《密码应用与安全》课程面临挑战与建设思路*

郑世慧 肖达 毕经国 谷利泽

北京邮电大学网络空间安全学院
北京 100876

摘 要 密码技术是网络安全的核心支撑技术之一，在全国深化研究生教育改革的契机下，我们加强建设《密码应用及安全》课程。以培养综合素质过硬的密码人才为目标，秉承教师为主导、学生为主体的教学理念，我们重构课程内容框架，梳理知识点，设计引导问题来帮助学生建立知识体系。同时，借助多种现代化教学工具提高课程质量。

关键字 密码应用，密码系统，问题驱动，智慧教学方法，过程性考核

Challenges and development idea for the course "Cryptography Application and Security"

Shihui Zheng Da Xiao Jingguo Bi Lize Gu

School of Cyberspace Security, Beijing University of Posts and Telecommunications
Beijing 100876,
shihuizh@bupt.edu.cn

Abstract—Cryptography is a core technology for network security. In response to the country's graduate education reform, we have enhanced the "Cryptography Application and Security" course. Our goal is to cultivate highly skilled cryptographic talents. Adhering to the teaching philosophy where teachers guide and students actively participate, we have restructured the course content, organized key knowledge points, and designed guiding questions to help students develop a comprehensive knowledge system. Additionally, we utilize various modern teaching tools to improve the course's quality.

Keywords—Cryptography Application, Cryptographic system, Problem-driven, Smart teaching methods, Process Assessment

1 课程建设背景

近年来，随着信息技术的飞速发展，计算机信息网络服务已经成为各行各业的基础服务，是国家间、行业间、以及个人间快速沟通的重要媒介。但是，由于基础设施、网络安全技术与人员管理的漏洞，涌现了大量危害国家和社会的安全事件，据不完全统计，仅 2023 年上半年，全球共发生了 3,676 次数据泄露事件，涉及超过 27 亿个记录，造成了巨大的经济损失[1]。目前，网络与信息的安全问题已经成为全球关注的焦点，而其安全性保障很大程度上取决于密码技术的发展。换句话说，有效的密码防护技术有助于抵御恶意的网络访问或者数据泄露。

为了加强我国网络与信息的安全建设，我国逐渐形成以《网络安全法》、《数据安全法》、《密码法》和《个人信息保护法》等为重要组成部分的网络与信息保护法律体系。它们积极推动了国内密码安全防护的辐射效应，从政府组织，企业和用户等各个环节提出了严格的责任和要求。特别是 2020 年颁布的《密码法》，要求提高密码安全水平，加强相关技术安全审查，维护社会公共安全秩序，确保民众的人身、财产安全。

法规政策不仅明确指出密码技术在保障网络与信息的安全性方面不可或缺的地位，也为进一步推广应用和发展研究密码技术提供了坚实的法律后盾。与此同时，为培养网络安全专业人才提供了机遇[2]。2019 年 12 月，教育部正式发布了《关于加强密码学课程建设和培养密码人才的指导意见》，旨在强化国家密码学产业人才培养体系建设，为密码学技术发展营造良好的环境，进一步促进我国信息安全技术创新和提高信息安全产业水平。为此，《指导意见》规定要倡导高等学校深入密码学领域，开设相关本科、硕士和博士课程，培养高等学历人才，推进密码学新技术的教育研究，

*基金资助：2023 年北京邮电大学研究生教改项目“《密码应用与安全》“一精多能”型人才培养模式的探索”（项目编号：2023Y012）。

促进相关学科的深入发展，树立密码学产业和信息安全工程及相关应用技术人才的素质要求。

1．1 课程建设面临的挑战

首先，先修课程《现代密码学》对应现实中的攻击者抽象出黑盒环境下的攻击模型，揭示密码原语和协议的基本原理。这些密码方案通常被称为教科书式的安全方案，教学中主要关注方案的正确性，而不探讨实际部署问题。如“选择一个安全的大素数”，这一安全假设如何在现实中部署？部署中可能存在哪些安全风险和安全漏洞。因此，弥补理论和实践的鸿沟是急需解决的问题[3][4]。

其次，从密码理论和技术的发展来看，我国仍相对落后。目前密码的重要研究活动主要由美国发起，安全产品也以美国标准算法为主。因此，先修课程中常以美国联邦标准作为示例。为了促进密码技术国产化进程，抵制后门攻击造成的危害，需要帮助学生理解和掌握我国的密码标准和技术规范。

再次，侧信道分析技术提出后二十多年里，针对密码实现技术的灰盒分析技术及白盒分析技术取得了长足发展，故而掌握相关攻击技术与防御方法是密码人才的基本素养。

最后，学习环境相对自由，手机等电子设备极具吸引力，以往以灌输为主的讲授模式，无法保障学生注意力长时间集中。然而，密码技术理论性强，环环相扣，走神会导致后续内容很难理解，最终丧失学习动力。为此，需要多元化的教学方式方法来激励学生，最终达成教学目标[5]。

