Research on the Experiment Teaching Method for the Information Security Major Based on the Educational Psychology

OU Qing-yv[1], ZHANG Chang-hong[2], ZHOU Da-wei[3]
Depart. of Information Security, Naval University of Engineering, Wuhan, 430033, *China*
1. *ouqingyv@sina.com*, 2. *Hgdzch*@163.*com*

Abstract: From the aspects of the practical teaching for information security, and combined with the characteristics and objectives of the experiment teaching for information security major, in this paper, the experimental teaching method and its innovation are researched by the way of the educational psychology.

Key words: Information security; experiment teaching; educational psychology

从教育心理学角度探索信息安全专业实验教学方法

欧庆于[1]，张昌宏[2]，周大伟[3]
海军工程大学电子工程学院信息安全系，湖北 武汉 430033
1. ouqingyv@sina.com, 2. Hgdzch@163.com

【摘　要】从信息安全教育实际出发，结合信息安全实验教学的特点、目的，利用教育心理学理论对信息安全专业的实验教学方法进行了研究，提出了信息安全实验教学改革和创新的思路。

【关键词】信息安全；实验教学；教育心理学

1 引言

信息安全专业所包含的课程种类较多，要求学生充分理解信息安全的基本概念，掌握各种信息安全应用的基本技术及方法，并牢固树立信息安全意识[1]。通过长期的教学实践，发现信息安全相关课程实践性较强，单纯地通过课堂讲授难以使学生充分理解相关的知识点及相关技术。因此，非常有必要根据专业的培养目的，有针对性地实施信息安全实验课程，让学生通过实验过程的动手实践，发现问题并解决问题，最终达到深入理解信息安全知识内容，掌握相关安全技术、培养良好的安全习惯的目的。同时，也充分培养学生发现问题、分析问题、解决问题的能力。

在学生学习过程中，除智力因素外，不能忽略非智力因素的影响。动机就是其中之一。动机是一个人行动的理由，学习动机是指个人的意图愿望、心理需求或企图达到目标的一种动因、内在力量[2]。为了有效提高信息安全实验课程的教学效果，课程组在教学过程中从教育心理学的角度，对信息安全专业实验教学方法进行了研究。通过激发学生学习的动机，唤起他们的兴趣，调动学生学习的积极性，提高教学质量。

2 从学习任务的利用性价值激发学习兴趣

要激发学生学习的兴趣，首先必须使学生对学习有一个正确的认识。信息安全是将各种密码学理论、先进的计算机技术、半导体技术、电子技术和各个行业的具体应用相结合后的产物，这就决定了它必然是一个技术密集、高度分散、不断创新的知识集成系统。

兴趣是建立在需要的基础之上的，可以从完成这一学习任务以达到其他目的这一利用性价值来激发学生的学习兴趣。密码学作为信息安全专业的骨干基础课程，为了加深学生对所学知识的理解，往往需要对密码算法的正确性进行验证。而在以往的教学中，大多数是通过理论证明或软件方式来验证密码算法是否可以正确实现，这不仅缺乏直观性，而且与实际情况相脱节。国家密码委早已规定，一切密码算法的使用都必须建立在硬件的基础上。有鉴于此，我们参照密码在各种行业中的实际应用情况，制定了与密码学相关的嵌入式实验。该实验主要分为三部分，分别是：

验证型实验、综合型实验以及自主研究型试验。

其中，验证型实验作为配合密码学课程开设的实验环节，其主要目的在于帮助学生理解、掌握密码学课程中所讲授的各类算法，为后期的深入学习奠定一定的基础[3]。在验证型实验中，学生利用各类实验平台（如 ARM9 实验平台、SOPC 试验平台等）实现密码算法，然后下载到嵌入式实验平台中，并利用超级终端观察程序在嵌入式平台运行的情况。通过验证型实验，学生能够体会到密码算法在实际中应用的情况和特点。

基于验证型实验而开设的综合型实验，其主要目的是培养学生对密码学课程中所讲授的各基础知识点综合运用的能力。在综合型实验中，要求学生运用网络编程知识，选择适当的密码协议，实现基于对称密码的密钥分配、基于公钥密码的密钥分配以及端端密码通信等功能。这就需要学生深入掌握网络编程、密码协议等相关知识。在实际实施过程中，我们选择 JAVA 语言作为网络开发平台，使得学生在利用 JAVA 语言进行密码应用网络编程的过程中，进一步体会到 JAVA 语言的平台独立性和安全性[4]。

自主研究型实验针对密码学课程中所介绍的某些较新的密码算法及相关研究热点，在老师的启发下，由学生提出解决方法和方案，并尝试进行实现。其主要目的是考察学生对所学知识的理解、掌握和灵活应用的程度及与现实相关联的能力，培养学生运用所学知识解决实际问题的能力。在近三年的实施过程中，我们主要选取了 3-DES 密码算法的并行化实现、RSA 密码算法快速实现、有限域乘法的优化设计、ECC 密码算法并行化等研究热点作为实验内容，使学生能够对当前密码学领域的发展动态进行了解。在具体的实验环节中，会给学生介绍出大概的实验流程，然后安排学生组成 2～3 人的实验小组，利用课余时间查找相关资料，最终上机形成完整实验过程，并由老师进行点评。

3 以明确要求和相应期望增强教学实施效果

心理学中期望理论的基本主张认为，个体力求成功的努力程度取决于他们对奖励的期望。所以教师对学生期望需要适度。太高的期望容易让学生产生畏惧，动机就会削弱，而过低的期望会使学生认为任务简单，无需努力也可以获得一个满意的成绩，这样学习积极性也不会提高。

