Exploration on teaching of "Cryptology"

XU Hong, ZHENG Yong-hui, GU Chun-xiang

Information Engineering Institute, Information Engineering University, ZhengZhou, 450002*, China*

*xuhong*0504@163.*com*

Abstract: The features of Cryptology course are analyzed, the status at present and the existing problem in the teaching of cryptology are summarized, and some suggestions are made on how to set appropriate course system and how to select appropriate content and teaching methods.

Keywords: Cryptology; Teaching Methods; Information Security

密码学课程的教学方法探讨

徐　洪，郑永辉，顾纯祥

*信息工程大学信息工程学院，郑州市，*450002*，中国*

*xuhong*0504@163.*com*

【摘要】分析了密码学课程的特点，总结了密码学课程授课的现状和存在的问题，从课程体系的设置，授课内容的取舍以及教学方式的使用等三个方面提出了几点建议。

【关键词】密码学；教学方法；信息安全

1 引言

随着计算机，互联网以及通信技术的迅猛发展，信息安全问题成为人们日益关注的焦点问题。人们往往需要多种不同的安全机制和技术来达到保护自己信息的安全性的目的，而在这些各种各样的安全技术当中，密码技术则是信息安全技术中最为关键的技术之一，很多的安全服务都可以通过密码技术来实现。密码学，作为研究密码技术的一门学科，已经成为很多高校为信息安全、计算机科学与技术、通信工程和信息与计算科学等专业的本科生或研究生必开的一门专业基础课。总体而言，由于课程开设的时间较短、积累的经验较少，和许多其他课程相比，还有许多教学问题值得大家研究和解决。

本文根据我们学院面向本科生开设密码学必修课的实践经验，总结了这门课程自身的特点，分析了当前这门课程的教学现状，对课程的授课方法也进行了一些简单的探讨。

2 密码学课程的自身特点

要对密码学课程的授课方式进行一些有益的探索，首先应该摸清这门学科自身的特点和规律。

2.1 密码学是一门古老而又年轻的学科

密码作为一门技术源远流长，最早可以追溯到几千年前的远古战争时代。长期以来，密码这一技术总是与军事、外交情报领域联系在一起的。直到现在它也是获取敌方情报的一个重要手段。由于它涉及国家机密。因此他一直由政府指定的机构来研究，是机密的，不对民间公开的[1]。20 世纪 70 年代以来，随着计算机、通信和信息技术的发展，密码领域发生了新的变化，比如：社会对密码的需求更加迫切，密码应用范围日益扩大，密码研究领域不断拓宽，密码科研也从专用机构走向社会和民间，密码在上世纪 70 年代才真正形成了一门学科。

2.2 密码学是一门理论和应用并举的学科

密码学是集数学、计算机、网络与通信等多学科为一体的一门学科，涉及的知识面广，尤其是需要涉及数论和代数学等一些专门的数学知识，理论性很强。同时，密码学又是一门应用性很强的学科[2][3][4]，它不同于高等数学、数学分析等基础课程，对于这些课程，学生很难在现实生活中感受到它们的应用。而密码学却不同，在实际的工作和生活中都有着广泛的应用背

978-1-935068-09-9

景，比如加密技术、签名技术在电子商务中的应用，在银行证券行业中的应用等等。

2.3 密码学是一门集攻击与防护为一体的学科

密码学分为密码编码学和密码分析学两个分支，密码编码学研究的是如何设计出能够抵抗各种现有攻击方法的安全有效的密码算法；相反，密码分析学研究的则是如何寻找现有密码算法的弱点并提出攻击算法，在不知道用户私钥的情况下还原明文消息或者用户的私钥等等。这两个分支既相互独立，又紧密联系，一个防护，一个攻击，相互促进，共同发展[5]。

3 密码学课程的教学现状及存在的问题

目前已经有很多高等院校都开设了密码学这门课程，经过众多同行的共同努力，密码学课程的授课理念和方法已经取得很大的进步，但很多学校的教学力量，无论是从师资队伍还是教学条件抑或是实践环境来看，还比较薄弱，离课程要求还有一定差距，有些方面，特别是在课程体系的安排，教学内容的取舍，和实践教学方式的使用上还存在一些问题。如何合理地解决好上述这些问题，提高教学质量值得我们共同探讨和思索。

4 密码学课程教学方法探讨

4.1 完善密码学课程体系

密码学是一门多学科高度融合的学科，在课程体系的安排上要注意数学、计算机、网络和通信等学科，特别是数论、代数学和复杂性理论等知识的补充。

4.2 优化授课内容

由于密码学覆盖的内容较多，所以该课程的授课内容就要有所选择和有所针对性。有所选择就是要注重基本知识的介绍和基本技能的培养，注意教学内容的层次性；有所针对性就是针对不同的专业和方向，或者不同的水平，选择不同的教学侧重点。

同时，作为一门应用性非常强的学科，密码学涉及的知识更新换代比较快，授课时不能仅仅拘泥于讲授课本知识，还应该时时关注相关知识的最新研究状况并在课堂上穿插补充这些新知识。

4.3 加强实践和科教结合的教学方式

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。这就要求我们在教学活动中应该采取不同于初等数论、数理逻辑等基础课程的教学方法，淡化理论的推导，为学生提供更多的实践机会。通过各种渠道和形式让学生参与各种各样的科研活动，采取科教结合的教学方式，加深学生对课堂知识的理解。

5 结束语

本文总结了密码学课程自身的一些特点和当前国内外一些高等院校在开设本门课程存在的一些普遍问题，在此基础上，结合作者多年的教学经验从课程体系设置，授课内容的取舍以及实践和科教结合的教学方式的利用等三个方面给出了一些自己的观点。

References (参考文献)

[1] David Kahn. The Codebreakers[M]. Baker & Taylor,1967.
[2] Bruce Schneier. Applied Cryptography: Protocols, Algorthms, and Source Code in C[M]. John Wiley & Sons, 1996.
[3] Alfred Menezes, Paul van Oorschot and Scot Vanstone, Handbook of Applied Cryptography[M]. CRC Press, 1996.
[4] Niels Ferguson and Bruce Schneier. Practical Cryptography[M]. John Wiley & Sons. 2003.
[5] William Stallings. Cryptography and Network Security[M].Prentice Hall. 2003.