密码学课程教学改革之思政元素融入探索

罗　鹏　张春明
武警工程大学　陕西西安　710086

摘　要：针对当前专业课程进行思政元素融入的教学实际，根据教育部颁发的《高等学校课程思政建设指导纲要》中对理工课程进行思政建设的总体要求，在分析网络空间安全专业核心课程密码学特点的基础上，从六个方面阐述了进行课程思政的基本设想。

关键词：网络空间安全；密码学；课程思政

On the integration of ideological and political elements in the teaching reform of cryptography course

Peng Luo, Chunming Zhang
Engineering University of PAP Xi'an, Shaanxi 710086

Abstract: in view of the current ideological elements into the practical teaching of specialized courses, according to the Ministry of Education issued by the institutions of higher learning education course construction guidelines, to general requirements of the construction of the ideological course of technology, based on the analysis of the network space safety professional core course characteristics on the basis of cryptography, the lessons from six aspects this paper expounds the education of basic ideas.

Keywords: cyberspace security; Cryptography; Curriculum ideological and political

2020年6月，教育部印发《高等学校课程思政建设指导纲要》，明确了课程思政的具体建设目标和内容重点，对不同类别课程的教学设计和不同类别专业课的教学内容提出了基本要求，是学校全面推进课程思政建设、健全质量评价机制、加强组织保障的重要指导。其中对于理学、工学类专业课程做好课程思政给出了具体要求，即把马克思主义立场观点方法的教育与科学精神的培养结合起来，提高学生正确认识问题、分析问题和解决问题的能力。理学类专业课程，要注重科学思维方法的训练和科学伦理的教育，培养学生探索未知、追求真理、勇攀科学高峰的责任感和使命感。工学类专业课程，要注重强化学生工程伦理教育，培养学生精益求精的大国工匠精神，激发学生科技报国的家国情怀和使命担当。

随着社会信息化的不断加深，各种信息安全风险也伴随而生。国际上围绕网络空间安全的斗争愈演愈烈，争夺网络空间安全控制权是战略制高点。我国已成为网络大国，由于网络技术基础薄弱和网络空间安全人才不足，我国还不是网络强国网络安全关系到国家安全、社会稳定、经济发展、人民生活等各个方面，必须确保我国的信息安全，要建设国家信息安全保障体系，政府、军队、公安等国家重要部门，以及金融、电力、能源等重要基础设施等都需要大量信息安全专门人才。

密码学对于网络信息安全来说是属于基础性学科，密码体系如果需要改变的话，那么涉及的整体网络信息安全都需要进行相应的调整。因此密码学对于网络空间安全具有极端重要性[1][2]。

密码学相对于其他大学理工科课程来说，具有如下特点：课程所涉及的知识跨度广，课程难度高，理论性和应用性均比较强。密码学的学习需要诸多前置课程作为基础，根据课程设置的侧重点不同，前置课程分别包含数论、近世代数、有限域上数学运算和网络安全协议等。前置课程的知识难度较大，尤其体现出密码学这门课程对数学基础的要求很高。

同时，密码学课程本身知识跨度也很广。总的来说，其授课内容往往包含密码学基础、古典密码学、私钥密码学、公钥密码学、哈希函数、数字签名、身份认证和鉴别、电子商务中的密码学应用、网络安全协议的设计与开发以及公钥基础设施等等。知识跨度广的特点决定

了密码学这门课程具有较高的教学和学习难度。大部分学生反映课程难度太大，学起来困难重重。因此授课过程需要对算法细节进行详细的推导和分析，并且要想尽办法增加课程内容的趣味性和应用性，以吸引学生。此外，密码学课程的特点还体现在另一个方面，即授课内容的基础理论性和应用性都较强，学生学习这门课程的过程中对密码学的应用很感兴趣[8]。

1 厚植学生爱国主义情怀

在密码学课程介绍和导入时，可以从中国革命战争时期最值得我们骄傲的“豪密”讲密码与战争的关系，让同学们明白正是有了这个高级密码才保证了党和军队无线通信的绝对安全，运筹于帷幄之中，决胜于千里之外。同时也可以讲当下的密码学界的传奇人物王小云教授，多年来，由美国标准技术局（NIST）颁布的基于Hash函数的MD5和SHA-1，是国际上公认最先进、应用范围最广的两大重要算法。这两种算法的厉害之处在于，对于输入信息的任何一次小的篡改都会立刻引起“雪崩效应”，从而保证信息的数字指纹的唯一性和不可伪造性。因此，按照常规方法，即使调用大型计算机，也需运算100万年才有可能破解。但是，这两大世界最安全的密码算法却在2004年和2005年被王小云先后破解，震惊了国际密码学界。最为重要是，破解这两大算法时，她的大部分工作是在普通电脑和手算之下完成。她的工作也导致工业界几乎所有软件系统中MD5和SHA-1哈希函数的逐步淘汰[3]。哈希函数的两大支柱算法遭受重创后，2007年，美国国家标准技术研究院向全球密码学者征集新的国际标准密码算法，王小云放弃参与设计新国际标准密码算法，转而设计国内的密码算法标准。这部分内容可以放映短片的形式展示给学生，通过声音与画面的完美结合，使得课堂上学生们的民族自豪感油然而生。

