

The cryptology teaching discuss

ZHAO Yong-chi, ZHAO Gang

computer center Mianyang Normal University, Mianyang, China

zhao0426@yahoo.com.cn, zhghunter@163.com

Abstract: The paper had first expounded the study cryptology curriculum needs very many aspects the elementary knowledge, next has carried on the analysis to the cryptology curriculum, then proposed should adopt four kind of teaching strategies in the teaching process: Transfers the initiative which the student studies to coordinate the teaching the smooth development, certainly requests the student positive participation, may achieve between teacher and student's interaction, completes the teaching task smoothly; In the teaching process wants the unceasing induction, the contrast, the summary, but also needs to carry on the language in the teaching process to temper, the simplification is main, simultaneously requests to reduce a hall curriculum the teaching time; The stationary point simple duty lets the student ponder that, is advantageous in the student cryptology knowledge consolidated and the deepening; Needs to design from the shallow to the deep experimental technique to confirm studies the content, the final paper summarized the teaching improvement effect.

Keywords: Cryptology education; Teaching design; Experimental teaching

密码学教学探讨

赵永驰, 赵罡

绵阳师范学院, 绵阳, 中国, 621000

zhao0426@yahoo.com.cn, zhghunter@163.com

【摘要】 论文首先阐明了学习密码学课程需要很多方面的基础知识, 其次对密码学课程进行了分析, 然后提出了在教学过程之中应该采取四种教学策略: 调动学生学习的主动性来配合教学的顺利开展, 当然要求学生积极的参与, 可以达到老师与学生之间的互动, 顺利完成教学任务; 教学过程之中要不断的归纳、对比、总结, 还需要在教学过程之中进行语言锤炼, 精简扼要, 同时要求压缩一堂课程的教学时间; 留点简单任务让学生思考, 有利于学生密码学知识的巩固与深化; 需要设计由浅入深的实验方法来验证所学习内容, 最后论文总结了教学改进的效果。

【关键词】 密码学教育; 教学设计; 实验教学

1 引言

近年来, 随着信息安全技术的逐步深入人们的日常生活, 同时对信息安全理论知识的不深入理解与实践的运用, 对其研究的深度与广度都有很大幅度的提高。密码学作为信息安全的最核心技术, 可以利用它来保障信息的私密性、认证性、完备性和不可否认性等。密码学的基础知识作为信息安全的核心理论, 越来越多的学生与学者进行了学习与实际应用的推广, 因此近年来《密码学》成为大多数高等院校计算机专业本科生相继开设的课程。绵阳师范学院在 2006 年面向计算科学网络专业其以后年级学生开设了《密码学》的学位课程。密码学建立在数论(尤其是计算数论)、代数、信息论、

概率论和随机过程的基础上, 间或也用到图论、组合数学等很多涉及数学方面的基础知识。现代密码学课程一般包含以下层次的内容: 第一, 古典密码学的基础。其包括古典密码体制、古典密码体制的分析, 该内容一般作为密码学的开始, 讲解该部分内容, 关键在于学生学习密码学兴趣提高的关键所在! 第二, 密码学的基本课题。包含有单向函数、序列密码、分组密码、公钥密码学、数字签名等许多密码学的基础知识。第三, 密码学的高级问题。包含有零知识证明、秘密分享、密钥管理等等问题。第四, 密码学的新应用。密码学提出了一个一般的学科领域都难以遇到的难题: 即它需要密码学和密码分析学紧密结合互为促进、互为发展的学科。

