ISW 教学法在《密码学基础》中的教学设计探索

——以置换密码为例

李志飞　王宏艳
军事航天部队航天工程大学航天信息学院　北京　101416

摘　要：《密码学基础》是信息安全及相关专业的一门综合性专业核心课程，具有很强的理论性和实践性，课程内容复杂、难度高，涉及多门学科的知识，这会严重影响教学效果，难以达到“新工科”专业的培养目标和要求。介绍了参加 ISW 的体会和收获，以《密码学基础》课程中－置换密码为例，给出按照 ISW 进行课程教学模式改革的新方案，进而避免“填鸭式教学”以提高教学质量，可为高等教育教学的改革与创新提供借鉴。

关键词：ISW 教学；密码学；置换密码；教学设计

引言

随着数字虚拟货币、区块链、移动互联等新技术、新应用的飞速发展和广泛应用，各大高校开始设立信息安全专业来培养密码学人才，这其中开设密码学课程群一个重要举措。《密码学基础》作为信息安全专业的核心必修课程，能够为学生的后续学习打牢坚实的理论基础和动手实践能力，在网络空间安全学科建设中发挥了举足轻重的作用。早在 2014 年 2 月，习近平总书记强调“没有网络安全，就没有国家安全”，网络安全已然已经上升为国家安全战略 [1]。

密码学是一门集数学、计算机科学、统计学等多学科为一体的交叉学科，是一门综合性的尖端学科 [2–5]。航天工程大学的设置密码学课程群涵盖《信息安全数学基础》、《密码学基础》以及《密码学算法实验》等核心专业课程，均为信息安全专业的必修内容。这些课程涉及数学知识领域非常广泛，包括数论、离散数学、概率论等方面的内容，致使学生的接受程度较低。授课教师在密码学课程群的教学过程中，如何促使学生提升学习的自主能动性，而教师由知识的输出者转变为学生的辅助者，对“新工科”背景下密码学课程群的教学具有重要意义。

近年来 ISW（Instructional Skills Workshop）风暴席卷全球高等教育，ISW 打破原有的教育体系和设计结构，兼具教学流程独特、体验式学习方式密集、理论讲授与多轮微课相结合等特点，深度体现“以学生为中心”的教育理念，被认为是“课堂革命新范式”，为不同学科的教和学创造了全新视角 [6–9]。针对《密码学基础》课程特点及教学现状，结合国内外 ISW 的成功教学经验 [10–13]，本研究以置换密码（微课）为基础探索出可内嵌 ISW 的《密码学基础》课程教学模式改革新方案，该教学模式符合当今教育理念、目标和要求，对高等院校课程教学改革具有借鉴意义。

1 ISW 教学法

ISW 教学技能培训模式是由加拿大的温哥华大学教授 Douglaskerr 团队创建，创建初期旨在通过教学技能培训帮助新任教师提升教与学的水平。在取得良好效果后，培训对象扩展到所有教师，培训领域从高等教育持续延伸到中等、初级教育，培训范围也由加拿大逐渐扩大到其他国家。ISW 培训实践通常历经 3 天，共花费 24~30 小时时长，着重强调全程参与。该培训由两个部分构成，即理论讲述以及实践教学，二者时间占比大致呈 4 ： 6。就理论讲授形式而言，通常采用集体授课；而实践教学部分，则以分组方式推进，每组配置 4 至 6 名被培训人员以及 2 名引导人员 [14]。

1.1 角色转换式的培训方式

ISW 将学习与指导相结合，每位参与者需在教师和学生间完成角色轮换。在 ISW 架构下，开展自身授课训练之际，还要以为学生身份听取其他参与者的授课，并在引导员的指导下及时地给出反馈意见。从同僚及学生的双重反馈视角，这为参与者提供了一个能直接审视教学收获的机会。这样的转换式组织形式，可使参与者在平等互助、相互学习、协同工作的环境里获得锻炼与提升。对其而言，这是取长

补短、高效学习的良好契机，根本原因是在日常教学中学生的反馈很难及时的传导到教师手中。在此种的训练中，参与者可集中钻研、探讨课堂设计、教学策略及技巧等教学问题，尝试采用新型教学方法与技巧，而非单纯照搬过往成功做法。通过不断地实践、思考、分析、借鉴和提高，进而有效地打破已有思维局囿，充分整合所见所学所想的教学理念与方法，促进教师提升教学技能。

