文章编号：1672-5913(2016)03-0132-04　　中图分类号：G642

提高信息安全数学基础课程教学效果的几种途径

秦艳琳，吴晓平
（海军工程大学 信息安全系，湖北 武汉 430033）

摘　要：针对信息安全数学基础课程讲授过程中存在的突出问题，结合实际教学经验，从激发学生学习积极性和主动性的角度出发，提出精心设计课堂互动教学环节、注重介绍数学知识的应用实例、引导学生解决实际问题、建设配套网络课程、增设实验环节等提高课程教学效果的几种改进措施。

关键词：信息安全数学基础；教学互动；网络课程；编程实验
DOI:10.16512/j.cnki.jsjjy.2016.03.036

0　引　言

信息安全数学基础是大部分高校信息安全本科专业的一门学科基础必修课程。课程设置的起因主要是考虑到信息安全专业的学习和研究中有很多重要内容，如信息安全模型的建立、密码算法的设计与破译等，需用到数论、抽象代数、椭圆曲线理论等方面的数学知识[1]，而非数学专业学生学习这些数学知识则会感觉困难。信息安全数学基础课程教学可对相关数学理论进行系统全面的介绍，为学生今后学习密码学等其他信息安全专业课程打好数学基础。

1　精心设计课堂互动，提高学生学习兴趣

要提高课程的教学效果，首先要激发学生的学习热情和主动性，彻底改变学生在课堂上只做“听众”的消极状态；通过精心设计教学互动环节，深入挖掘学生自由思考的潜能，引导学生参与各个数学知识点的引入、展开及应用环节，创造良好的课堂氛围。

示例 1 ：在引入同余的概念时，教师可先提出两个问题：① 5 月 2 号是周六，5 月份还有几个周六，在哪些天？② 6、11、16、21、26、36 与数 5 的关系是什么？学生通过回答问题可归纳出同余的定义。

教师继而介绍凯撒密码的加密方法：将明文字母循环右移 3 位后得到密文字母，即 a → d，b → e，c → f……z → c。这时教师再次提出问题：“若用 0—25 分别表示 26 个英文字母，m 表示明文字母，c 表示密文字母，则如何用数学公式表示凯撒密码的加密过程？”

按照教师之前介绍的规律，学生一般会回答：“$c=m+3$。”老师提示学生当明文为 y（$m=24$）时，通过该公式得到的密文 $c=27$，超出了 0—25 的范围，应该怎么处理？学生进一步思考解决办法：将公式“$c=m+3$”修改为“$c=m+3(\mathrm{mod}26)$”即可。

通过本次互动，学生对同余的概念有了较为深入的理解，可以得到比单纯理论知识讲解更好的教学效果。

示例 2 ：在讲解完欧拉定理的概念后，教师可以介绍该定理在 RSA 算法中的应用。由于学生还未学习过密码学课程，对于密码体制的基础知识并不熟悉，因此在互动环节中，教师可选择 3 名学生分别扮演加密者、解密者及攻击者，请解密者选择自己的公开钥和私钥（如 $p=7$，$q=11$，公开钥 e 为 13，私钥 d 为 37），并将公开参数 $\{e,n\}$ 记录在黑板上，私钥则保存在自己的笔记本上。

基金项目：海军工程大学教育科研重点项目（NUE2015112）。
第一作者简介：秦艳琳，女，讲师，研究方向为密码学及网络安全，qinyanlincool@163.com。

教师宣布保密通信开始，加密者选择明文信息（如数字 2），在笔记本上写出加密过程：$2^{13}(\mathrm{mod}77)=30$ ，并将密文 30 抄录在黑板上。这时，解密者对接收到的密文在笔记本上进行解密：$30^{37}(\mathrm{mod}77)=2$。加密者与解密者核对原始明文的一致性（但不要公布解密出的明文消息）并宣布正确解密。

教师提问：“正确解密是如何做到的？”这个问题能激发学生探究加密方法的兴趣，此时教师再介绍运用欧拉定理证明 RSA 算法解密正确性的过程，或让学生带着疑问自学相关知识点，教师进行重、难点的深入讲解。

最后，教师请攻击者尝试对刚才的加解密过程进行破解，即由密文 30 恢复出明文 2。攻击者掌握的信息有密文 30、解密者的公开密钥 13 及公开模数 77。对照 RSA 算法的解密过程，攻击者发现需要找到解密者的私钥才能正确解密，而由算法中的“ $ed \equiv 1(\mathrm{mod}\varphi(n))$ ”看出，若已知 e 和 $\varphi(n)$ 就可以求出私钥 d，故只需求出 $\varphi(n)$，根据欧拉函数的相关知识，想求出 $\varphi(n)$ 需要将 n=77 进行因子分解，而 77 很容易分解成 7×11，进而求出 $\varphi(n)$=60，再通过 $13d \equiv 1(\mathrm{mod}60)$ 就可将 d=37 求解出来，最后由 $30^{37}(\mathrm{mod}77)$ 求出明文消息 2。