2 密码学课程分析

分析一下密码学课程状况：密码学主要分为密码编码学和密码分析学，两者相辅相成，相互矛盾又相互促进发展，对立又统一的一对不断迅速发展的学科。结合我校现行的教学基本要求，教学内容主要涉及到：密码学概论、古典密码、Hash 函数、序列密码、分组密码、公钥密码、数字签名和认证、密码协议等。理论学时大概有 60 学时，其中还包括实验课程。由于密码学本科课程开设的时间相对很短、积累的教学经验一般比较少，密码学新的应用不断推陈出新，而对大部分学生来说，学习密码学的目的在于实际的应用。如果学习密码学之后不知道如何在实际之中得到应用，所学习的知识就会感觉到空洞无味，同时也可能所学知识迅速遗忘。因此，需要重视实践教学，让学生在学完这门课程之后知道怎么用。关键是在现实生活之中的应用，让学生知道现实之中无处不涉及到密码学的应用，应用反过来有助于推进学习，学习反过来在现实生活之中找到应用的地方，增加学习的乐趣和动力！且《密码学》自身结构特点决定该课程涉及的知识面非常的广阔，比如涉及电气方面、数学方面、计算机知识方面、通信知识方面等等的多学科的知识涉及，其中在数学方面涉及到高等数学、近世代数、数论、信息论、算法分析等许许多多数学知识来作为应用，一般而言不同基础的非数学专业的学生学起来比较吃力，由于诸多原因，可能很快会产生一些畏难情绪，那么对老师的教学就可能产生巨大的阻碍，则教师教学进展也就会更加的困难重重，特别是在教学课时不充裕情况下就更加加大了教学的难度和教学内容取舍的难度，显而易见存在的教学问题亟待不断研究、不断总结、不断分析，从而解决并在实践教学方式方法中的诸多问题，故需要不断的进行教学的改进。

3 采取的策略

3.1 调动学习的积极性

首先要利用上第一次课堂的机会来激发学生对计算机密码学学习的热情。第一堂课开始就要以趣味做为导入，那样会激发学生强烈的兴趣。教师要根据学生的探索未知世界的热忱、对新鲜事物的希奇性、探究性的学生特点来设计教学内容，从而精心设计课堂的开端，教师要把第一次课堂的教学变成一种向寻求乐趣的活动，甚至可以稍微显示神秘性探究活动，开

场白就把学生的兴趣给勾引起来，从而有利于以后的教学策略开展。

其次引导学生自己动脑、动手，充分地调动学生积极主动学习，提高学习热情。学习密码学的过程是：首先是看，看老师演示非常简单的事例，这个是关键，学生通过简单的事例可以看清楚问题的所在，其次看一部分非常聪明的同学的演示事例，可以达到意想不到的作用，而后才是看书上的讲解！与此同时老师要把事例分析与教材的理论讲解相互结合、相互对比，让学生充分理解，这一步可以加深学生的信心与爱好，让学生的思维得到良性的循环，可以推进下一阶段的教学任务的完成；其次是让学生思考，思考就会寻求原因、寻求类别、寻求思维的延伸！最后一个环节是操作，要求学生自己动手来设计一个非常简单的事例，越简单越好，复杂的应当不鼓励，同时也不提倡，通过以上三个环节的不断深化的学习过程。学习密码学从一个个小小的量变过程到最终的一个质变升华，学生会产生浓厚的学习兴趣，最终完成对密码学领悟，达到一种醍醐灌顶的感觉，从而能够充分利用密码学来解决现实生活之中的一些小问题或者能够应用密码学的一些知识来设计问题，那么为后续的网络安全课程奠定好基础，同时也是为了学生在网络安全方面的发展奠定一定的良好基础。

第三让学生学习密码学的实践应用，是保持学生学习积极性长时间起作用的关键因素。教师要利用各种有利的机会结合实际情况或者社会新闻来引进密码学的教学设计改革，不断向学生进行展示学习密码学的有用性教育，使学生明确学习密码学带来的实际应用价值与娱乐价值，不断激发其学习密码学的动机。在教学过程中，教师可以经常展示一些很有价值的密码学知识的意义和重要性，关键是通过一些举例来解决生活之中的实际问题，从而知道学习到的知识能解决什么实际问题，让其感受到生活中处处有密码学的知识存在。例如以古代的藏头诗来分析，同时也可以加入密码分析！又如以《银行存款被盗》的社会新闻为例，分析其被盗原因等等，让学生了解生活之中的密码学学问，这样可以提高学生的学习积极性，从而改善教学的效果！

