签名实验，养成严谨细致、团结合作等职业素养；	**职业精神**
14			结合当前社会和企业的实际需求，讲解“区块链”技术，增强学生兴趣，养成学生持续学习的习惯；	**职业精神**
15			讨论能不能“炒币”“发币”，帮学生树立起牢固的思想防线；	**安全意识**
16			通过对网络犯罪、知识产权、隐私权及计算机相关道德问题的学习，教育学生遵纪守法；	**职业规范**
17		任务3：密钥协商	引导学生在网络生活中积极履行自己的义务，严格遵守网络安全法律法规，共建和谐网络环境；	**安全意识**
18			通过了解国家安全事件“台湾间谍”，坚持总体国家安全观,增强维护国家安全的意识和能力；	**安全意识**
19			使用大家熟知的HTTPS安全网站，揭示D-H密钥交换协议，引导大家提高用户安全意识；	**安全意识**
20			失之毫厘谬以千里，一个小小的错误就会使实验结果南辕北辙，培养学生做事严谨、精益求精的工匠精神;	**工匠精神**
21			分享最傻密码榜单,提出怎样才能保护好十分重要的个人敏感信息呢?树立安全意识；	**安全意识**
22			遵守多媒体和机房管理条例，自觉维护卫生和安全；	**劳动教育**

23			通过案例讲解，亲身体会“无硝烟的战争”，学生体会祖国的强大富强，激发爱国主义情怀；	**爱国精神**
24			通过分组实验，提高团队合作意识；在课程实践当中注重职业素质和大国工匠精神，文档规范；	**职业精神**
25			课前任务：观看“厉害，我的国”，感受大国风采、科技创新，激发学生努力奋斗；	**民族自信**
26			通过沈安娜的字母表、熊向晖的密电典型故事，了解党领导下的保密工作发展历程，提高学生学习党史的积极性；	**爱国精神** **学习党史**
27		任务4：认证技术	通过了解互联网安全的现状，培养学生的学习热情，强调网络强国的战略思想；	**网络强国**
28			通过分析用户认证方式，强调保护个人信息在工作中的重要性，培养学生的敬业精神；	**职业精神**
29			通过对访问控制概念的介绍，强调诚信和守法，教导学生不要企图访问超过其权限的内容；	**诚信守法**
30			通过讨论防伪技术案例，强化学生的知识产权保护意识；	**知识产权保护**
31			讲到身份识别时，可以告诉学生我们的老祖先早就使用身份识别的思想了，那就是“兵符”；	**中国优秀传统文化**
32			讨论对敏感信息采用哪些加密方法保护，加强学生的信息安全意识、辨别能力和责任意识；	**安全意识**
33			华为、中国电信、中兴等一系列骨干企业以信息科技创新赋能疫情防控的实干报国的事迹，激发学生对所学专业和行业领域的自豪感，以及科技报国、勇担青年责任的信心与决心；	**爱国精神**
34			通过对网络犯罪、知识产权、隐私权及计算机相关道德问题的学习，教育学生遵纪守法。	**职业精神**

（3）课程思政融入专业课教学方法研究

为了更好地对专业课挖掘融入课程思政元素，课题组成员还进行了

课程思政融入专业课教学方法研究，研究总结如下：

1）案例教学是思政融入专业课教学的重要方式

案例、实例讲解往往是教师讲解理论知识，破解重难点，经常使用的教学载体和方式，在课程设计和实际教学中，教师可以透过案例教学和分析的过程融入家国情怀、价值观念、政治信仰、职业道德教育等，以便让学生习得批判性思维、悟得正确价值观。

2）加强实验实操环节，积累实操经验，培养学生学习和科研热情

《密码学基础》课程教学可以结合密码实践中各种鲜活的实例，而不仅仅是一些枯燥的知识传授。比如，了解工程系统实现中的嵌入算法，不仅考虑算法的安全性和实现效率，还要了解算法的应用场景。通过了解两种应用场景:数据块加密模式和卫星通信加密模式，学生很快理解各种工作模式的特点，而不是机械记忆模式的优缺点；再比如，利用GunPGP 安全通信实现互动，在趣味性操作的同时理解密码学的概念，提高了《密码学基础》课程的挑战度。

3）采用线上线下混合式教学模式，课前课后开展思政育人

通过线上线下混合式教学，课前课后发布预习任务、教学案例、教学资源，将思政内容渗透到教学的各个环节，通过师生之间的课上课下的交流与分享，切实提高课前课后教学的亲和力和针对性，打造教学全过程思政育人课程。

