✦ 第十届全国密码学与信息安全教学研讨会

文章编号：1672-5913(2019)03-0001-03 **中图分类号：**G642

密码学课程中的人文素质教育

窦本年，许春根，金晓灿
（南京理工大学 理学院，江苏 南京 210094）

摘　要：分析密码学课程的教学现状和课程思政实践的重要意义，提出在密码学课程中贯穿哲学、美学和爱国主义等人文素质教育，进行课程思政的实践，具体阐述哲学教育、美学教育、爱国主义和民族自信心教育在教学中如何运用，旨在以人才培养为核心，以立德树人为根本，实现学生德智体美全面发展。

关键词：密码学；课程思政；哲学教育；人文素质教育
DOI:10.16512/j.cnki.jsjjy.2019.03.001

0　引　言

进入 21 世纪，科学技术发展突飞猛进，知识经济初见端倪。各国的竞争日益体现为以科技、经济为基础的综合国力的竞争。综合国力的竞争最终取决于各类人才的竞争。教育在人才竞争中处于基础地位。我国的目标是在 21 世纪实现中华民族的伟大复兴，这一目标的实现很大程度上依赖于我国高等学校培养的人才——未来的社会主义事业建设者和接班人。因此，我国高等教育的一个核心任务是培养德智体美全面发展的人才，根基在于立德树人。习近平总书记在全国高校思想政治工作会议上明确指出，要坚持把立德树人作为中心环节，把思想政治工作贯穿教育教学全过程，实现全程育人、全方位育人；中共中央、国务院《关于加强和改进新形势下高校思想政治工作的意见》指出，要将思想价值引领贯穿教育教学全过程和各环节，要加强对课堂教学和各类思想文化阵地的建设管理，充分挖掘和运用各学科蕴含的思想政治教学资源。

“课程思政”理念正是对上述要求的积极回应，也是当前形势下深化高校思想政治教育改革、全面提升教育实效所进行的有益尝试。高等教育以人才培养为核心，以立德树人为根本，其重心是实现学生德智体美全面发展。这一目标的实现有赖于高校所有学科与课程的共同作用，需要各类课程的协同合作，发挥思想政治教育作用。这就特别需要教师在课堂教学中，不仅要注重学生知识和能力的培养，更要做好学生思想引领和价值观的塑造工作。多位学者对思政课程和课程思政进行了探讨 [1-2]。

密码学是各类高等院校本科生信息类、数学类和计算机类等专业竞相开设的重要选修课，也是信息安全专业的主干基础课。开设密码学课程的各高校对密码学课程内容的设置、教学方法的改革及教材建设进行了有益的探索，取得了丰硕成果 [3-5]。笔者所在的教学团队自 2005 年起一直负责南京理工大学密码学课程的教学工作，在近几年的教学中，团队不断探索密码学课程中所体现的人文与科学思想，进行“课程思政”实践，取得了一些经验。在文献 [6] 中，笔者总结了密码学课程教学中可穿插科研方法论等科学素质教育。

1　密码学教学中的哲学教育

辩证法三大规律，即对立统一规律、量变质

基金项目：2018 年教育部产学合作协同育人项目“北京安码科技产学合作协同育人项目之信息安全课程（教材）体系建设”；2017 年南京理工大学高等教育教学改革研究立项课题（2017-B-23）。
第一作者简介：窦本年，男，副教授，研究方向为密码学，benniandou@163.com。

变规律、否定之否定规律，在密码学课程处处得到体现。

1.1 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。

1.2 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。

1.3 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 密码学教学中的美学教育

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如下一些方面。

2.1 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。

2.2 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。

2.3 公式的简洁深刻美

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，也能感受到公式的深刻、简洁之美。

2.4 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爱情故事。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。另外，还可以说说密码学家在追求去中心化，实现某种程度的自治中，最终构造出了去中心化的货币——比特币的历史。此外，还可以讲述一些关于比特币之父中本聪身世的未解之谜。

3 密码学教学中的爱国主义、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。现代密码学（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。不过笔者认为在密码学教学中可从以下两方面着手。

3.1 尽量发掘课程中由中国人提出的理论或思想

诚然，现代密码学（包括课程中用到的数学）的基本理论大多是西方建立起来的，这会让学生对中国人的数学天赋有怀疑。事实不是这样，中国人是有数学天赋的，并且具有很高的数学天赋。比如，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”。再比如，讲数论基础知识时，可以告诉学生“中国剩余定理”（称之为孙子定理）是整个数学中少数几个以国家名字命名的定理。同时可以告诉学生关于孙子定理的诗，即著名的“三人同行七十稀，五树梅花廿一枝，七子团圆正半月，除百零五便得知”，并以此诗和学生做猜数游戏，以便告诉学生诗句对应的算法。