通过加、解密方的确认，承认攻击者的攻击成功。教师进一步提问：“为什么攻击者能够破解截获的密文呢？”

学生们作答：“是因为解密者选取的模数 77 太小，很容易分解，被攻击者利用后求出了解密密钥。”

教师继续提问：“实际应用中应该如何抵制上述攻击呢？”学生很自然能想到应“增大”模数 n，使其难于分解。这时教师可予以提示：“实际应用中模数 n 至少应取 1024bits，最好取 2048bits”。

教师或是进行过加、解密运算演示的学生又可以提出：“RSA 算法在加、解密过程中都需要进行复杂的模幂运算，若采取大规模的参数，将导致运算量加大，如何解决这一问题？”教师根据这一问题可顺势引出下节课的内容——模重复平方法。

通过上述一系列互动环节，学生可以掌握数论知识在 RSA 算法中的应用，整个课堂气氛也较为活跃，能够得到良好的教学效果。

示例 3 ：在讲解中国剩余定理时，教师先介绍《孙子算经》中记载的问题：“今有物不知其数，三三数之有二，五五数之有三，七七数之有二，问物有多少？让学生将问题转化为同余式组表示，进而尝试求解答案。

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

在学生经过思考后，教师开始介绍《孙子算经》中的算法，列出表 1。

表 1 《孙子算经》中的解法

除数	余数	最小公倍数	衍数	乘率	各总	答数	最小答数
3 ? ?	2 ? ?	3×5×7 = 105	5×7 ? ?	2 ? ?	35×2×2 ? ?	各总之和	取模 105 后的答数

教师以模 3 为例，分别给出除数、余数、最小公倍数、衍数、乘率及各总后，要求学生给出模 5 和模 7 的除数、余数、最小公倍数、衍数、乘率及各总，并求出答数和最小答数。

在熟悉具体问题和算法之后，教师再要求学生将《孙子算经》中的问题及相应解法推广到一般情况，并给出定理的证明过程。

通过这一互动过程，教师引导学生参与整个教学活动中，积极主动地寻求解决问题的方法，克服“灌输式”教学方式的弊端。

2　注重介绍数学基础知识在密码学和信息安全领域中的应用实例

信息安全数学基础课程是针对信息安全专业

学生设置的一门专业基础课程，因此在教学过程中应以数学知识在密码学等专业课程中的应用为主线，突出数学知识与密码算法及各类安全协议的密切联系，使学生充分认识到该课程对后续专业学习的重要作用，从而调动学生的学习积极性。表 2 列出信息安全数学基础相关知识点在密码学中的部分应用实例 [2-3]，以供参考。

由于信息安全数学基础课程通常在密码学等专业课之前开设，因此在介绍应用实例时应避繁就简，对涉及的密码学概念尽量用通俗易懂的方式进行介绍，使学生能够轻松地接受和理解，最终目的是通过讲解实例，帮助学生由被动接受知识变为在课堂上主动思考，在课后还能自觉查阅文献资料，进行更深入的研究。

表 2　信息安全数学基础相关知识点在密码学中的应用实例

知识点	应用实例
素数、整数的唯一分解定理	RSA 公钥密码算法
同余的概念和基本性质	加法密码及仿射密码
欧拉定理	RSA 公钥密码算法
中国剩余定理	Asmuth-Bloom 门限方案
二次剩余理论、勒让德符号	Goldwasser-Micali 公钥密码算法
二次同余式的求解	Rabin 公钥密码算法
原根及离散对数	Elgamal 公钥密码算法、Diffie-Hellman 密钥交换协议
有限域	AES 分组密码算法、椭圆曲线公钥密码算法
置换群	DES 分组密码算法
素性检验	RSA、Elgamal 等公钥密码算法参数设置
椭圆曲线理论、循环群	椭圆曲线公钥密码算法及密钥协商算法

3　引导学生利用所学数学知识解决信息安全领域的实际问题

信息安全的教育不仅是知识教育，还是一种创新素质教育。教师在讲解课程基本知识的同时，应结合学科前沿，及时补充信息安全领域产生的最新数学成果及应用，注重培养学生利用所学数学知识进行密码算法设计与分析、构建信息安全模型的意识和能力。