4）注重过程化考核方式，体现课程思政考核内容

课程考核评价从知识、能力、素质、“课程思政”和职业技能等级证书考核要求几个方面展开，注重理论知识、实践动手能力、过程和职业素质考核。课程的考核涵盖过程考核（50%）和期末考核(50%)两个部分。其中过程考核分为线上考核（20%）、线下课堂考核（20%）和职业素

质和思政考核（10%）。线上考核包括平时线上考勤，线上资源学习、线上作业、线上课堂互动、线上讨论等内容；线下课堂实操考核主要是课堂任务实操完成情况考核；职业素质考核主要包括学习态度、任务执行力、分析问题、解决问题等能力，思政考核主要包括爱国主义情怀、爱岗敬业、信息安全从业人员职业道德等“课程思政”方面进行考核。

5）以时事热点为切入点，有助于开展国情教育

课堂上，教师可以从学生最感兴趣的话题开始，激发学生的兴趣，吸引学生的注意，打破沉闷的氛围，让他们不再“抵触”上专业课，同时还能拉近师生之间的关系，但对话题的选择，教师也要考虑到国家环境、时代背景等因素，以便全面的开展国情教育，从而让学生树立民族自豪感，学会理性思考、辩证批判。

6）明确政治立场、增强政治意识是专业课的核心要素

世界是多元化的，从不同的立场去判断或衡量某一事物或事件，产生的结果往往也是不一样的。现实世界充满诱惑，思维尚未完全成熟、价值观尚未充分确立的大学生，极易被误导走入误区或是危险区，所以在形成健全思维和人格前，应该学会理性思考、明辨是非，从而明确自己立场、增强政治意识。

7）实践锻炼是思政教育融入课程教学的有效途径

开展实践锻炼既能更加有效、无形地把思政教育融入其中，也能检验课堂教学的成果，所以应该延伸课堂教育，走进学生的课外实践团队、走进学生生活社区、走进学生网络，贯通课堂内外，从而更深入地服务和支持学生的实践发展、社会发展以及创新创业的需求。例如，以大思政育人为指导方向，以志愿活动为媒介，建设若干个符合思想政治实践学分标准的实践基地及服务性学习教学实践基地，强化实践锻炼，建立

起与课堂教学同向并行的实践教学成绩单，激励学生将远大抱负落实到具体的实践探索中。

8）邀请行业专家举办专业知识讲座报告，参加行业活动，树立积极正确的职业态度，提升民族自豪感

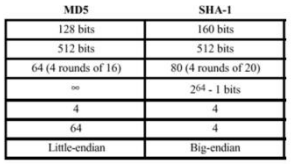
每学期邀请《密码学基础》课程相关领域的行业技术专家举办专业知识主题讲座报告，每学年组织学生外出参加信息安全行业活动，通过请进来走出去的方式，激发学生学习积极性，培养学生职业精神，提升民族自豪感。

（4）“课前课中课后”三段线上线下混合式教学过程设计

案例由哈希函数、数字签名、密钥协商、认证技术 4 个任务组成，共计 14 课时，具体教学过程设计见表 2-3。

表 2-3 教学过程设计表

教学过程	教学步骤	教学具体活动	教学手段	思政育人融入
案例模块：保护信息安全（14 课时） 任务 1：哈希函数（2 课时）				
课前	1）预习任务 2）查看预习任务 **20分钟**	1）提前发布预习视频学习任务和预习练习题 2）课前查看学生预习情况，做到心中有数。	职教云平台发布视频、文档	
课中	1）任务引入 **2 分钟**	视频引入，开讲吧（王小云教授） 	视频展示	

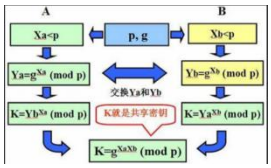
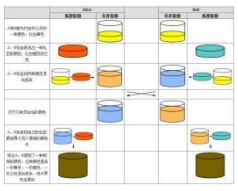
	2）引发思考 **5 分钟**	王小云教授解决的难题是什么？对美国军用算法有什么影响	分组讨论	通过全球网络安全事件强调网络安全对于国家安全的重要性，培养学生在网络行为中的网络安全意识和国家安全意识
	3）知识讲解 **8 分钟**	讲解哈希函数	讲授法	哈希函数的单向性，告诫学生，遵守国家网络安全，一旦违法，承担相应的法律
	4） 知识讲解 **【重点】** **20 分钟**	讲解 MD5 算法	讲授法	通过讲解王小云教授不懈奋斗的典型案例，用榜样人物的成长经历激励学生成长，引导学生努力做到刚健有为、自强不息
	5）实验练习 **10 分钟**	利用 MD5 转换工具对字符学生本人姓名进行加密，解密；利用 Hashmyfile 工具对合同或协议进行加密，解密；	现场演示 实操指导	通过 md5 的反向查询网站，警示大家网络中以密文形式传输，个人口令设置安全可靠；
	6）知识讲解 **15 分钟**	讲解 SHA 函数	讲授法	
	7）学生实操 **8 分钟**	1.利用 SHA 转换工具对字符学生本人姓名进行加密，解密； 2.利用 Hashmyfile 工具对合同或协议进行加密，解密；	现场演示 实操指导	在以后的职业岗位上，树立责任意识和责任担当，提高团队合作意识
	8）对比 **10 分钟**	类比法加深对 Hash 函数的理解  	讲授法	
	9）小组汇报 **5 分钟**	根据预习，学生分享 HASH 函数应用场景  	分组讨论	

