附件 3

江西警察学院课程思政教学设计

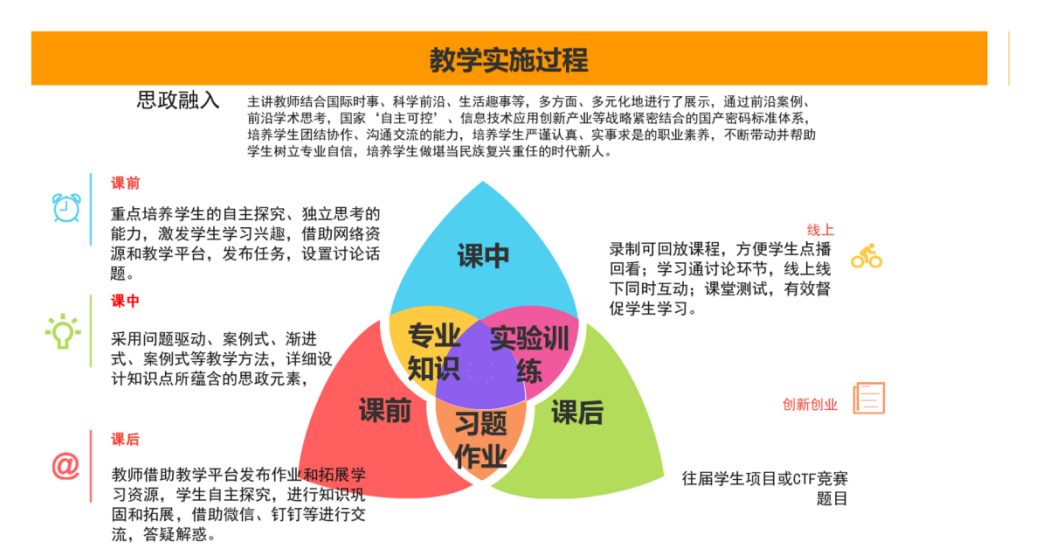
《现代密码学》“课程思政”教学案例

一、课程信息

课程名称	现代密码学	授课对象	网络安全与执法、信息安全大二学生
课程类别	专业课	课程学时	32 学时/64 学时
教材信息	应用密码学（第 4 版），胡向东，魏琴芳，胡蓉编著，电子工业出版社		
课程概况	1、现代密码学是网络安全与执法专业和信息安全专业的专业基础课。《现代密码学》课程教学以中华人民共和国密码法、网络安全法、数据安全法为引领，采用“专业教学、思政教育、创新创业”融合的线上线下混合式教学模式，在课程中多维度、多角度、全方位、立体化融合思政元素，打造思政元素与国家“自主可控”、国产密码标准算法紧密结合的思政创新内容体系，着力提升学生国家安全战略视野，实现为党育人、为国育才、为警铸剑的课程育人目标。 2、课程目标： （1）知识方面：能够较全面地掌握密码学的基本概念、古典密码体制、对称密码体制和非对称密钥体制、消息摘要算法等基础密码理论及典型算法，以及在数字签名、认证协议等方面的应用； （2）能力方面：培养发现问题、分析和解决问题的能力，能运用现代密码学的基本概念、基本原理、密码算法、协议和技术，分析并能应用密码技术的具体实现过程和方法； （3）素质方面：树立正确的人生观和价值观，具备良好的政治觉悟、道德品质和文化素养，具备良好的网络安全法制观念和网络安全防范意识，具备多角度思考问题的辩证思维能力 3、多元考核评价体系：构建多目标（知识、能力、素质）、多主体（学生自评，生生互评，教师评价）的评价体系，思政内容融入考卷中，思政教育全方位融入。 4、建设成绩：教学测评排名第一，带领学生参加各级各类网络安全大赛，指导学生完成科研项目和创新创业项目，反哺教学。		

