The Course Construction and Educational Reform of "Fundamentals of Cryptography"

HU Wei，WU Xiao-ping，QIN Yan-lin
Department of Information Security, Naval Univ. of Engineering, Wuhan, China,430033
Huwei-1212@126.com

Abstract: Firstly the important status of "Fundamentals of Cryptography" course in information security subject is emphasized. And the basic teaching concept and characteristic of this course are introduced. Secondly the course Construction and educational reform for recent years are summarized. Finally some deficient aspects for this course Construction are given. It must be some help for improving on the teaching quality of this course.

Keywords: Cryptography; Information Security; Course Construction

"密码学基础"课程建设与教学改革

胡　卫，吴晓平，秦艳琳
海军工程大学信息安全系，武汉，中国，430033
Huwei-1212@126.com

【摘要】本文强调了"密码学基础"课程在信息安全学科的重要地位，介绍了我校"密码学基础"课程的基本教学理念和特色，然后将近几年该课程建设和教学改革的经验进行了交流，指出了课程建设的不足和尚需改进方面。希望对提高"密码学基础"课程教学质量具有一定的借鉴意义。

【关键词】密码学；信息安全；课程建设

1 引言

21世纪是信息的时代，信息成为一种重要的战略资源。信息的安全直接关系到一个国家的政治稳定、经济发展和社会进步。为加强对信息安全人才的培养，我国教育部、科技部、信息产业部、国防科工委、国家自然科学基金都把"信息安全"作为优先发展的领域。2001年以来国内已有50多所高等院校建立了信息安全本科专业，部分院校还设立了信息安全相关的硕士点、博士点。

密码学是一门研究密码编制、密码分析和密钥管理等内容的综合性应用科学，是信息安全的基础和核心。因此绝大部分院校在各自的信息安全专业人才培养方案中都将《密码学基础》课程作为一门专业必修课。作者自本校 2004 年设立信息研究与安全本科专业以来，一直负责《密码学基础》课程教学和建设，积累了比较丰富的建设经验，希望能与大家分享。

2 课程特色与基本理念

《密码学基础》课程遵循素质教育、创新教育指导思想，课程教学突出"以人为本"，从关注教转向关注学，突出学员学习的主体地位。教学过程中以激发学员积极性和创新思维为主，在教学过程中注重密码学理论和实际应用相结合。在教学的同时，加强学员思想政治教育，引导学员树立良好的道德规范，为今后的任职打下坚实的专业技术和政治思想基础。课程组在教学过程中做到了五个注重：

（1）注重教学内容与教学方法的改革。从设置《密码学基础》课程以来，我们依据"少、精、严"的指导思想，广泛参考军内外同类课程教学内容的选取和安排，紧密结合本专业学员的知识结构和学习特点，精心选择了适合本专业需求的教学内容。为激发学生对密码学课程的学习兴趣，在教学中注重介绍密码学在信息安全和网络安全中的应用实例。同时，针对该

课程内容具有知识面宽、课程教学信息量大、更新速度快的特点，在教学过程中及时补充最新的教学成果和应用案例，充分运用现代化教学手段，注意开展启发式、讨论式、研究式教学，以理论教学为引导，以课程实验和习题为手段，极大地调动了学员的学习积极性和主观能动性，教学效果优良。

（2）注重学生创新素质与自我学习能力的培养。在计算机技术和网络技术飞速发展的信息时代，对信息安全的认识已不能只停留于基本理论，对信息安全的教育也不仅仅是知识教育，更是一种创新素质教育。在传授基本知识的同时，我们注意结合实际，传授在信息安全研究和应用中所产生的一些新的教学成果和最新的信息安全发展状况，培养学员的创新性思维，激发学员对本门课程的学习热情，增强学员的自我学习能力。同时加强实践性环节，在各章设置了必要的实验和习题，供学生操作和训练。实践表明，相关实验和习题是培养学生综合运用所学知识，提高分析解决实际问题的意识、兴趣和能力的一种有效手段，是提高学生自我学习能力的重要途径。