	10）小组讨论【难点】15 分钟	哈希函数安全性分析：课堂通过学生分组讨论哈希函数安全性，教师总结，再以数学推导，具体的数字显示安全性	分组讨论 讲授法	
	11）小结与作业 2 分钟	整合本节课所讲内容，对本节课的学习内容进行回顾讲解，引导学生思考回答问题。	讲授法	
课后	课后拓展	线上对学生提交的学习成果进行课后评价，与学生交流互动，完成课后答疑。		
任务 2：数字签名 ——数字签名 RSA（2 课时）			录制 50 分钟示范课堂教学视频	
课前	1）预习任务 2）查看预习任务 20分钟	1）提前发布预习视频学习任务和预习练习题 2）课前查看学生预习情况，做到心中有数。	职教云平台发布视频、文档	1.通过学习《中华人民共和国电子签名法》和《中华人民共和国个人信息保护法》，培养学生网络安全意识和国家安全意识;教育学生知法、懂法、守法；
课中	1）任务引入 3 分钟	视频引入，如何保证线上合同的完整性、身份认证、不可抵赖性？	微课视频辅助教学 	
	2）引发思考 5 分钟	传统认识中手写签名和印章作用是什么？ 教师借助平台课堂活动“选人”功能，摇一摇选人，确定所在小组进行问题回答	教师平台摇一摇	
	3）引出内容 6 分钟	 那究竟什么是数字签名数字？	讲授法	

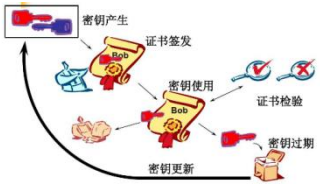
	4）知识讲解 **8 分钟**	1）数字签名满足的要求 2）数字签名发展 	讲授法	习近平总书记说过：没有网络安全，就没有国家安全。每个人要有主人翁精神，自觉地遵守法律法规和道德准则，自觉地规范网上行为。
	5）抛出问题 **3 分钟**	数字签名有哪些应用了？学生讨论，抢答回答	教师平台设置抢答	
	6）知识讲解 **【重点】** **20 分钟**	数字签名模型讲解，三步完成：系统参数和密钥对、签名、验证	讲授法	解密与加密也就是攻与防对立的两个方面，这对矛盾不断促进密码学的发展
	7）小组讨论 **【难点】** **15 分钟**	RSA数字签名方案讲解，三步完成：系统参数和密钥对、签名、验证	分组讨论	欧拉函数φ(n)，将复杂的理论或算法抽象为公式，容易记忆、容易理解，更能揭示事物的本质。
	8）案例引入 **15 分钟**	RSA 签名方案举例【案例】对借条设计一个基于 RSA 数字签名方案	讲授法 案例分析	在大数据时代，各种信息泄露，我国即将颁布《中华人民共和国个人信息保护法》，各位同学日常工作或生活中电脑密码、家用 WIFI、社交类网站密码设置高强度密码。
	9）学生练习 **10分钟**	RSA 签名方案练习，明确任务后，认真分析问题，完成练习	练习法	
	10）学生实操 **10 分钟**	RSA 签名方案实验，使用之前学习的工具，根据“数字签名实验指导书”，验证数字签名技术实现过程，体会在数据传输过程中的保密性和完整性保护。	实操指导	在今后职业岗位上，应该具备严谨的工作态度和团队协作职业精神。
	11）小结和作业 **5 分钟**	通过小组讨论和教师点评，总结本节课的知识点。回答得好可加 1-2 分,布置作业	讲授法	