考虑到学生的知识水平，教师应从简单的密码算法入手，鼓励学生查阅文献资料，搜集日常生活中使用到的密码算法，并运用已经掌握的数学知识对实际应用中的算法开展安全性分析，大胆提出改进措施。学生可组成 3~5 人的课外研究小组，分工合作，将研究成果形成小论文或利用计算机编程实现；老师对小组的工作进行指导评分，最终作为课程考核成绩的一部分。表现突出的学生还可在教师的指导下对研究成果进行修改和完善，进而作为全国大学生信息安全竞赛的参赛作品。

另外，教师还可结合课程内容，向学生介绍著名学者借助扎实的数学基础解决信息安全领域各类难题的实例，激励学生运用所学知识解决实际的信息安全问题，通过“学习—应用—再学习”的过程，培养创新思维与动手能力。

4　建设网络课程，提高学习效率

信息安全数学基础课程知识内容多、范围广、

难度大与课程教学学时不足的矛盾在各高校普遍存在，很多学生会感觉学习难度较大，部分基础薄弱的学生上课跟不上进度，课下又找不到有效的自学方法，逐渐丧失学习的信心，最终达不到课程设置的总体要求，影响后续专业课程的学习[4]。

为了解决这一矛盾，教师可以建设一门信息安全数学基础配套网络课程，主要功能包括：①为信息安全专业学生提供课后复习巩固及自学的平台；②补充讲授要求学生自学的知识点；③补充数学知识在信息安全领域内的应用，提高学生的学习积极性；④为教师与学生提供具有辅导答疑、自测阅卷等功能的互动交流平台。

信息安全专业及参加信息安全竞赛的学生能利用网络教学平台进行远程学习，作为课堂授课的有效补充，促进课程教学质量的提高。

5　增加实验环节，提高素质能力

信息安全数学基础课程中的部分内容与密码学中密码算法的工程实现联系紧密，单纯理论知识的讲解会让学生感觉相应的算法原理晦涩难懂。对实践性较强的内容设置实验环节，可使学生通过动手操作或编程实现，加深对具体算法及其数学原理的理解。

教师可在授课中开设部分简单实验，如利用运算器工具完成大数运算、素性测试、模幂、原根、求逆等；同时开设一些计算机编程实现实验。针对课程教学中数学理论内容设置的部分编程实验见表 3。

表 3　对应数学知识点的编程实验设置

知识点	实验设置	
辗转相除法求最大公因数	用 C 语言实现辗转相除法计算两个整数 a、b 的最大公因数，并求出整数 s、t, 使得 $sa+tb=(a,b)$	
模重复平方计算法	设计程序实现模幂运算 $b^n \bmod(m)$	编写程序实现 2^{512} 的 RSA 公钥密码系统
素性检验	编程实现 Miller-Rabin、Fermat 素性检验算法	
模逆运算	$(a,m)=1$, 编程实现计算 $a^{-1}(\bmod m)$	
勒让德符号	编写程序计算勒让德符号	
中国剩余定理、模 p 二次同余式的求解	设计程序实现 Rabin 公钥密码	
原根、离散对数	编写程序实现 2^{512} 的 Elgamal 公钥密码系统	
有限域	编写程序生成一个次数为 50 的本原多项式	

表 3 中较简单的实验可由学生个人独立完成，稍复杂的实验可由学生组成小组共同完成。学生在编程过程中可以参考各类文献资料或部分源代码，但必须通过消化整合，最终才能提供完整的加解密界面。编程实现的过程能够使学生对所学数学知识有更深入的理解，并锻炼自主学习和动手能力。

6　结　语

信息安全数学基础课程在整个信息安全人才培养中占据着重要的基础性地位，但由于其理论性较强，在教学过程中往往容易出现“老师满堂灌、学生被动学”的局面。笔者基于“教为主导、学为主体、打牢基础、着眼应用”的教学理念，初步探讨了几种提高课程教学效果的途径，希望引起广大同行的思考和讨论。

参考文献：

[1] 秦艳琳, 吴晓平, 罗芳. 信息安全数学基础[M]. 武汉: 武汉大学出版社, 2014: 1.
[2] 李继国, 余纯武, 张福泰, 等. 信息安全数学基础[M]. 武汉: 武汉大学出版社, 2006: 53-54.
[3] 陈恭亮. 简明信息安全数学基础[M]. 北京: 高等教育出版社, 2011: 32-33.
[4] 巫玲. 信息安全数学基础任务型专题教学模式探讨[J]. 计算机教育, 2014(1): 47-48.

（编辑：宋文婷）