1.2 合理的培训周期

在 ISW 培训中，每位参与者需要完成：筹备 3 次微课、撰写 3 次教案、开展 3 次课堂讲授，且以学生身份听讲 3 次并即刻给出反馈见解。微课的授课时长被设定为 10 分钟，此设定具备双重目的，一方面能确保每节课堂总时长适度，从而预留充足时间用于反馈交流；另一方面则是保障 ISW 规定的各个环节得以完成，促使其他参与者能够及时发现教师存在的问题。ISW 组织的 3 次微课是按照发现、尝试和提升的过程循序渐进开展。第 1 次微课主要是让教师学会怎样组织好一堂课，增加自己对授课的理解；第 2 次微课主要让教师熟悉在 ISW 框架下一般课程的组织方法和所包含的要点，并基于此提供教学试验与创新的契机；第 3 次微课则致力于协助教师对所学讲课技巧予以巩固整合，助力教师养成优良教学习惯并培育自身风格。这三次微课，为处于认知、行为与情感这三个不同学习阶段的教学设计，提供了相应的实践机会。

2 BOPPPS 教学模型

2.1 BOPPPS 模型简介

课程教学的 BOPPPS 模型由 Bridge-in、Objective、Pre-assessmen、Participatory Learning、Post-assessment、Summary 共六部分组成。BOPPPS 教学模型显示了一次完整的教学过程所包含的六个环节，如表 1 所示。

表 1 BOPPPS 教学模型

类别	内容	描述
介绍	Bridge-in	强调课程开始的引入，激发兴趣
	Objective	需要明确课程学习的目标
	Pre-assessment	了解学生的已有基础
主体	Participatory Learning	强调授课过程的交互性
结论	Post-assessment	重点考察教学的即时效果
	Summary	对课程内容的总结

2.2 BOPPPS 模型的教学实践

对每位教师而言，对如何达成有效教学这一问题，是需要正视与深度思考的。BOPPPS 教学模型是 ISW 培训的核心内容板块，教师应该深入理解其内在并将其嵌入到课程设计环节中，从而实现对教学效果的改善与提升。

2.2.1 Bridge-in（导入）

在课堂教学中，导入占据着关键地位。在开始讲授之前，学生的思维或许尚处于游离状态。此时，导入所发挥的效用便是促使学生思维迅速聚焦于课堂本身。若能妥善运用“导入”这一环节，将会达成事半功倍之效。导入环节一般需凭借多媒体手段、问题等途径予以开展。

2.2.2 Objective（学习目标或效果）

学习目标应按照 BLOOM 教学目标分类法阐明学习目的，该方法将多维认知过程解构为记忆、理解、应用、分析、评估、创新这六个层级，旨在确切告知通过本次课程学习能够懂得什么或者学会做什么。目标应该是具体的、可观察的、可量化的、可描述的，而不是熟悉、了解、知道这类模糊的词语。

2.2.3 Pre-assessment（课前评估）

借助课前评估的方式来检测学生对本次授课内容的知识储备状况以及熟悉程度。并以此为基础，适时对授课内容或授课侧重点进行针对性地调整。一般采用提问、雨课堂、头歌、头脑风暴等方法进行。

2.2.4 Participatory Learning（参与式学习）

作为教学设计的核心和主体阶段，学生应达最大程度地发挥自身能动性来参与学习过程，而教师需要将各类教学媒体、课程资源加以综合运用，在一种轻松活泼、循序渐进、知识充盈的氛围中助力学生完成学习。参与式学习一般涵盖两种方式：其一是教师与学生间的互动式交流；其二是学生内部之间的研讨式交流。

2.2.5 Post-assessment（课后评估）

对本次课新学知识的进行评估，形式多样，主要目的是了解学生学习效果、判断其是否达成设定的学习目标、检验其运用所学知识解决实际问题的能力等。一般情况下，课后评估还应与课前评估相对应，进而直接体现通过参与式学习产生的增量。课后评估通常采用答题的方式进行，可借鉴雨课堂等平台实时反馈正确率。

2.2.6 Summary（总结）

教师对本节课学生学习内容、学习效果的总结反思，同时对自己教学理念、设计、效果进行反思，并为下一次

授课过程预留话题空间。

3 ISW 微课教学设计 – 以置换密码为例

3.1 Bridge–in 环节

在课程开始之前，教师通过假定这样一个场景，即假设在春秋战国时期，你需要将敌人下一步进攻的城池向朝廷密报，但是你手头可以用的就是木棒和布条（羊皮条等带状物），问你应该如何将信息进行加密处理，以确保军事秘密的安全性？留给学生几分钟思考时间后，授课教师通过自制一个斯巴达密码棒（如图 1 所示），这看似简单的操作便实现了信息的加密处理，为什么会产生这样的效果呢？进而开展本次授课。