课后	课后拓展	分析 RSA 数字签名的安全性，复习和总结任务，下发至云平台；		树立安全意识，学生讲电子设备、社交类网站等密码设置高强度密码
任务 2：数字签名 ——数字签名 SM2（2 课时）				
课前	1）预习任务 2）查看预习任务 **20分钟**	1）提前发布预习视频学习任务和预习练习题 2）课前查看学生预习情况，做到心中有数。	职教云平台发布视频、文档	通过对网络犯罪、知识产权、隐私权及计算机相关道德问题的学习，教育学生遵纪守法。
课中	1）内容回顾，引入任务，学生汇报 **5 分钟**	带领学生回顾上半节课程所学内容，将学生注意力引回课堂之中，根据预习任务，分组汇报国密算法在日常工作生活中的应用	分组讨论	
	2）引出内容 **5 分钟**	你还知道其他数字签名方案吗？	任务驱动法	
	3）内容回顾 **20 分钟**	线上测评，回顾数学基础知识，教师讲解椭圆曲线数字签名算法和验证算法	讲授法	
	4）小组讨论 **8 分钟**	分组讨论区块链中的数学签名和验证过程	分组讨论	1.通过区块链的学习，提高学习的积极性； 2.通过讲述比特币之父中本聪的故事，体会发现曲折的美。
	5）知识讲解 **【重点】** **20 分钟**	SM2数字签名	讲授法	
	6）小组汇报 **5 分钟**	根据预习任务，学生分享数字签名标准的发展脉络	分组讨论	

	7）知识讲解 **【难点】** **15 分钟**	教师讲解数字签名DSA算法	讲授法	
	8）学生练习 **8 分钟**	通过案例加深对算法的理解	案例驱动法	
	9）强化训练 **6 分钟**	学生练习，加深对算法的理解	现场演示	
	10） 知识讲解 **6 分钟**	通过图片理解盲签名原理 	讲授法	讨论能不能“炒币”“发币”，帮学生树立起牢固的思想防线
	11） 小结和作业 **2 分钟**	通过测试，总结课程知识点和存在的问题	讲授法	
课后	课后拓展	线上对学生提交的学习成果进行课后评价，与学生交流互动，完成课后答疑。		
任务 3：密钥协商 ——D-H 密钥交换协议（2 课时）				
课前	1）预习任务 2）查看预习任务 **20分钟**	1）提前发布预习视频学习任务和预习练习题 2）课前查看学生预习情况，做到心中有数。	职教云平台发布视频、文档	了解Diffie- Hallman的故事，感受科学家持之以恒的科研精神，激发学生奋发图强，在本行业中砥砺前行
课中	1） 任务引入 **5 分钟**	对称加密算法解决了数据加密的问题。我们以AES加密为例，在现实世界中，小明要向路人甲发送一个加密文件，他可以先生成一个AES密钥，对文件进行加密，然后把加密文件发送给对方。因为对方要解密，就必须需要小明生成的密钥。现在问题来了：如何传递密钥？	问题导入	

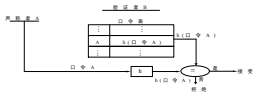
	2） 任务讨论 **5 分钟**	将问题转化为一个很形象的情景问题（邮局问题）：假如 Alice 和 Bob 住在农村，当时的邮政系统还不发达，邮局人员可以看到公开的信息，Alice 希望给 Bob 发送一个非常私密的文件（密钥，对称密码体制的密钥），请问如何处理？	分组讨论	引导学生思考，感受到了启发式教学的无穷魅力
	3） 知识讲解 **3 分钟**	密钥交换的起源	图片、PPT展示 讲授法	使用大家熟知的HTTPS安全网站，揭示D-H密钥交换协议，引导大家提高用户安全意识
	4） 知识讲解 **6 分钟**	D-H协议的应用： 在不安全的信道上传递加密文件是没有问题的，但是，如何如何在不安全的信道上安全地传输密钥？	讲授法	目前大多数网络技术掌握在发达国家，在新的技术面前，教育学生加强专业知识，未来掌握网络的核心技术，把我国发展为网络技术强国。
	5） 知识讲解 小组讨论**【重点】** **20 分钟**	 分组讨论并角色扮演，理解D-H密钥交换协议过程	角色扮演法 分组讨论	
	6） 引入案例 **12 分钟**	 通过大家熟知的场景，模拟DH密钥交换协议	案例分析法	
	7）现场演示案 **8 分钟**	DH算法交换密钥的步骤 A 计算 $Y_A = 5^{36} \bmod 97 = 50$ B 计算 $Y_B = 5^{58} \bmod 97 = 44$ A 和 B 交换公钥后，双方均可单独计算出对称密钥 K： A 计算 $K = (Y_B)^{X_A} \bmod 97 = 44^{36} \bmod 97 = 75$ B 计算 $K = (Y_A)^{X_B} \bmod 97 = 50^{58} \bmod 97 = 75$	现场实验	公钥的发展体现知识积累呈现的螺旋上升，培养学生探索、发现新的知识的热情和习惯。