2 增强学生科学报国使命感

在介绍课程内容时，让学生了解现代密码学以及很多数学理论都是西方建立起来的，虽然我们励精图治取得了长足的进步，密码学某些领域已经取得世界领先水平，但是仍要正视差距。回首我国近代历史，中华民族遭受的苦难之重、付出的牺牲之大，在世界历史上是罕见的，而我国落后挨打的根子之一就是科技落后。战火纷飞中，很多知识分子深切体会到了“中国要想强盛，只有靠中国人自己的力量”。面对苦难，他们奋起抗争，终于在中国共产党领导下踏上了实现国家独立和民族解放的正确道路，也为科学报国找到了最广阔的人生舞台。一代人有一代人的奋斗。无论是苏步青、黄纬禄、程开甲、朱光亚，还是屠呦呦、袁隆平、黄旭华、黄大年……时代变迁，科学家精神早已融入一代代中国科学家血脉之中，穿越时空、传承至今。这些优秀知识分子怀着炽烈的爱国情怀，凭借深厚的学术造诣、宽广的科学视角，作出了彪炳史册的重大贡献，体现出高尚人格风范和优良作风学风。

3 进行科学伦理教育

密钥管理过程需要管理与技术并重，密码系统的安全性取决于密码系统最薄弱的环节，即“木桶理论”[5]，再好的技术，如果没有有效的管理，终将毫无意义。因此加强安全从业人员的管理、培训尤为重要。计算机技术是一柄双刃剑，这把剑能够造福人类还是为祸人间取决于执剑人的道德意识，所以提升计算机从业者和用户的道德教育尤为重要，这种提升应该是全方位的，既要包括对他们的不良心理情绪的疏导，也要包括帮他们树立正确的人生观、世界观、价值观，既要帮助他们正确看待生活中出现的种种不如意，又要让他们认识到自己的能力和价值，给与其社会认同感。根据马斯洛相关理论，要从饮食需要、自我保护和社会保护、团队融入、得到认可以及自我实现等多个方面满足计算机技术拥有者的需要。预防信息技术从业人员犯罪的重要手段之一就是把公民道德建设纲要的内容作为网络道德宣传的核心内容，相关教育部门应将计算机道德教育列入普及德育教育的范畴，通过提高人们明辨是非的能力，使其形成正确的道德观[4]。

4 开展工程伦理教育

在讲解经典密码设备构造原理时，可以引入英尼格玛密码机进行工程伦理的教育。德国工程师亚瑟·斯雪比尤斯设计的英尼格玛密码机安全性极高，对于敌方，即使拥有密码机，如不同时掌握三道防线组成的密钥，就无法破译。二战时期上至德军统帅部，下至陆海空三军，都把“恩尼格玛”作为标准的制式密码机使用[6-8]。可以说英尼格玛密码机是密码发展史上的一个重要里程碑，但是它没有造福人类而是协助德国法西斯犯下滔天罪行。在当下社会工程实践目标也很容易被等同于商业利益增长，这一点随着越来越多工程的实施遭到了社会批判。人们日益认识到工程师因为应用现代科学技术拥有巨大力量，要求工程师承担更多伦理的义务和责任。从人才培养角度来说，信息安全的从业人员强调行业的专业化和独立性，也需要加强职业伦理建设。从工程实践（项目开发）来说，好的工程要给社会带来更多的便利，在课程思政建设过程当中必须要关注社会背景下工程实践中的伦理问题，这些问题仅仅依靠工程方法是无法解决的，必须在讲授相关内容时注意引导学生树立正确工程建设（项目开发）价值观。

5 训练科学的思维方式

科学思维是网络空间安全学科核心素养的要素之一，是形成科学方法论的重要途径。许多重要概念和规律都是科学思维的产物，而科学思维的形成，需要在问题的不断提出和解决中完成，因此，课堂教学中进行适时、适量、适度的问题串设计，可有效培养和发展学生的科学思维[9]。比如在讲解公钥密码体制提出的背景时，可以简单描述分组密码、序列密码等对称密码体制的基本原理，引导学生思考加解密双方所用的密钥都是秘密的，而且需要定期更换，新的密钥总是要通过某种秘密渠道分配给使用方，在传递的过程中，稍有不慎，就容易泄露。所以它的局限性在于它存在着通信的贸易双方之间确保密钥安全交换的问题。此外，某一贸易方有几个贸易关系，他就要维护几个专用密钥。它也没法鉴别贸易发起方或贸易最终方，因为贸易的双方的密钥相同。另外，由于对称加密系统仅能用于对数据进行加解密处理，提供数据的机密性，不能用于数字签名。因而人们迫切需要寻找新的密码体制。