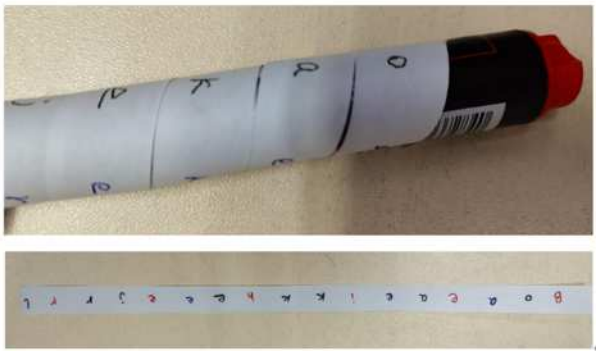

图 1 斯巴达密码棒（自制）

3.2 Objective 环节

3.2.1 知识目标

1）能够描述置换和置换密码的定义（记忆、理解）；

2）能够列举置换的典型特点（记忆、理解）；

3）能够描述置换密码的加密流程与原理（记忆、理解）；

3.2.2 能力目标

1）能够根据置换密钥对信息进行加密，并给出加密结果（应用、分析）；

2）能够判断某些算法是否属于置换密码（应用、分析）；

3.2.3 素质目标

1）逐步树立没有网络安全就没有国家安全的信念和决心；2）逐渐养成科学思辨、勇攀高峰的职业素养

3.3 Pre–assessment 环节

这里采用提问的方式进行，斯巴达密码棒能进行加密，背后的数学机理是什么？能否给出对应的数学表达形式。

3.4 Participatory Learning 环节

置换密码，又称为换位密码（Transposition Cipher），是一种通过重新排列明文中字符位置以生成密文的密码技术（依据特定规则对明文进行重排，以破坏其原有的结构特性）。这种密码的核心特征在于，明文中的所有字符均被保留不变，仅通过字符位置的变换来实现对原始信息的扰乱，从而达到加密的目的。

实际上，古希腊斯巴达人所使用的密码棒就采用了置换密码算法。密码棒加密时沿着木棒写上相应的明文字母，展开后羊皮条上的结果就是加密后的密文，如图 2 所示。

定义 1.1（置换）有限集 X 上的运算 $\sigma: X \to X$，σ 是一个双射函数，也就是说，σ 既是单射又是满射，并且定义域和值域相同，那么称 σ 为一个置换。即任取 $\forall x \in X$，存在唯一的 $\forall x' \in X$ 使得 $\sigma(x) = x'$。同理可以定义逆置换 σ^{-1}，即 $\forall x' \in X$，存在唯一的 $\forall x \in X$ 使得 $\sigma^{-1}(x') = x$ 且 $\sigma^{-1}\sigma = 1$。

【例 1】设有限集 X ={1,2,3,4,5,6,7,8}，σ 为 X 上的一个置换，并且满足 $\sigma(1)=2$，$\sigma(2)=5$，$\sigma(3)=3$，$\sigma(4)=6$，$\sigma(5)=1$，$\sigma(6)=8$，$\sigma(7)=4$，$\sigma(8)=7$。因为置换可以简单用对换表示，所以上述置换 σ（即密钥）可以形式化表示为对换的乘积（如图 2 所示），即

$$\sigma = \begin{pmatrix} 12345678 \\ 25361847 \end{pmatrix} = (125)(3)(4687) \quad (1)$$

则其逆置换 σ^{-1} 可以表示为

$$\sigma^{-1} = \begin{pmatrix} 12345678 \\ 25361847 \end{pmatrix}^{-1} = \begin{pmatrix} 12345678 \\ 51372486 \end{pmatrix} = (152)(3)(4786) \quad (2)$$

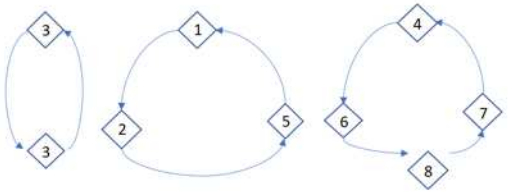

图 2 置换示意图

置换用对换表示不仅形式上简单，同时也提供了一种快速求逆置换的方法。若置换为

$$\sigma=(x_{11}x_{12}x_{13}\cdots x_{1(l-1)}x_{1l})\cdots(x_{m1}x_{m2}x_{m3}\cdots x_{m(n-1)}x_{mn}) \quad (3)$$