	8）学生练习 **10 分钟**	通过练习，了解DH算法的本质，进一步如何通过数学定律保证了双方各自计算出的密钥是相同的。	练习法	培养团结协作能力，提高职业素养
	9）引入案例 **10 分钟**	实际场景举例，由于不能鉴别双方身份，容易遭受中间人攻击	案例分析法	
	10）小组讨论 **【难点】** **16 分钟**	模拟中间人攻击场景，分析密钥的不安全性	分组讨论	
	11）小结和作业 **5 分钟**	点评学生完成的实验，并把存在问题列出来进行总结。	讲授法	失之毫厘谬以千里，一个小小的错误就会使程序运行结果南辕北辙，培养学生做事严谨、精益求精的工匠精神。
课后	课后拓展	发布课堂知识测验。通过本节课学习，仍存在个别同学学习要求未达标，需要对这极少数同学进行辅导		
任务 3：密钥协商 ——密钥管理（2 课时）				
课前	1）预习任务 2）查看预习任务 **20分钟**	3）提前发布预习视频学习任务和预习练习题,搜集密钥的故事 4）预习SSH概念、CA证书以及SSL连接 5）观看“厉害，我的国” 6）课前查看学生预习情况，做到心中有数。	1）职教云平台发布视频、文档	课前任务：观看“厉害，我的国”，感受大国风采、科技创新，激发学生努力奋斗；
课中	1）问题引入 **5 分钟**	密钥是控制密码算法实施加密解密的钥匙，谈谈对密钥的认识 	视频展示	

	2）引发思考 **5 分钟**	回顾对称密码、公钥密码、数字签名使用的密钥有何区别?	讲授法	
	3）分组汇报 **15 分钟**	根据预习内容，分组汇报关于密钥的故事	分组讨论	搜集密钥的故事,通过沈安娜的字母表、熊向晖的密电典型故事，课堂上通过小组讨论，了解密钥、密钥管理的概念和重要性。
	4）知识讲解 **25 分钟**	了解密钥管理概念	讲授法	
	5）引入案例 **【重点】** **30 分钟**	引入案例“上海电信密钥管理系统设计方案”，理解密钥生命周期——密钥生成 	案例驱动法	通过案例讲解，亲身体会“无硝烟的战争”，“在实践中，学生体会背靠一个强大的、负责任的祖国的强势，大家的爱国主义情怀被激发了出来。
	6）上机操作 **5 分钟**	实验：生成RSA密钥对	现场演示、实操指导	分享最傻密码榜单,提出怎样才能保护好十分重要的个人敏感信息呢?
	7）上机操作 **5 分钟**	使用Telnet，演示实验过程，讲解如何在 Linux 服务器上制作密钥对，设置 SSH，最后通过客户端登录完成，分组完成该实验	现场演示、实操指导	引导学生在网络生活中积极履行自己的义务，严格遵守网络安全法律法规，共建和谐网络环境。
	8）上机操作 **25 分钟**	实验：SSH 远程登录 动画形式讲解SSH远程登录的原理 	现场演示、实操指导	通过实验养成严谨、细致的工作、学习作风。
	9）知识讲解 **15 分钟**	密钥生命周期	讲授法	

	10）小组讨论 **【难点】15 分钟**	密钥的协商与分发，在课堂上通过角色扮演和课堂讨论密钥的协商，实时显示积分，激发学生积极性。	角色扮演 分组讨论	
	11）上机操作 **50 分钟**	实验：CA 证书与 SSL 连接：SSL 通道建立--创建自己的证书服务器，分组完成	现场演示、实操指导	通过解读最新的国家安全事件“台湾间谍”，指导学生保持警惕，不出卖国家机密信息，不信谣不传谣不造谣。
	12）小结和作业 **5 分钟**	引导学生思考实验过程中出现的问题，再次明确工匠精神在岗位中的重要性，总结实操过程中的问题点。	讲授法	
课后	课后拓展	整理教学中的问题进行复习与巩固		
任务 3：密钥协商 ——密钥管理实验（2 课时）				
课前	1）预习任务 2）查看预习任务 **20 分钟**	1）提前发布预习视频学习任务和预习练习题 2）课前查看学生预习情况，做到心中有数。	职教云平台发布视频、文档	观看“厉害，我的国”，感受大国风采、科技创新，激发学生努力奋斗；
课中	1）提出问题 **5 分钟**	怎样才能保护好十分重要的个人敏感信息呢	讨论法	
	2）知识讲解 **15 分钟**	密钥管理手段	讲授法	
	3）案例引入、知识讲解**【难点】** **30 分钟**	密钥的生命周期		通过案例讲解，亲身体会“无硝烟的战争”，学生体会祖国的强大富强，激发爱国主义情怀；
	4）教师演示**【难点】10 分钟**	SSL 通道建立--创建自己的证书服务器	角色扮演	