科学的思维方式不仅能应用到专业领域，还能应用到日常生活中。掌握科学的思维方式对学生的学习有很大帮助，让学生能更理性地思考问题，有效地解决问题。教师引导学生深入思考，让学生养成良好的行为习惯，形成良好的品质，树立正确的三观，建立健全的人格。同时教师应培养学生敢于挑战、勇于创新的科研精神，鼓励学生积极创新，将信息安全相关技术服务于国民经济。

6 培养精益求精的大国工匠精神

在讲授DES、AES等设计精巧的密码算法时，注意引导学生树立精益求精、细而又细的工匠精神。当今世界，凡拥有发达制造业的国家，无不重视工匠精神的培育。工匠精神是工匠们在加工产品过程中表现出来的精神理念，如严肃认真的敬业精神、精益求精的品质意识、持之以恒的执着追求、淡泊名利的崇高境界等。不光生产建设需要工匠精神，科学研究同样离不开工匠精神[1]。

科学研究是追求真理、揭示规律的崇高事业，要求科研人员必须具备高度的责任感和敬业精神。对世界各领域杰出人士的调查显示，只要有认真负责的敬业精神，即使不是在自己最喜欢、最理想的岗位，也可以创造出非凡的业绩。科学研究也是如此，只有本着极端负责的态度，严肃认真地对待所从事的科研工作，才有可能在探索未知的道路上有所发现、有所突破。

一丝不苟、精益求精，才能打磨出精品。只有在实验中摒弃“可能”“也许”“差不多”等心理，才能在坚实的地基上矗立起胜利的高塔。密码学界很多前辈在科研工作中，为完成写成一篇高质量学术文章，经常逐字逐句反复讨论修改，直至觉得没有任何问题再发表。由此可见，只有坚持高标准、严要求，每一个环节、细节都想周全、做精细，才有可能达到最高水平[10]。

科学研究中失败往往多于成功，“九死一生”是其常态。只有在日复一日、琐碎而枯燥的研究中持之以恒，才有可能到达胜利的终点。回顾科学研究的历史长河不难发现，所谓灵光一现，其实往往是出自几年、十几年如一日的坚持与执着。

7 结束语

落实立德树人根本任务，必须将价值塑造、知识传授和能力培养三者融为一体、不可割裂。全面推进课程思政建设，就是要寓价值观引导于知识传授和能力培养之中，帮助学生塑造正确的世界观、人生观、价值观，这是人才培养的应有之义，更是必备内容。密码学课程作为网络空间安全专业的核心课程，在“课程思政”理念的引领下，在《高等学校课程思政建设指导纲要》指导下，通过挖掘课程思政元素，不断提升人才培养水平，把学生培养成具备扎实专业知识和坚定信仰的创新性人才。

参考文献：

[1]杨华.教育也需要工匠精神[J].课程教育研究：学法教法研究，2018（13）：119-119.

[2]李艳俊，欧海文.特色院校密码学优质课程建设研究[J].北京电子科技学院学报，2020，28（3）：74-80.

[3]王党卫.军校专业背景课程群“课程思政”建设与运用路径[J].空军预警学院学报，2021，35（03）：221-224.

[4]潘萌.科学研究中的伦理与道德之网络信息安全浅析[J].数码世界，2019（06）：244-245.

[5]郭宇燕，江明明，肖建于，孙梅.课程思政视域下信息安全专业课程建设探索[J].廊坊师范学院学报（自然科学版），2021，21（02）：100-103.

[6]窦本年，许春根，金晓灿.密码学课程中的人文素质教育[J].计算机教育，2019（03）：1-3.

[7]贾忠田，刘悦，张波.网络攻防课程建设经验探讨[J].计算机教育，2019（03）：12-15.

[8]贾伟峰，杨礼波.密码学的课程特点及教学方法探讨[J].华北水利水电学院学报（社科），2010，26（03）：169-170.

[9]李瑾，曹进，张跃宇，张美茹，李晖.信息安全专业课程思政的逆向教学设计——以西安电子科技大学“无线通信网络安全”课程为例[J].网络与信息安全学报，2021，7（03）：166-174.

[10]胡爱群，李古月，彭林宁，李涛.融入思政的网络空间安全前沿技术教学探索[J].网络与信息安全学报，2019，5（03）：54-66.