Exploration on the Teaching Methods of Modern Cryptography Course

WANG Hongli [1], ZHAO Guangfeng [2]

Department of Mathematics and Information Science,Tangshan Teachers' College, Tangshan, China

Email: tslily@163.com，

Abstract: Cryptography is an important basic course in information security and related profession. Based on the inherent characteristics of Modern Cryptography course, this paper discusses the teaching content and teaching methods of Modern Cryptography course, especially aiming at the information and computing science profession in our college and the practical situation of students. Firstly the existent problems are pointed out in Modern Cryptography course on aspects of course design, teaching contents, experiment course，practice and teaching form. Analysis on these problems is presented and the corresponding recommendations for improvement are proposed to improve teaching effectiveness, expand scope of knowledge, pay attention to experient course, organize students' practical activities and etc.

Keywords: Modern Cryptography; course design; teaching contents; teaching methods;

现代密码学课程的教学方法探究

王红丽 [1]，赵光峰 [2]

唐山师范学院数学与信息科学系，唐山，中国，063000

Email: tslily@163.com

【摘要】密码学是信息安全及其相关专业的一门重要基础课程。本文根据现代密码学课程的自身特点，针对我院信息与计算科学专业开设的密码学课程及其学生的实际情况，在教学内容和教学方法上做了探讨。首先从课程设置、授课内容、实验课程、实践环节及其教学形式上指出密码学课程存在的问题，然后分别对以上几个方面进行分析研究，并提出了相应的改进建议：要提高教学效率，拓展知识面、重视实验课程，组织学生实践等。

【关键词】现代密码学；课程设置；教学内容；教学方法

1 引言

随着互联网和通信技术的飞速发展，我们充分体验了信息共享带来的便捷服务，但同时信息安全问题也日趋严重。密码技术是信息安全技术的关键和核心，密码学为信息安全提供了深刻的理论依据和丰富的应用实践。它是集数学、计算机科学以及通信和信息系统等多个学科为一体的交叉学科。因此密码学课程的教学极其重要。现在很多高校的信息安全专业、信息与计算科学及其他信息类专业都开设密码学课程。但由于这一课程包含很多相对复杂的数学基础知识，如数论、抽象代数学、概率论、复杂度理论等，有一定的难度，使得学生学习起来比较吃力。而老师如何设置课程内容、采用何种教学方法和教学手段等能提高教学质量，这就急需我们去思考与探索。

根据我们学院信息与计算科学专业开设密码学选修课的实践经验和这门课本身的教学特点，本文在教学方法上进行了一些分析。

资助信息：唐山师范学院发展基金项目（07c17）资助

2 密码学课程存在的问题

我院信息与计算科学专业开设密码学课程时间比较短，所以从师资、课程设置、教学条件、实验环境等方面都还存在一定差距。

2.1 课程设置不太合理

密码学的核心基础是数学，特别是作为密码学重要基础支撑的抽象代数以及数论。而本专业的初等数

978-1-935068-09-9

论课程设置为选修课，因此在学密码学课程时就出现了学生数学基础参差不齐的现象，使得讲授密码学课程时具有一定的困难。如再补授基础知识，又占用大量宝贵的时间，影响后面课程的进度。

2.2 授课内容没有拓展

现在授课内容基本以书本知识为主，主要对课本上的算法进行描述分析。不太注重知识的更新，有关算法的最新研究成果，比如算法的改进等介绍偏少，这样使得学生无法了解到前沿知识，学到的总是落后于实际应用的技术，无法与社会接轨。

2.3 未设置实验课程

密码学是一门理论性较强的课程，但同时也是一门实践性很强的课程。而我院并未设立相应的实验课，还处于完全理论教学阶段，使得理论与实践相脱节。学生被动的学习枯燥的理论，从而遏制了学习密码学的热情，学生不能了解所学知识在实际生活中的应用情况，也无法提高解决实际问题的能力。

2.4 教学形式比较单一

主要是以课堂教学，教学手段用黑板或课件。老师讲，学生听。缺乏灵活性和多样性，这样的方式难以调动学生的积极性，也无法与实际相结合。

3 教学方法探讨

针对我专业存在的以上问题，我觉得密码学课程的教学方法改革势在必行，并提出以下建议：

3.1 对本专业课程设置需要进一步改进

密码学在课程安排上应当先修初等数论和抽象代数课程，当然最好还具有计算复杂性理论的知识。这样学生具有密码学的数学理论基础，水平相当，不用再占用有限的课时，也有益于后期教学工作。