（3）注重教师自身素质与能力的提高。教师队伍的素质与水平，决定着教育活动中人力开发的质量与效率。近年来，通过建立并实施组长负责、以新知识吸收能力强的中青年骨干教师为主讲的组织制度；建立并实施集体备课、分段查评、考教分离的工作制度；建立并实施以督导与专家听课和学员网络评教相结合的考评及奖惩制度，密码学基础课程组教师的教学水平和教学能力得到显著提高。同时鼓励教员到地方和军队重点高校进修、培训或攻读博士学位，极大地提高了教员的专业素质和教学科研能力。

（4）注重教学研究和科学研究相结合。积极开展教学研究和装备科研，有多项科研和教学成果获奖。并注重科研成果和教学成果的相互转化。近几年，由课程组主持和参与的科研项目有22项，其中国家自然科学基金2项，教育科研5项，装备科研15项。通过科研课题的研究，加强了密码学基础知识的应用，也提高了教员的科研学术水平，促进了教学质量的提高和学员素质能力的培养。

（5）注重为人师表、教书育人。在搞好教学工作的同时，注重与学员之间的思想交流，及时的发现和帮助学员解决学习上、思想和生活上存在的问题，及时的做好学员的思想政治工作，使学员树立正确的人生观和世界观。注重为人师表、言传身教。

3 课程建设规划与教学改革

3.1 课程建设规划

课程建设目标：将密码学基础课程建设成为军队院校精品课程。

课程建设实施步骤：

- 建立结构合理、学术水平较高、相对稳定的师资队伍；
- 优化课程体系、改革教学内容；
- 全面制订（或修订）课程标准，规范教材的编选；
- 编写完整、规范、不同层次的高水平教案。
- 建设配套实验室和实作环境，改革教学方法和手段；
- 抓好教学管理，完善题库建设、逐步实现考教分离；

（1）教学队伍建设。针对该课程在信息安全专业课程中的核心地位，我们及时进行相关知识的更新，鼓励教员及时充电，聘请知名专家教授不定期讲座，派遣部分教员去比较知名的学校接受相关知识的学习和培训，以期在学术水平和理论深度方面有更进一步的提高。送派部分教员不定期到相关单位进行网络信息化建设，加强与业务部门的沟通，同时增强在军队信息化建设保障中的实践经验。

（2）教学内容组织。在教学内容的设计和安排上，主要采取由浅入深，先介绍与密码算法相联系的信息安全数学基础的知识，然后结合各种密码体制在信息安全业务中所起的作用，逐步深入，讲解具体的加、解密算法。同时，在分层讲解上对内容进行了优化组合，将某些较难的章节作为学生毕业设计内容或是组织学生参加全国大学生信息安全竞赛，这样的安排有利于培养学员对密码学研究、应用和创新的能力。

978-1-935068-09-9 © 2010 SciRes.

（3）系列教材建设。根据密码学基础教学的特点以及信息安全相关专业学生的培养目标，为了符合部队信息化建设中网络与信息安全建设的实际需要，已编写出版三部与密码学相关的教材:《密码学基础》、《密码学》和《密码新技术与应用》。辅助教材陆续使用的教材有武汉大学出版社出版的《密码学引论》；北京邮电大学出版社出版的《现代密码学基础》；科学出版社的《现代密码学》；电子工业出版社的《应用密码学手册》和机械工业出版社的《应用密码学》等。

（4）教学配套建设。收集整理了大量密码学图片视频资料，制作了精美的多媒体课件，整个教学过程中能向学员演示加密、解密、密码通信过程等，使学员将抽象知识具体化。教学直观易懂。建设了专用的实验机房，购置了相应的密码学基础实验软件，满足密码学课程教学的需要，同时还在自主开发密码学综合实验平台，不断完善密码学实验课程体系。具有代表性的演示实例，能够帮助对密码学理论知识的理解。

（5）教学管理制度。坚持了集体备课和教学研究制度；坚持了教案检查与新教员试讲把关制度；坚持了到学员队调研座谈制度；坚持了定期召开教学形势分析会制度；坚持了以老带新、听课检查、辅导答疑、作业批改制度；坚持了教改创新制度；坚持了课程结束时讲评、总结分析制度以及考教分离制度。对教学资料实行专人、专柜负责管理，建立教研室内的教学网络，对课程建设的文件资料及电子文档资料进行网络管理，实现资源共享，以利于资料交流。

