Cryptography Course Research and Practice for Junior College

SHANG Yan-hong[1], WANG Xiang[2]
1. *Computer Science Department, Tangshan Teacher College, Hebei Tangshan, China*
2. *Computer Science Department, Tangshan Teacher College, Hebei Tangshan, China*
1. *yh_shang@126.com*, 2. *tswang@126.com*

Abstract: Cryptography is an important basic course for information security. In the paper, based on Tangshan Teacher College computer science department students and the cryptography course, the teaching situation is analyzed from theoretical teaching and practice teaching. At the same time, the teaching experience is summed up for junior college students: cultivating interest from the cryptology stories, selecting the important algorithms, computer experiment on cooperation, examination on daily.Teaching effect is better. Hope to provide reference for peers.

Keywords: Cryptography; Teaching Content; Teaching Methods

专科密码学课程的教学探索与实践

商艳红[1], 王　祥[2]
1. *唐山师范学院计算机科学系，河北唐山，中国*，063000
2. *唐山师范学院计算机科学系，河北唐山，中国*，063000
1. *yh_shang@126.com*, 2. *tswang@126.com*

【摘要】密码学课程是信息安全专业的一门重要基础课程。本文结合唐山师范学院计算机科学系专科学生实际情况及课程本身的特点，从理论教学和实践教学等方面分析了该课程的教学现状，总结了几点适合专科学生的教学经验：从密码故事培养兴趣，算法选择突出重点，上机实验注重合作，考核成绩看平时。教学效果较好，希望为同行提供一定的参考和借鉴。

【关键词】密码学；教学内容；教学方法

1 引言

目前，许多高校都相继开设了信息安全专业以适应安全需求，密码学作为其核心关键学科，是信息安全专业必不可少的必修课程[1,2]。然而，密码学是集数学、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[3]，而且，国内高校开设该门课程时间不长，尚无权威的教学大纲和授课范围，为本门课的讲授增加了难度。特别是对专科学生来说，本身数学基础较差，又喜欢学那些只需动手不需动脑就可完成的内容，而不注重理论知识的学习和积累，所以普遍反映密码学太深奥，太难学。如何在专科学生中较好地完成密码学的教学任务，是需要认真思考的问题[4,5]。

唐山师范学院从 2007 年为信息安全方向专科学生开设密码学考查课开始，直到 2010 年作为考试课，影响逐渐增强。笔者结合四年来自身的教学实践和计算机应用技术专业学生的知识基础，对教学内容和教学方法进行了一些分析和探索，使学生在对密码学知识系统理解的前提下，充分发挥计算机专业学生的专业技能，达到能够将该门课中的知识应用到实际的能力。

2 理论教学选内容

密码学所涉及的知识内容较广，且较深的数学知识尤为突出。这使得专科学生学习起来难度加大。因此，笔者认为在讲授内容上须从学习兴趣上加以重点培养，算法难度上略有降低，笔者在教学内容的选择中注重以下几个方面。

2.1 注重历史讲故事，激发兴趣是关键

任何一门新课都会从学科发展背景开始，密码学

也不例外。笔者在从简单的照本宣科到目前绘声绘色的介绍，最大体会就是，不能忽视第一节课。利用好这一节课，使得学生的兴趣高涨是整个学期的敲门砖。在教学过程中，一般会把《密码故事——人类智力的另类较量》这本书推荐给学生，并以历史故事开头介绍密码学的发展背景，从玛丽女王的密码到维热纳尔密码，从密码盘到恩格玛机，借助于多媒体教学中丰富的图片，逐步过渡到密码学研究的基本问题上来，尤其是密码体制、单向函数等的简单阐述，既让学生对密码学有一个大致的了解，又为以后即将学习的各种加密方案以及密码安全性做好铺垫。另外还需着重介绍一下密码学贴近生活的主要用途，让学生认识到密码学不只是存在于故事中的战争里，也存在于学生身边，从而激发学生的学习兴趣。

自采用此种方法讲授的两年来，学生在第一节课感受到的是新奇是惊喜，自然会紧跟教学，一探究竟。除此，在下课之前，让学生及时总结所学，提出下一步学习展望，以期兴趣的长效性。

2.2. 古典密码不能省，打下基础最重要

有了兴趣只能算是第一步，密码算法是整门课重点。而古典密码作为算法入门，一定不能忽视。麻雀虽小，五脏俱全。它提供了密码算法的两种思想——代换和置换。故此非常重视古典算法的讲解，这也是专科学生最易听懂的部分，也是最基础的部分。在讲授过后，一定结合上机编程，重点理解。

2.3. 现代密码讲经典，DES、RSA 不能少

密码学的核心就是现代密码。由于针对专科学生，所以我们采取重点讲授分组密码 DES 和公钥密码 RSA，配以算法步骤图片和动画演示，充分利用多媒体技术，同时，以程序执行给出具体加密效果，让学生掌握现代密码的加密思想。之所以选取这两个算法重点讲解，一是算法较易理解(DES 就是古典算法的两种思想，承前)；二是算法用途大（RSA 是公钥的代表，也是后续密码应用的重点，启后)。其他算法也作为讲授内容，一般采取学生自学、资料查找、上课互动的方式进行，开拓知识点。

2.4. 密码体系须把握，理清脉络一线穿

有了以上内容，只能说密码算法稍微掌握，理清课程脉络才算真正学会。接下来，我们帮助学生整理密码学，从各个技术解决的安全问题上，理清思路。以下是总结的密码学知识体系框图。