最后还要与学生进行情感交流，可以有效缩短学生与老师之间的距离，学生就会喜欢老师，从而也就更加喜欢老师的课堂，潜意识激发了学生的学习兴趣与学习动机，更加有利于密码学知识的接收与后续的

教学任务的完成。

3.2 改进教学策略

要改进理论课教学策略，密码学的思维延伸在于不断的归纳、对比、总结，如对各种公钥密码加密算法的对比、解密算法之间的对比，以及能否由此及彼之间的内推得到关系之间的串联。又如对分组密码之间的对比，能否达到记住 DES 加密体制，就可以很容易记住 AES 的加密体制，关键在于事例的对比以及事例之间的对比而产生的不同点以及相同点，对于学习分组密码学的掌握是很有帮助的。

其次要语言锤炼，精简扼要。上理论课程时教师必须锤炼自己的语言使用技巧，不断提高语言的简洁性，例如就解释什么是单向函数，教材的定义如下：

一个函数 $f: \{0,1\}^* \rightarrow \{0,1\}^*$ 称为强单向函数，若下列两个条件成立：

(1) 计算 $f(x)$ 是容易的，即 $f(x)$ 是多项式时间可计算的；(2) 计算 $f(x)$ 的逆 $f^{-1}(f(x))$ 是困难的，即对每一多项式时间概率算法 M' ，每一正多项式 $p(n)$ 和一切充分大的 $n(n \geq n_0)$ 有 $\Pr\{M'(f(U_n)) \in f^{-1}(f(U_n))\} < 1/p(n)$ 。

学生看见如此的定义，不一定很感兴趣，再一看 $f(x)$ 是多项式时间可计算、对每一多项式时间概率算法 M' 、 $\Pr\{M'(f(U_n)) \in f^{-1}(f(U_n))\} < 1/p(n)$ 等可能迅速产生不好的印象，可能阻碍了教学。那么可以举一个简单的例子如：打碎一个酒杯是很容易的，但是把一堆碎酒杯渣还原成一个酒杯，就是非常困难的一件事情！

教育教学过程中实际是师生双方思维活动一种交流的过程——教师将教学内容化为精简语言传授给学生，让他们深刻理解，并且产生感情上的共鸣。这要求教师在教学过程之中要不断加强和提高自身的科学理论水平、自身专业水准和文化修养，追求丰富自身语言词汇、善于表达不同思想感情的语言方式，多学习与理解语法规则，对其能够灵活自如，争取达到给人一种醍醐灌顶的意境。

三是要压缩一堂课程的教学时间，因学生思维集中时间是有限的。稍微长了的教学时间，学生可能产生犯困，导致教学副作用产生。充分而且有效地利用教学课堂时间，是教学成功的关键点。一堂课的时间是有限的，并且最佳时间不过在上课的前面二十分钟左右，要根据学生的心里特点、生理特点、注意力集

中时间的长短等因素，需要精心安排教学的任务和教学的内容。最好的方式是学生的注意力、兴奋度相当高时完成教学任务与内容，达到质的突破。教授新的课程内容的时间最好是 20 分钟，如果一堂课时间长，可以采用分段时间授课，达到良好的效果，从根本上防止疲劳，可充分调动学生的参与意识。

四是改进教学过程之中的间断性，穿插一点其他有趣的内容或者讲一个笑话在教学过程之中，如果与教学内容紧密相连的话，则很好地让学生的注意力得到放松，同时可以让学生的注意力又很快的集中。

3.3 任务驱动法

任务驱动法的教学方式就是让学生从实际思考的问题作为出发点，先提出问题，后对问题加以分析，寻求解决问题的方法，从而在实际应用之中解决现实问题的一种过程中就不断地重现密码学的知识和加强密码学使用技能。该作用有利于培养学生的创新能力。