	5）学生操作【难点】15 分钟	学生分组完成实验：Web 服务器配置	现场演示、实操指导	
	6）学生操作【难点】10 分钟	学生分组完成实验:建立 SSL 通道	现场演示、实操指导	
	7）学生操作【难点】10 分钟	学生分组完成实验：客户端访问 Web 服务	现场演示、实操指导	通过分组实验，提高团队合作意识；在课程实践当中注重职业素质和大国工匠精神，文档规范；
	8）小结和作业 5 分钟	引导学生思考实验过程中出现的问题，再次明确工匠精神在岗位中的重要性，总结实操过程中的问题点。	讲授法	
课后	课后拓展	整理教学中的问题进行复习与巩固		
任务 4：认证技术 ——身份认证（2 课时）				
课前	1）预习任务 2）查看预习任务 20分钟	1）提前发布预习视频学习任务和预习练习题 2）课前查看学生预习情况，做到心中有数。	职教云平台发布视频、文档	
课中	1）任务引入 2分钟	小品《开锁》的视频中，引入了身份识别的教学内容，而且可以了解身份识别的实现方式和应用场合。 	微课视频辅助教学	
	2）引发思考，展开讨论 8分钟	如果大家想向其他人证明自己是身份，可以通过什么方式证明呢？	教师平台摇一摇	

	3）引出内容 **2分钟**	那究竟什么是认证？	问题导入	
	4）知识讲解 **20分钟**	口令认证，提出如何设置安全性强的口令？ 	头脑风暴	通过最傻密码榜单的展示，讨论对敏感信息采用哪些加密方法保护，如何设置安全的口令，提高学生对密码学的兴趣，加强学生的辨别能力和责任意识
	6） 知识讲解 **【重点】25分钟**	站点认证，报文认证： 举例如何检查操作员的 IC 卡声称的操作员身份是否正确	案例分析法	
	7） 知识讲解 **【难点】25分钟**	完整性认证： 根据预习，分组讨论如何防止电脑彩票（刮刮乐）的伪造问题？讲解完整性认证。 	案例分析法、分组讨论	通过讨论和案例，强化学生的知识产权保护意识，让学生学会尊重知识产权，明白不能剽窃别人的论文和观点，不用盗版软件、不买盗版书籍、影像资料等。
	7）引发思考 **6分钟**	毕业证和学位证是怎样防伪的？	平台摇一摇提问	提高自主创新能力，并学会拿起法律的武器来保护自己的创新成果
	8）知识应用 **5分钟**	HASH函数在身份认证中应用	讲授法	通过分析用户认证方式，强调保护个人信息在工作中的重要性，培养学生的敬业精神，通过讨论等教学方法完成任务目标，培养学生集体意识和团队协作能力

	9）小结与作业 7分钟	结合板书，对本项目的学习内容进行回顾讲解，引导学生回答问题。	讲授法	
课后	课后拓展	线上对学生做出的反馈进行审核评价		

（三）教学成效

1.学生知识技能水平不断提高，学习成绩稳步提升

《密码学基础》这门课程是信息安全技术专业的专业基础课，由于该专业首次开设该课程，且理论性强，通过课程思政，融入思政元素、密码故事，讲解最新密码学案例，最终学生期末成绩优秀率达到 18.3%，比期中提高 3.3%（见图 2-2）。