了解到这些素材后，学生会发觉中国的数学一直是领先的，只是由于一些原因在近代落后了。这样，学生的民族自信心在得到加强的同时，更感责任重大，更加自觉地为祖国科技事业的发展加倍努力。

3.2 给学生讲一些密码学家的事迹

中国的许多数学家和密码学家身上都流淌着深深的爱国血液。比如民国时期破译了日本密码的池步洲。1937 年，“七七事变”爆发，怀着深深的民族责任感，池步洲放弃了在日本的安定生活，带着妻子和 3 个孩子毅然回国，侦收日军密电码，并负责研译。当时年仅 30 岁的池步洲，深感情报的重要性，用无比热枕的救国情怀投入到工作当中，池步洲通过破译截获的一份由日本外务省致驻美大使野村的特级密电，得出了日军将要袭击美国珍珠港的计划。再比如，中国最出色的密码算法专家章照止是一个先天视力障碍的半盲人，20 世纪 60—70 年代为国家破译国际情报密码方面作出卓越贡献，被人称作“中国的眼睛”。给学生讲这些密码学家的事迹，能感染学生，在他们心灵深处烙下深深的爱国印。只要大学生心里时刻装着祖国，中华民族的伟大复兴指日可待。

4 结 语

笔者所在教学团队近些年一直负责南京理工大学密码学课程的教学工作，我们在实际教学中将人文教育融入课程教学中，在学科内容教学的同时，对学生进行哲学、美学和爱国主义等人文素质教育。这些实践，取得了良好的教学效果。所教学生不仅获得过校“百篇优秀设计”和全国密码技术竞赛一等奖等科技奖项，而且能树立起

（下转第7页）

的新成果来讲解。在连续两年的全国科普讲解大赛中，武警工程大学的选手均选择了学科前沿性知识，如二维码、大数据安全、电磁泄漏和区块链，这些主题与当前的热点问题或重要研究领域紧密结合，体现了前瞻性与较强的专业素养。

案例 4：目前最火的互联网技术莫过于区块链，但大部分人只知道这个名词而已，由于底层理论知识的欠缺，要理解该技术的细节可以说困难重重。2018 年全国科普讲解大赛中，选手孙京键从网络购物引出交易的可靠性问题，又从借钱这样一件生活中的小事入手阐述区块链分布式存储的本质，并借助于动画表现区块链的概念，即便是外行也一听就懂。

4 结 语

科学普及是提高公民科学素养的主要渠道，而科学素养是实施国家创新驱动发展的战略基础。今天，互联网与新媒体技术的结合正改变着传统的学习方式，网络平台的普及应用更使大学的优势资源得到整合，促进科学教育的社会化。在这样的时代背景下，科普讲解的发展也走上了快车道。作为从事密码学教学科研的基层科技工作者，我们应担负起社会责任，积极投身于密码学与信息安全的科普工作中，充分利用丰富的知识和在讲台上锤炼出的讲课功底，用生动有趣的方式阐述密码学，让普通大众了解密码，掌握密码并熟练使用密码，最终让科学知识造福人类。

参考文献：

[1] 朱才毅. 科普讲解新理念及实践研究[M]. 广州: 广东教育出版社, 2018.
[2] 邱成利, 刘文川. 提高科普讲解能力的方式与途径初探: 基于全国科普讲解大赛的分析[J]. 科普研究, 2015(1): 5.
[3] 王后珍, 张焕国. 密码学课程建设及教学方法探讨[J]. 高教学刊, 2016(4): 22-24.

（编辑：孙怡铭）

（上接第3页）

健康的婚恋观、正确的是非观，在面对复杂的国际形势，能时刻保持清醒的政治意识，不少学生向我们反馈，他们自感责任重大，会更加自觉地为国家安全、社会发展和民族复兴而奋斗终生。

参考文献：

[1] 高德毅, 宗爱东. 从思政课程到课程思政:从战略高度构建高校思想政治教育课程体系[J]. 中国高等教育, 2017(1): 43-46.
[2] 邱开金. 从思政课程到课程思政,路该怎样走[N]. 中国教育报(2017-03-21).
[3] 李梦东.《密码学》课程设置与教学方法探究[J]. 北京电子科技学院学报, 2007, 15(3): 61-66.
[4] 射绒娜, 郑秀林, 李子臣. 密码学课程实践教学体系探索[C]. 第九届中国通信学会学术年会论文集, 2012: 472-475.
[5] 张瑞霞, 唐成华, 唐麟. 密码学实验教学改革应用实践[J]. 计算机教育, 2013(5): 68-71.
[6] 窦本年, 许春根. 密码学课程的科研方法论教育探究[J]. 计算机教育, 2018(3): 18-21.
[7] Katz J, Lindell Y. Introduction to modem cryptography[M]. Florida: CRC Press, 2008: 1-534.

（编辑：孙怡铭）