任务驱动法教学的具体操作是把学习过程设置成为简单的、有实际意义的问题场合，学生通过自我总结、自我查找资料、自我探索或者与他人互相合作来解决这些实际问题，逐渐发现隐含于实际问题背后的密码学知识，逐渐形成自己解决问题的能力，增强自主学习的能力，更好培养学习的思维能力，也就培养了学生的创新能力。在此过程之中，注意避免扼杀掉学生创新精神和创新能力，推进任务驱动法教学，可以有利于发挥学生的主体能动性，创造了平和、自由、和谐、均等、充满个体能动性的教学手段。在任务驱动法教学过程之中注意遵从教育规律，设计具有学生阶段性特点、课程教学内容特性的问题，才可以充分发挥学生追求目标、能够很好完成任务的积极性。要充分鼓励学生敢于打破常规、独辟蹊径的思路，这些都要给予充分的肯定与赞扬。

3.4 实验目的

实验操作是学习计算机密码学非常重要的一环，实验题目的制定上，密码学课程的实验教学分为基础验证实验和综合设计实验两个层次。基础验证实验主要是对课程教授内容中的基本原理进行设计实现，使学生能对所学内容全面掌握并加深理解，关键是老师给出非常简单的验证实验，最好可以通过笔算都可以进行验证，验证完之后，要求学生总结报告，下次的实验是在上次简单实验基础之上的稍微难的实验，同

时不要忘记了对其实验效果进行验证。一般而言计算机专业的学生具有编程基础,进一步的基础验证实验主要要求学生对具有代表性的古典加密算法和现代密码体制加密算法进行验证实现。其次是综合设计实验,要求学生能运用已学的密码学基础知识,以及结合其他课程知识,首先设计出一个简单的并且完整的具有一定的实际运用意义的系统,在实验课上可以要求学生在此基础之上修改完善该实验,达到一定的实验高度水平,充分体现计算机专业学习过密码学的水平,一般采用的题目是设计一个文本文件加密系统。如此这样的题目涵盖了现代密码算法的部分精华,同时也逐渐的加深密码学实验难度与提高学生密码学的水平。实践表明,基础实验与综合设计实验逐步深入有助于加强学生动手能力和创新能力的培养,同时锻炼了学生的思维和操作能力,激发了学生的学习兴趣,使学生充分发挥了学习主动性。

4 总结

密码学技术在不断迅速发展,应用领域不断加宽和不断推陈出新。对密码学的课程教学改革显然应该得到不断探索,通过教学方法的改进以及实践环节教

学的充分完善,保证课程的先进性和实用性,应用以上的教学方式方法,得到了满意的教学效果。改进教学的目的在于需要提出一种优良的教学方案:学习是一种娱乐,玩耍是一种学习,那么该教学方式是最佳学习方式,可以从根本上改变学生学习的积极性。

References (参考文献)

- [1] HELei, SUNTong, HUANG Chun. Research on experimental learning of cryptography course[J]. Beijing.P436-440.
贺蕾,孙彤,黄春. 中国电子学会第十六届信息论学术年会论文集[J], 中国电子学会第十六届信息论学术年会 2007. P436-440.
- [2] LI Meng-dong, The Course Design of Cryptology and Its Teaching Method [J], *Journal of Beijing Electronic Science and Technology Institute*, 2007, 9(2), P61-65.
李梦东.《密码学》课程设置和教学方法探究[J].北京电子科技学院学报, 2007, 9(2), P61-65.
- [3] FENG Deng-guo. Status quo and trend of cryptography[J]. Beijing: Journal of China institute of communications, 2002,5(23),P18-26
冯登国, 国内外密码学研究现状及发展趋势[J], 通信学报, 2002,5(23),P18-26
- [4] Zhang Zhaozhi, modern cryptology foundation [M], Beijing University of Posts and Telecommunications Publishing house, 2004,P53
章照止, 现代密码学基础[M], 北京邮电大学出版社, 2004,P53