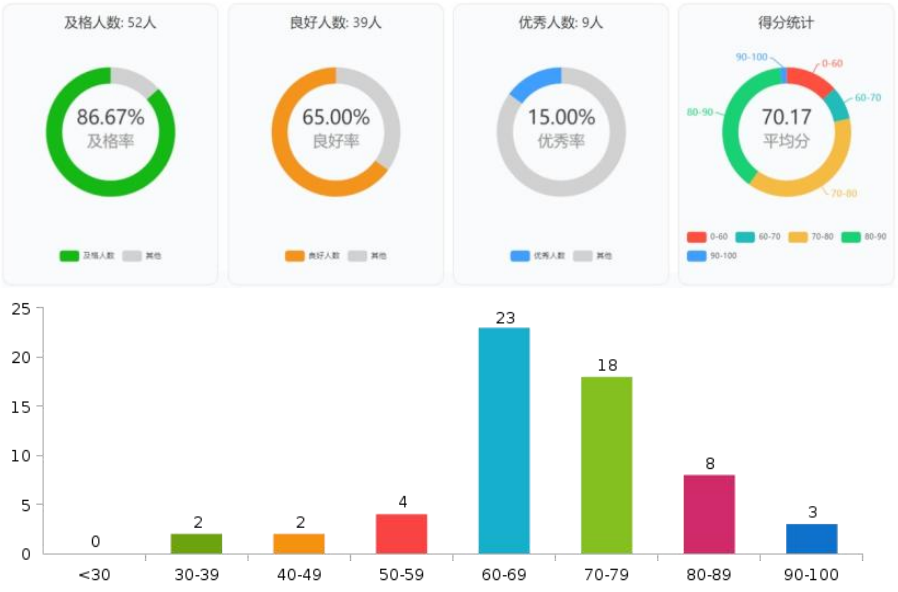


图 2-2 期中与期末成绩对比

2.学生学习热情和积极性显著提升

大多数学生在爱国意识、学习动力和努力方向等方面有了更大的收获。从“要我学”变为了“我要学”，学习积极性大幅提升（见图 2-3），学

生能主动获取知识，课前预习、课后作业和巩固都能主动完成（见图 2-4），并且对本专业有了更高的认可度。

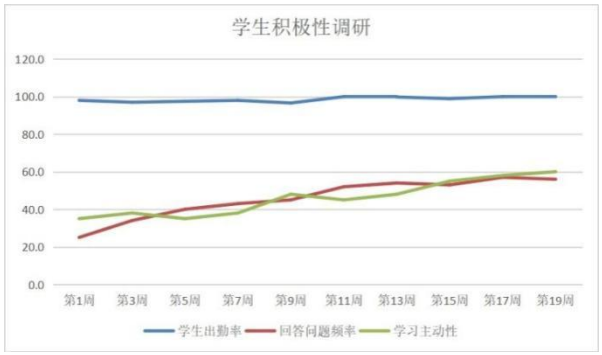


图 2-3 学习积极性问卷调查

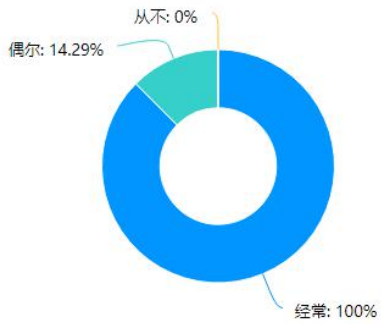


图 2-4 预习、作业完成情况

学生出勤率上升，课堂抬头率、互动率也得到了明显的提高（见图 2-5）。实践能力得到了提升，学习满意度和获得感显著增强，多名同学获得学习奖学金（见图 2-6）。

图 2-5 课堂互动截图

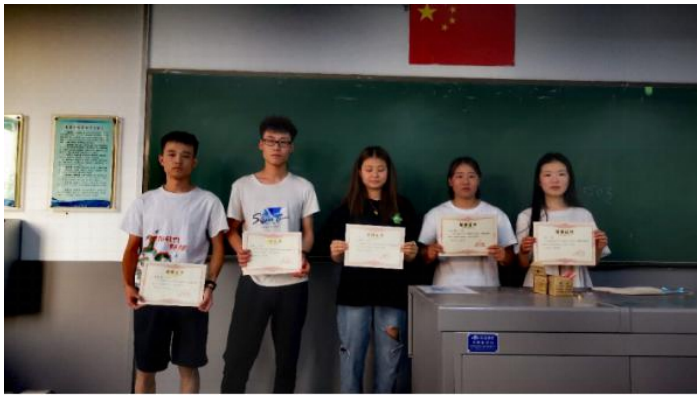


图 2-6 学生获得奖学金

3.学生在技能竞赛中获奖

加强理论与实践教学的结合，通过开展技能大比武赛项（见图 2-7），提高学生动手能力，提升学生网络安全责任意识，引导学生在学习专业技能的同时，坚定理想信念，增强团队合作意识。

图 2-7 学生参加技能大比武

课题组教师将职业精神、工匠精神融入到软件测试竞赛指导（见图 2-8），以精益求精、严谨细致、耐心专注、专业敬业的宗旨培育学生，提升学生职业核心素养。在 2021 年全国软件测试竞赛中获得三等奖。