Table 1. the **knowledge system of cryptography**
表 1. 密码学知识体系表

章节	内容	作用
密码算法	借助密钥，完成信息的保密	看不懂了吧？
密钥管理	为使算法安全，对密钥进行管理	钥匙安全吗？
Hash 函数	确保网上数据传输的完整性	信息完整吗？
数字签名	保证网上数据传输的不可抵赖性	是我的？
身份识别	确保网上数据传输前的身份辨别	你是谁？
PKI 技术	可信第三方的相关技术	谁公正？

通过以上知识体系表格，学生明白密码学的讲授内容，同时帮助学生归纳总结各种技术的作用，使学生的知识得以融会贯通。

3 实践教学重收获

计算机应用技术的学生不同于通信和数学专业的学生，他们的长处在于较强的程序设计能力。然而专科学生底子薄，不能要求他们全部编程实现所学算法，但也不能不重视实践教学，由于我院学生密码学的前导课中开设了 C 语言，所以编程环境为 C 语言，给出新的密码学实验素材，使学生在巩固上学期所学的基础上，更加认识 C 语言的重要。故此，我们在上机实践这一块是这样安排的。

3.1 古典密码算法独立编

古典密码算法选出凯撒密码、移位密码、单表代换密码为必做题目，一人为一组，撰写实验报告，要求重点写出自己的收获。对于学习能力强的学生，给出几个备选算法，例如，维吉利亚密码、Playfair 密码、利用频率统计破译移位密码等。

通过以上方式，绝大多数学生能主动独立完成必做题目，可喜的是，在有了编程兴趣的基础上，有部分学生还给出了算法的改进，可见学生不但理解了算法，也实践了算法，更驾驭了算法。

3.2 现代密码算法需合作

由于现代密码算法本身较繁琐，加之目前很多环境中已有组件实现，又考虑专科学生编程能力和实践学时的局限性，这部分的上机，算法实现部分的源代码由教师提供，要求学生每 2-3 人为一组，尽量读懂分析代码，并应用到小组的程序中去，完成一界面友好的加密软件。这种上机实践方式，减少了编程工作量，但锻炼了学生合作能力，而这样的编程方式也是

978-1-935068-09-9 © 2010 SciRes.

目前各大公司的编程方式。学生的编程效率提高了，编程积极性提高了，学习效果逐步凸显，此种方式普遍受到学生的欢迎。

3.3 密码应用是重点

密码学上机实践的另一个非常重要的环节就是现有密码软件的使用，也是最贴近学生实际的部分。这部分重点使用密码软件 PGP，让学生体会密码在网络上信息安全中的作用，并重点强调该软件的各部分都是由课程所学组成，以此巩固总结整门课程知识点。

4 考核评价看平时

一直作为考查课的密码学，我们在考核机制方面给予了更多思考。考核机制旨在让学生减少学习压力，能比较轻松的通过，同时激励学生为兴趣和取得满意的成绩付出力所能及的努力。在这样的机制里，把考核分成 3 部分：1）平时成绩(主要考查出勤率或习题作业)，2）开放式上机实验考试成绩，采用小组答辩的形式为学生赋分，同时重视实验质量，把实验报告作为学生成绩评价的一部分，报告必须能清楚地描述实验过程和实验结果，并给出合理的解释，如实验结果不理想也应尽可能分析出错可能和改进方向等，鼓励学生重点总结出实验收获。3）附加机动分数，机动分主要由教师结合教学内容，选择部分有趣的加解密方法、算法分析等作为备选题目，学生可以根据兴趣、难度决定是否参与。对于完成较好的学生及对于算法有所创新的学生另附机动分数，激发学生兴趣。

以 2008 一 009 学年第二学期为例，参与密码学的 58 位学生，平均得分 81，总评分 85。从教学反馈来看，学生们系统地掌握了该门课的知识，对于这种考核方式大多感到满意、乐于接受。

5 总结

密码学在我院为专科学生已讲授四年了，笔者根据教学实践和学生特点，给出了理论教学内容和实践教学内容，充分发挥了学生的专业优势，尽力激发并维持了学生的学习兴趣，通过可行的考核机制看，取得了较满意的教学效果。下一步要做的是研究如何进一步优化实践教学的内容设计，提高学生的多学科整合能力，加强整体专业素质的培养。

致　谢

非常感谢北方工业大学邹建成导师的帮助，感谢唐山师范学院计算机科学系信息安全教研室同事的大力支持。

References (参考文献)

[1] Chen Lusheng,Shen Shiyi Modern cryptography[M] Beijing: Science Press, 2002.3−20.
陈鲁生,沈世镒.现代密码学[M].北京:科学出版社, 2002.3−20.

[2] Yan Bo. Modern cryptography[M] Beijing: Tsinghua university press,2003.4-25.
杨波.现代密码学[M].北京:清华大学出版社,2003.

[3] Shen Ying,Chen Zhiyan Multilevel Teaching Practice in Cryptography[J],*computer education,* 2007，(2), P85-88(Ch).
沈瑛，陈志杨．密码学多层次教学实践[J].计算机教育，2007，(2), P85-88(Ch).

[4] Ding Yong An exploration of the teaching of cryptography in the discipline of information and computational science[J], *Guilin university of electronic science and technology journal,* 2008，(2), P131-133(Ch).
丁勇．信息与计算科学专业密码学教学研究[J].桂林电子科技大学学报，2008，(2), P131-133(Ch).

[5] Zhang Xinglan, [J],*computer education,* 2008，(8), P85-86(Ch).
张兴兰．信息安全专业的密码学教学[J].计算机教育, 2008，(8), P85-86(Ch).