3.2 教学内容要有重点、提高教学效率

结合我专业现行的教学要求，教学内容主要包括：密码学概论、古典密码学、序列密码、分组密码、公钥密码、数字签名和认证。由于密码学涉及面广泛，又要求有较高的数学基础，再加上上述必需内容，就决定了密码学课程必然包含了庞杂的教学内容。而课堂学时数是有限的，要完成全部内容的教学，让学生掌握概念学会应用存在一定困难。所以必须合理地组织教学内容，加强教学方法的改进。采用灵活丰富的教学手段，能够突出重点，提高教学效率。 由于课时少，难以对每种方法都加以详细介绍，可以采用比较教学法。有重点、有选择的详细讲解具有代表性的经典算法。而对其他同类别的加密方法做一个简单介绍，让学生对这一类方法有一个总体的了解，触类旁通。必要时，可应用一些研究工具软件，使教学效果和质量得到提升。总之，做到有目标、有层次、有重点的教学。

3.3 注意拓宽学生在本课程方面的知识面

由于科学总是在实践中不断地发展，密码学新方法、新技术、新进展不断涌现。比如量子密码学、信息隐藏等方面。应该在课堂上对这部分内容加以介绍，或者可以请专家作报告，以专题形式介绍密码学方面的前沿和进展，并组织学生讨论。使学生真正了解密码学在实际生活中的应用，拓展学生知识视野，接触前沿分支，展现密码学的总体轮廓，使学生更深地了解密码学与其它学科之间的联系。这就更需要提高教师自身的教学水平，有必要时可以进修学习。

3.4 注重理论，但更要重视相应的实验课程

密码学的目的是为人们提供可靠的密码技术来解决现实生活中的信息安全问题，因此要对密码学的实验教学环节予以高度的重视。本课程中可以设置实验的内容有古典密码体制、序列密码体制、分组密码体制、公钥密码体制以及数字签名等。如对 DES 对称加密的实现和相关性质的验证、RSA 公钥密码的实现及简单的密码学分析、密码学系统的设计与分析等。在教学中应为学生提供模拟实验室、设置一些相应的问题，通过不断地模拟训练巩固学生的知识，也能够通过实验教学来培养学生能力。使学生学完课程后，对密码学的原理、思想和算法都有清晰、深入的理解。让学生通过多个密码算法的程序设计实现，更好地掌握密码算法设计的机理和方法并能掌握密码学系统设计的基本方法和步骤环节。也可以对某些算法展开讨论，谈谈自己对这方面的认识以及在生活中的应用。为完成上述基本目标，需建立一个细致、规范的实验教学模式。学校也要大力加强实验室建设，为学生提供良好的实验环境。

3.5 组织实践活动

鼓励学生组织团队设立创新项目，在老师的指导下让他们独立完成一些力所能及的项目。尽可能让学

生参与实践活动，使学生充分了解密码学在实际生活中的应用。比如加密技术、签名技术在电子商务、银行证券等行业中的应用。如有条件还可以让学生亲密接触密码产品，如加密机，了解它们的工作原理或带领学生参观上述行业中的密码系统运行状况，通过这些环节来提高学生的学习兴趣，从而提高学生适应社会的能力，教学形式也实现了多样化。

4 总结

密码学课程作为信息与计算科学或新兴的信息安全专业的一门重要课程，对于密码学课程的教学一直是有关专业教师关注的核心内容。本文针对本院密码学教学情况进行了总结，给出了教学方法的改革建议。但由于教学经验不足，还需要具体深入探讨如何把实验教学融入理论教学，如何采用有效的多样化教学 ，如何更好地安排教学方法，如何调动学生学习积极性等这些实际问题。这些都是提高我专业密码学课程的关键问题，亟待解决。

References（参考文献）

[1] Chen Lusheng，Shen Shiyi, Modern Cryptography[M], Beijing: Science Press,2002
陈鲁生、沈世镒，现代密码学［M］，北京：科学出版社，2002

[2] Yang Yixian,Sun Wei,Niu Xinyi,The New Theory of Modern Cryptography[M], Beijing: Science Press,2002
杨义先，孙伟，钮心忻，现代密码新理论[M]，北京：科学出版社，2002

[3] Feng Dengguo,Cryptography Theory and Practice[M], Beijing: Publishing House Electronics Industry, 2003
冯登国译，密码学原理与实践［M］，北京：电子工业出版社，2003

[4] Li Zhijun, Liao Minghong, Study on the teaching of cryptography course[J],*Computer Education*,2006.9. P28-30.
李治军、廖明宏，密码学课程的教学研究[J]，计算机教育，2006.9，P28-30.

[5] Shen Ying,Chen Zhiyang,Multi-level teaching practice of cryptography[J], *Computer Education*, 2007.12, P85-88
沈瑛、陈志杨，密码学多层次教学实践[J]，计算机教育，2007.12, P85-88.

978-1-935068-09-9