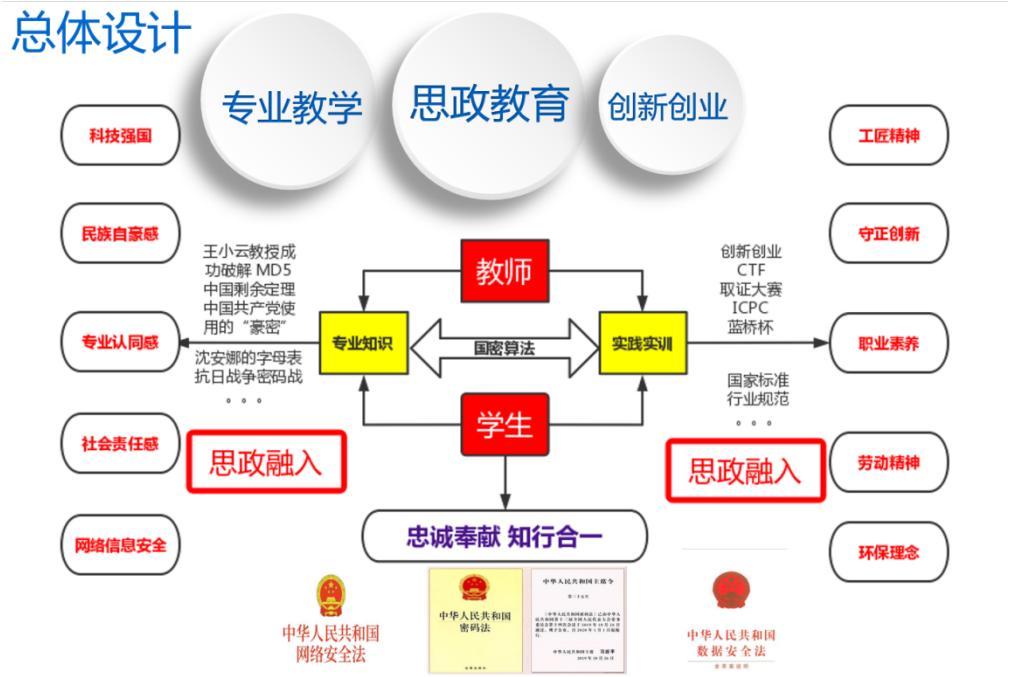
二、课程思政教学典型案例

授课内容	Hash 函数
教学目标	知识和能力目标： （1）理解散列算法的概念；（2）了解 Hash 函数的应用； （3）掌握 SHA 系列算法的原理；（4）理解 Hash 函数的安全性。 思政内容和目标： （1）从生活中找单向性为切入点，理解 Hash 函数单向性，激发创造和创新精神； （2）了解单向函数的安全性，理解密码学中对立统一的辩证思维； （3）介绍国产密码算法 SM3，提升民族自豪感； （4）美学融入，感受对称的美、曲折的美、算法的美，培养学生处世智慧； （5）了解王小云教授攻克 MD5、SHA-1 的励志故事，鼓励学生勇于探索、不怕失败，激发爱国主义精神，培养执着专注、精益求精、一丝不苟、追求卓越的工匠精神。
教学切入点及思政内容融入思路	教学切入点：视频“开讲吧（王小云教授）”。她是全中国最懂密码的人，她曾经沉潜 10 年，破解了世界上公认的两种最安全、最先进、应用最广泛的 Hash 算法：MD5 和 SHA-1。王小云教授不懈奋斗的典型案例贯穿于教学过程，用榜样人物的成长经历激励学生，鼓励学生勇于探索、不怕失败，激发爱国主义精神，培养执着专注、精益求精、一丝不苟、追求卓越的工匠精神。再从法律层面、国密算法、爱国主义等多维度深度挖掘思政元素，构建价值引领体系，增强保障国家网络信息安全的责任感；从课堂教学、实践教学、多元化评价体系等全方面抓好落实，构筑立体化思政教育联动阵地，达到润物细无声的教学效果。

教学过程	“课前课中课后”三段线上线下混合式教学过程设计  课前：新课导入：预习任务，提前发布预习视频任务点 课中：任务引入：视频“开讲吧（王小云教授）”  引发思考：分组讨论，王小云教授解决的难题是什么？破解了美国曾认为最安全的算法，说明了什么？【思政融入：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（民族自信；科技创新）】