在每次实验教学开始之前，我们将本次实验的目标明确传达给学生，使得学生形成对自己的要求并为之努力。例如，在 DES 算法验证型实验中，其实验目标为基于 ARM9 实验平台，利用 C 语言编程实现 DES 的 16 轮迭代变换以及 S 盒；在端端密钥分配综合型实验中，其实验目标为基于 ARM9 实验平台，通过网络编程实现两组之间的共享密码密钥分配，并确保其传输过程的安全性。

而在讲解实验流程及相关要求时，应注意创造亲切的心理气氛。在向学生明确提出要求的同时，通过目光注视、语言暗示等手段向不同的学生提出适度的不同期望，利用皮格马利翁效应使不同层次的学生都能够在规定时间内逐步熟悉并掌握实验流程及要求。

4 通过及时反馈与评价增强其学习动力

心理学家指出，学生如果获得成功，将会产生轻松、愉悦的情绪，这种情况反复出现就会产生学习兴趣，久而久之就产生了学习动机。反之，经常失败会导致学生感觉到无助，这时学生往往会认为不管自己做什么，都注定要失败或毫无意义。

为了有效增强学生的学习动机，这就要求教师帮助学生把握好成就动机，使其更为有效地促进学习。信息安全实验作为一门强调学生动手能力与自主学习能力培养的课程。其最终目的是培养学生应用理论知识解决实际问题能力，并加深对理论知识理解。所以，在实施过程中，应尽量创造条件，使学生获得一定的成功满足感，体会到学习的愉快和成功的喜悦，认识到学习并不是一件很困难的事[5]。

例如，在对每组尽心评价时，应注意对各组实验结果的评价不能过于笼统，而应仔细观察其实验流程、所采用的实验方法以及在实验过程中针对各种问题所采取的解决方案。如表扬实验流程规范、实验操作方法准确，解决方案有新意等。针对不当或错误之处，则应与学生一起分析原因，并总结纠正的方法与需要注意的事项，使得学生能够正确对待失败，并养成在失败中吸取经验、教训的习惯。特别是学习成绩不好的学生，要注意保护他们的自尊心和自信心。多些鼓励的表扬。要抓住学生身上瞬息即逝的“闪光点”去评价学生，使学生因看到自己的长处和成绩被认可而感到快乐，进而激发学习动机。

此外，为了激发学生进一步学习的愿望，应提供明确、及时的反馈，并帮助学生及时发现、纠正错误，调整学习的进度，使用合适的策略来完成任务。

978-1-935068-09-9 © 2010 SciRes.

5 合理安排评价、奖惩的频率

行为主义理论研究证明，不管奖励多么有效，如果奖励的次数不够频繁，那么奖励对改善行为没有多大作用。

然而，如果一个学生经常性受奖，久而久之将会损害已有的内部学习动机，起不到激励作用。同样，经常受惩也将使学生丧失自信心，对学习失去兴趣。因此，为了最终到达培养学生动手能力及自身学习能力的目的，必须在实施信息安全实验教学的过程中合理安排评价、奖惩的频数，让所有学生都有获奖的可能性，使受奖受惩都能促进学习，激发学习动机。

例如，在进行评价时可从以下几个方面进行：1、操作的规范性；2、解决问题的能力；3、解决方案的新意；4、实验完成程度；5、实验报告撰写情况等。通过细化评价准则，对每个学生的闪光点进行及时的奖励。同时，在表扬的同时应指出其仍可改进之处，鼓励其进一步完善。对于较差的学生，应避免对其进行公开的批评。而应选择单独与其谈心的方式，使其明确信息安全实验课程的重要性，培养其学习兴趣。

6 结论

通过近五年来，信息安全实验课程教学方法的探索与改进，我们对参与信息安全实验课程共两级信息安全专业本科学生，供 138 人进行了调查。从专业课程的考试成绩来看，改进实验教学方法后，学生成绩有较大程度的提高，反映了学生对于相关理论及知识点理解较充分。从学生随堂实验情况和实验报告完成情况看，学生对课程的学习兴趣和发现问题、分析问题、解决问题的能力都有所提高。因此，通过对信息安全实验教学方法的改革探索，起到了调动了学生的学习积极性、培养学生的创新意识、提高教学质量的目的。

References (参考文献)

[1] PENG Guo-jun, ZHANG Huan-guo, LIU Dan. Undergraduate of Experiment Teaching and Information Security[J]. Computer Education, 2007,23(5):142-144.
彭国军,张焕国,刘丹.实验教学与信息安全本科生[J].计算机教育, 2007, 23 (5):142-144.

[2] LI Bing-de. Didactics[M].Beijing: People Education Press,1991.
李秉德. 教学论[M]. 北京: 人民教育出版社, 1991.

[3] FENG Xiang-dong, CHENG Jin-hua. Innovation and personnel training in the lab[M].Wuhan: Wuhan University Press.2003.
冯向东,成金华.实验室创新与人才培养[M]. 武汉：武汉大学出版社.2003.

[4] Ishihuchi H, Tanaka M. Multi-objective programming in optimization of the interval objective function[J]. European Joumal of Operation Research, 1990, 48: 219-225.

[5] DU Mei-yi. Inventions derived from experiments[J]. Research and Exploration on laboratory,2005,24(3):1-3.
杜美义. 发明源于实验[J]. 实验室研究与探索, 2005, 24(3): 1-3.