3.2 课程教学改革

在内容安排上，重点突出，难易适宜。针对现代密码技术的不断更新和发展特点，不但拓宽学员的知识范围，紧跟现代密码技术发展步伐。**在课堂授课中，解决问题，充分利用。**学员课前预习，课堂上抓好“教”和“学”的互动，课后要求学员对讲过的内容要复习，并且以所学知识为起点，查阅相关资料，拓宽知识范围。对课后的思考题要认真引导，以达到学员掌握所学知识和提高解决问题的能力为目的。**在教学手段上，讲授演示，手段多样。**不仅让学员从感性上认识所学的知识，而且能够比较深刻地去理解和掌握。**在考核方法上，灵活机动，比例合理。**采用平时成绩和期末笔试相结合的，按一定比重分配，最后得出总成绩。

4 结束语

经过近五年的教学，学校督导组对本课程课堂教学质量的评价较高，学员对该门课程的评价普遍较好。学员课程考试成绩分布正常，下图是近几年学员的考试成绩统计图。

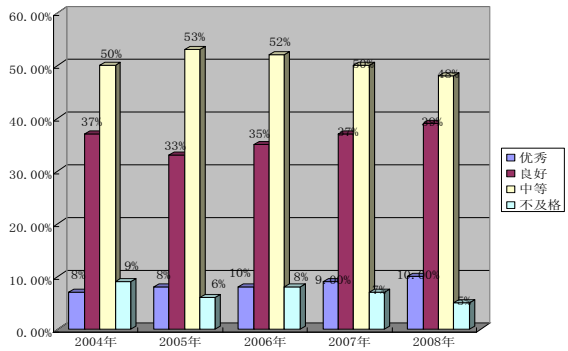

Figure1. Examination Results Chart
图1. 考试成绩统计图

虽然《密码学基础》课程取得了一定成绩，但是还有一些不足之处需要改进。需加强人才引进的力度，更好的落实教员进修培养计划；在教学内容体系方面需进一步系统设计；实验设备建设方面仍需要投入一定的经费，完善所有相关实验。相信再经过几年的投入和建设，《密码学基础》课程组会取得更好的成绩。

致谢

在这里首先感谢海军工程大学信息安全系主任吴晓平教授，对我的悉心指导。同时感谢与我共同完成论文的秦艳琳教员，在论文写作过程中给我很多帮助。

References (参考文献)

[1] ZHANG Zhao-zhi. Modern Cryptography[M]. Beijing: Beijing University of Posts and Telecommunications Press, 2004.
章照止. 现代密码学基础[M]. 北京:北京邮电大学出版社, 2004.

[2] ZHANG Huan-guo,Huang Chuan-he. Information security of undergraduate professional talent training and curriculum system [J]. Higher Education of Natural Sciences . 2004,(2).
张焕国，黄传河等.信息安全本科专业的人才培养与课程体系[J]，高等理科教育，2004，(2).

[3] Yu Li, Xu Shuang. Information security professional talent training mode innovation and practice teaching reform [J]. computer education ,2008,(23).

余琍，徐霜.信息安全专业人才培养模式创新思路与实践教学改革[J].计算机教育，2008，(23).

[4] ZHANG Huan-guo, Liu Yu-zhen. Cryptography Introduction [M]. Wuhan: Wuhan University Press, 2004.
张焕国，刘玉珍.密码学引论[M].武汉：武汉大学出版社，2004.

[5] Feng Deng-guo, Pei Ding-yi. Cryptography guide [M], Beijing: Science Press, 1999.
冯登国，裴定一.密码学导引[M].北京：科学出版社，1999.

[6] Wu Xiao-ping, Huang Wei. Cryptography [M]. Beijing: National Defense Infustry Press,2007.
吴晓平，黄魏等.密码学[M].北京：国防工业出版社，2007.

[7] Wu Xiao-ping, Qin Yan-lin. Mathematical foundation of information security [M]. Beijing: National Defense Infustry Press, 2009.
吴晓平，秦艳琳等.信息安全数学基础[M].北京：国防工业出版社，2009.

978-1-935068-09-9 © 2010 SciRes.