	深度思考：SHA-1 已经破解了，为什么还要学、还要用？学习 SHA-1 为了什么？ 具体内容讲解： （1）以王院士破解 SHA-1 案例为切入点，引出 SHA-1 ；讲解 Hash 函数的概念和 SHA 系列算法。结合 SHA-1 演示算法，讲解 SHA-1 原理及流程；【思政融入：美学融入，感受对称的美、曲折的美、算法的美，培养学生处世智慧。】 （2）采用翻转课堂教学，学生讲述 SHA-1 用途及安全性【思政融入：今天，王小云院士领头设计的中国第一个国产的密码算法标准 SM3 作为重要的国产信息安全基础设施，不仅为国家安全保驾护航，连我们的银行卡、我们的社保卡、我们通过高速的 ETC，我们家的电卡、水卡，都在这套密码算法系统的保护之下（民族自豪感）。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。】 （3）利用 MD5 及 SHA 转换工具对字符学生本人姓名计算哈希值；利用 Hashmyfile 或校验 MD5 等工具对合同或协议进行哈希值计算【通过哈希算法反向查询网站，警示大家网络中以密文形式传输，个人口令设置安全可靠。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。】 （4）对比 MD5 和 SHA，类比法加深对 Hash 函数的理解。 （5）教师讲解：生日悖论（令人吃惊的概率问题）、鸽洞原理或称抽屉原理，学生分组讨论 Hash 函数安全性，教师总结，以数学推导，具体的数字显示安全性。【思政融入：鼓励学生用于探索、不怕失败，激发爱国主义精神，培养执着专注、精益求精、一丝不苟、追求卓越的工匠精神。理解密码学中对立统一的辩证思维。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，从而理解密码学中对立统一的辩证思维。】 （6）学生讨论：如何运用哈希函数确保系统中密码存储安全及信息的完整

	性？ （7）教师知识总结，课堂教学结束。【思政融入：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。（守正创新）】 课后： （1）完成作业：用 SHA-1 完成消息填充，学习通任务点和实验 （2）创新创业活动：引导学生将 SHA-1，特别是国密算法 SM3 创新应用于科研项目和竞赛中，培养学生组织、协同合作和应用创新等能力，鼓励其用于挑战自我，提升其学习的主动性和应用创新能力。

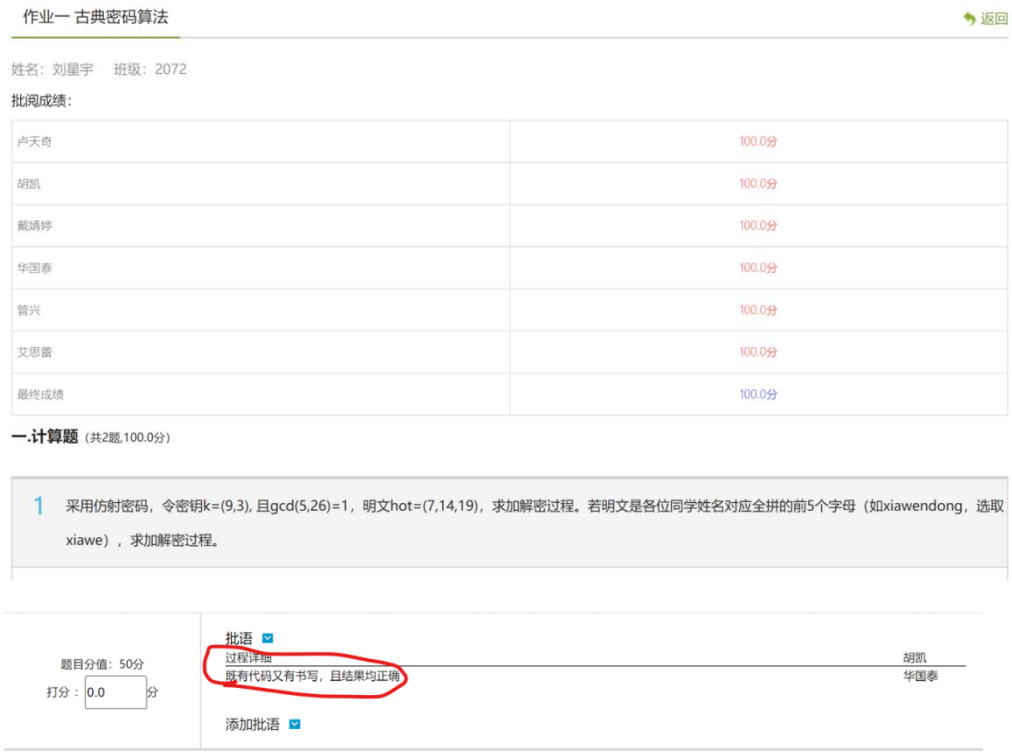
教学效果分析	《现代密码学》课程教学团队始终坚持高阶性是质量保障，创新性是发展动力，挑战度是根本特征，不光重视传授知识、培养能力，还重视对学生道德品质的塑造，并适时融入社会主义核心价值观的引导，即做到教书与育人并重。课程教学以中华人民共和国密码法、网络安全法、数据安全法为引领，采用“专业教学、思政教育、创新创业”融合的线上线下混合式教学模式，在课程中多维度、多角度、全方位、立体化融合思政元素，打造融合思政元素与国家“自主可控”、国产密码标准算法的思政创新教学体系，提升学生国家安全战略视野，实现为国育人，为党育才的课程育人目标。  本课程自 2021 年起开展课程思政，取得良好教学效果： 1、学生知识技能水平不断提高，学习成绩稳步提升 《现代密码学》是网络安全与执法专业和信息安全专业的专业课，该课程理论性强难度大，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，学生学习成绩有很大提升，优秀率高。 2、学生学习热情和积极性显著提升 师生共建思政资源库，激发学生们的学习热情，寻找资源的过程也是一种学习。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，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，过程性考核成绩能取得好成绩。