相应的逆置换为

$$\sigma^{-1}=(x_{11}x_{1l}x_{1(l-1)}\cdots x_{13}x_{12})\cdots(x_{m1}x_{mn}x_{m(n-1)}\cdots x_{m3}x_{m2}) \quad (4)$$

3.5 Post–assessment 环节

课后评估主要采用答题的方式进行，这里再次回到前面给大家列举的斯巴达密码棒的例子（如图 1），并请学生回答两个问题。第一斯巴达密码棒能够加密的原理是什么？

第二是它的加密过程具有什么特点。在此基础上，给出明文和密钥，能够根据置换对信息进行加密，并给出加密结果。

3.6 Summary 环节

本次课程我们以斯巴达密码棒作为课程整个牵引，进而引出置换和置换密码的定义与加密方法，使同学们达成本次课程设计的教学目标。后续，我们将继续介绍如何基于置换密码对大量文本信息进行加密处理的方法。

4 结语

目前，ISW 模式已得到了国内外众多高等教育机构的认可，采用 BOPPPS 教学六要素来开展教学过程，能够重塑传统意义下以教师为中心的“填鸭式”教学范式，这对于提升学生的内在驱动力以及强化上课质量与效用具有重要意义。本研究进一步给出了可结合 ISW 的教学设计案例，相关研究成果能推进我国信息安全专业人才教育和课程体系建设具有重要的借鉴价值。

参考文献：

[1] 习近平 . 把我国从网络大国建设成为网络强国 [EB/OL]. (2014-02-27)[2025-09-20].http：//news.xinhuanet.com/2014-02/27/c_119538788.htm.

[2] 姚宣霞 , 边胜琴 . 现代密码学细粒度、层次化实验教学设计 [J]. 计算机教育 ,2024,(11):145-149.

[3] 欧庆于 , 罗芳 , 叶清 , 等 . “密码学课程综合设计”教学改革研究 [J]. 教育教学论坛 ,2023,(34):60-63.

[4] 李德顺 , 姚姜源 , 羊秋玲 , 等 . “应用密码学”专题研讨式课程教学设计 [J]. 工业和信息化教育 ,2023,(11):38-42.

[5] 周敏 , 王莉芳 . “新工科”背景下融合 MOOC 和翻转课堂的教学模式探索与实践——以西北工业大学《计算机编码与密码学》课程为例 [J]. 高教学刊 ,2021,(01):1-6.

[6] 杨兆 , 武晓岩 , 简洁 . 教学技能工作坊对教师教学能力提升的作用研究 [J]. 中国高等医学教育 ,2025,(04): 45-46.

[7] 谷秀青 .ISW：高校思政教师教学能力提升新路径 [J]. 长春教育学院学报 ,2023,39(05): 40-45.

[8] 徐杰 , 娄震 , 王君兰 , 等 . 加拿大教学技能工作坊（ISW）项目的实践与研究 [J]. 中国成人教育 ,2020,(16): 61-64.

[9] 张亚周 , 钟兆根 , 孙艳丽 . 以 ISW 为依托提升军校教员的教学技能 [J]. 电气电子教学学报 ,2020,42 (04): 34-37.

[10] 孙仓 . ISW 教学法在《药用植物学》中应用探索 [J]. 福建茶叶 ,2019,41(07): 133-134.

[11] 冯晓敏 , 沈重 , 张鲲 . 基于变分稀疏贝叶斯的 off-grid DOA 估计 [J]. 海南大学学报 (自然科学版), 2019,37(03): 193-202.

[12] 刘胜 , 陈海燕 , 马驰远 . ISW 培训及 VLSI 设计与验证教学实践体会 [J]. 计算机教育 ,2015,(11):21-24+35.

[13] 谭春娇 , 周海芳 , 刘越 , 等 . 结合加拿大模式开展我国教师教学技能培训 [J]. 计算机教育 ,2014,(04): 47-50.

[14] 张亚周 , 钟兆根 , 孙艳丽 . 以 ISW 为依托提升军校教员的教学技能 [J]. 电气电子教学学报 , 2020,42(04):34-37.

作者简介：李志飞，（1991—），男，汉，内蒙古自治区呼和浩特市人，博士，军事航天部队航天工程大学，讲师，信息安全

王宏艳，（1978—），女，汉，甘肃省庆阳市人，博士，军事航天部队航天工程大学，教授，电子对抗技术