图 2-8 软件测试竞赛

4.学生在“互联网+”大学生创新创业大赛中取得优异成绩

在教师的引导下，学生积极参加“互联网+”大学生创新创业大赛，其中《智能趣动释压健身房》入选校赛（见图 2-9），学生的创新意识与团队合作意识得到显著提升。

图 2-9 创新创业大赛作品

5.学生积极参加各项活动

（1）学术讲座

今年 6 月，课题组所在教研室组织学术讲座“新形势下网络空间安全技术探讨”（见图 2-10），10 月举办“洞悉安全态势，筑牢安全防线”主题报告（见图 2-11），报告现场学生兴致高昂，对网络信息安全的重要性、网络诈骗的危害性有了更深刻的认识，增强了学生的网络安全防护意识，拓宽了视野。

图 2-10 学术讲座

图 2-11 报告现场

（2）网络安全周博览会

2021 年 10 月，信息安全技术专业学生踊跃报名前往会展中心参观网络安全周博览会（见图 2-12），了解网络安全前沿技术，5G 安全、移动终端安全、网络支付安全等基础设施安全保护技术，增强了网络安全防范意识，提升了网络安全防护技能，树立正确的网络安全观。

图 2-12 学生参观网络安全周博览会

（3）学生活跃在志愿服务岗位

信息安全专业学生积极活跃在第十四届全国运动会、残运会（见图 2-13）、网络安全周博览会等志愿服务岗位，过程艰苦，但是收获很多，体会到强国的历史使命、深厚的家国情怀、开阔的全局视野。同时用运动员的精神勉励自己，锻炼强健的体魄，用积极乐观的态度，学好自己的专业。

图 2-13 学生参加十四运志愿服务

（4）学生助力疫情防控

信息安全专业学生主动参与协助学校大规模核酸检测工作以及留观学生的后勤工作，工作虽然辛苦，但同学们在关键时刻，有担当、不怕累，协助老师圆满完成了疫情防控相关工作。

三、案例反思

（一）特色与创新

1.学习思政育人国家政策，总结课程思政教教育现状，探讨课程思政理念，分析课程思政内涵，探索出课程思政挖掘和教学过程设计思路；

2.以信息安全技术应用专业人才培养方案为依据，按照课程标准的要求，根据案例内容提炼涵盖职业岗位知识、技能、素质培养和思政育人“双线并举”教学目标；

3.从课程包含的密码学知识中挖掘出（1）哲学教育、（2）美学教育、（3）数学思维、（4）家国情怀、爱国主义、民族自信心教育、（5）安全意识教育、（6）党史教育、（7）职业精神教育、（8）诚信守法教育、（9）知识产权保护学习、（10）中国优秀传统文化学习，共 10 个方面的思政切入点；

4.形成《密码学基础》课程 95 个思政融入课程教学的实例，其中案例部分的课程思政实例为 34 个；

5.提出 8 个课程思政融入专业课教学的方法。

（二）反思与改进

将研究成果在《密码学基础》课程中初步开展教学试点，按照课题研究成果中提出的课程思政构建思路、职业岗位知识、技能、素质培养和思政育人“双线并举”的教学目标、课程思政挖掘方法，将思政育人目标融入混合式教学过程中，使得学生对密码学、经典加密算法、保护信息安全、保护应用安全、保护主机安全有了完整的认识，同时树立了网络安全意识和国家安全意识，以及严谨的工作作风和团队协作职业精神，弘扬爱国情怀、传承中华民族传统文化，取得了一定思政育人的成效，但在还存在一些不足：

一是《密码学基础》课程为新开设的课程，截止目前只开展过一学期的课程讲授，课程理论性强且高职类教材偏少，部分教学内容的选取有待于研讨和提炼，教学过程设计还需要在实践中不断完善，符合行业需求的案例数量有限；

二是课程的育人资源虽然通过立项研究，进行了一定程度的挖掘，但深度和广度还不够，已挖掘的思政内容也还不够充分。部分教学资源“思政化改造”相对生硬，特别是一些红色教学案例的融入不够自然；

三是任课教师思政能力不足。自“课程思政”教学改革开展以来，任课教师也意识到了要发挥专业课的育人作用，但是由于思政育人能力不足而影响了“课程思政”教学理念实施的实效性。

因此，后续教学实施将做如下改进：

一是进一步整合教学内容。结合最新行业岗位需求和前沿科技知识，从实践方面帮助学生做到知行合一，以此提升课程思政的成效；

二是深挖思政元素。进一步了解学生对专业知识的掌握情况，分析学生的身心特点、价值观、思想动态等，同时针对学情分析结果，提升教师自身专业课思政挖掘能力，加强研究教学内容与课程思政的内在联系，以便在专业课上对学生进行思政教育时，做到思政切入点合理、因材施教，达到更好的思政育人效果；

三是加强思政理论知识学习。教师应在提升专业能力的同时加强思想政治修养，提高思想政治育人水平，确保思政理论知识在《密码学基础》及专业其他课程中的有效应用。