3、建成多元考核体系

构建了多目标（知识方面、能力方面、素质方面）、多主体（学生自评，生生互评，教师评价）的评价体系。

指定作业采用生生互评，如下图。



3、学生在个人修养、职业素养、理想信念上得到大幅度提高。

（1）学生参与课题项目和比赛的积极性提高，荣誉感明显提升，2022年五四青年节江西警察学院学生和山东警察学院学生联合发起“江&山五四分享会”；

（2）学生表现出了不怕苦、不怕累、精益求精、追求卓越的品质，他们创办微信公众号，分享学习和比赛心得；

（3）提升了学生的社会责任感，学生积极参加社会实践活动，在假期锻炼期间利用所学专业知识协助破案获锦旗及好评。

4、学生科研水平显著提升，学生在各类竞赛中获奖

近两年，课程负责人张亮老师指导所教学生完成国家级和省级大学生创新创业项目 4 项，在研大创项目 3 项，完成院级学生科研项目 1 项，在研 1 项；张亮老师带领学生参加“互联网+”大学生创新创业大赛及各级各类网络安全和大数据竞赛，获奖三十余项。

教学反思与评价	“专业教学、思政教育、创新创业”融合的线上线下混合式教学模式，使得学生对密码学专业知识有了完整的认识，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： 1、现代密码学理论知识点与实践并行讲解，强调理论结合实践，实践过程容易出现各类情况，从而课堂时间较难把握，节奏容易打乱，原来设计的思政元素就容易遗漏。经过三年多课程思政，已经较好地解决这个问题，通过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，采用了研讨式、情景化、翻转课堂等教学方法，同时教师自身专业课思政挖掘能力提升，能做到思政切入点合理、因材施教，达到很好的思政育人效果； 2、目前重点讲述国际通用密码算法，国产密码算法是作为思政融入点，已经很好融入了专业教学中，但是较少讲授国产密码算法。根据《中华人民共和国国家安全法》第 24 条、25 条规定“国家加强自主创新能力建设，加快发展自主可控的战略高新技术和重要领域核心关键技术”“实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控”，国家密码管理局批准了一系列国家密码标准。下一步，将结合国产密码算法对教学内容进行改进，让学生熟悉并掌握具有自主知识产权的国产密码算法，与工作实际紧密对接。