综上所述，为了落实“积极推动密码应用”和“加强密码应用安全审查”的任务，完善现有的密码学课程体系，形成一支能够应对多元化安全挑战的高素质密码人才队伍。我们，面向全校研究生开设了《密码应用与安全》课程，并借鉴其它团队在《现代密码学》课程上提出的多种教学经验[6][7]，积极探索多样化的教学方法来保障培养出合格的密码人才。

1．2 课程目标

通过《密码应用与安全》课程的学习，学生可以了解密码系统设计和分析的体系化问题，掌握密码算法工程实现的主要软硬件方法和技术；具备密码系统安全部署、配置和安全运维的能力；具备密码系统设计和安全性分析的系统化思维方式及工程化实现和测试的能力。此外，了解密码系统设计技术和密码系统安全测评技术国内外进展，具有对国际前沿科技文献的外语阅读和分析能力。

如图 1 所示，基础密码原语和协议在先修课程中有提及，本课程秉承国产化的理念，以国密的基本密码原语 SM2、SM3、SM4、ZUC 及相关密码标准作为基础，展示实践系统中如何设计部署密码策略。其次，本课程引用计算安全性的已有理论（先修课程中主要内容），重点探讨实际安全性和物理安全性（包含灰盒攻击环境和白盒攻击环境两个层次）。此外，以国密算法为实践案例，探讨密码原语部署的安全问题以及相应的应对措施。最后，选取典型的应用场景，如通信安全，从安全需求论证到工程化实现，促进学生理解并掌握密码系统的设计思维和动手实践能力。在引导学生构建自己的知识体系的过程中，我们需要遵循下述原则。

2 课程内容梳理

《密码应用与安全》课程的目标蕴涵三个层次子能力：识别安全问题与需求的能力，应用密码技术解决问题的能力，和评估密码系统安全性的能力。落实到知识模块的安排，体现为每一类密码技术能保障怎样的安全属性，怎样保障系统的安全性，以及如何衡量是否达到目标安全性。据此将教学内容分为相辅相成的四个板块，基础密码原语与协议板块，原语与协议的实践和部署板块，典型应用场景的安全解决方案板块，以及测试评估板块。

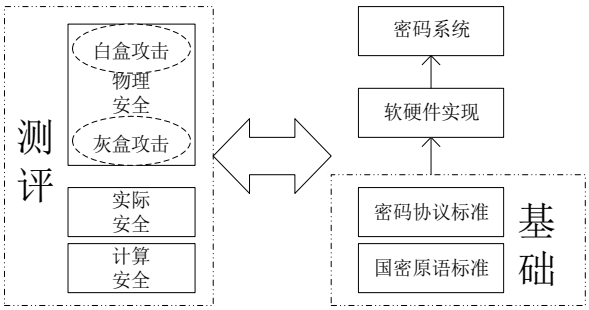

图 1 课程主要知识模块

(1) 本课程逐步向密码原语和基础协议的应用迁移。首先，面向实际应用中的安全属性，通过具体实施标准了解设计的完整流程，如加密算法确保机密性的运行模式如何选。其次，逐一解决单个原语的软硬件快速实现方法，如 AES 的有限域乘法和椭圆曲线的模幂运算。再次，同样通过标准了解协议的完整架构。最后，到整体的密码系统实现。例如通信安全系统，不仅包含主体功能部分 SSL，而且涵盖随机数模块为其提供不可预测的伪随机数；密钥管理模块负责各级密钥的分层分类管理；以及访问控制（身份鉴别）模块，为合法用户进行授权、鉴别及审计。

(2) 在系统的逐步实现过程，分析技术与设计技术相辅相成，遵循从发现问题到解决问题的循环往复规律。例如，从分组密码原语，通过可证明安全分析发现无法抵抗选择密文攻击（黑盒攻击），进而在设计中引入 AEAD 的工作模式。之后，对软硬件实现进行过侧信道和故障攻击（灰盒攻击），发现存在秘密信

息泄露点，故而在具体实现方案中添加掩码和冗余检测等技术进行防护。最后，对于软件存储的密钥，通过白盒的差分计算攻击等进行分析，发现依然存在秘密信息泄露，故而构造白盒密码进行防护。

(3) 在架构逐步细化过程中，始终体现安全性和效率的折中思想，使学生掌握根据具体应用场景部署适宜的密码系统的能力。如在原语的部署阶段，考察是否可以选用轻量级的算法。在原语和协议实现，可以根据实际软硬件资源，思量是否用存储换计算，如在线/离线方案。在协议部署阶段考虑分级分类部署的安全需求，如二级系统是否需要双因子身份鉴别，是否需要高阶掩码防护措施等等。

3 教学方法探索

教学目的是学生熟练应用密码技术解决复杂工程问题，为此，一方面以问题驱动课堂，引领学生寻知求索。另一方面，借助多种数字化教学手段和多元化的考核方法，提升教学效果。

3．1 问题驱动的教学模式

采用启发式教学方法，以问题为引导，让学生在实际应用中掌握密码技术，培养创新精神。首先，选择与课程内容相关且具有挑战性的问题，引导学生思考和探索。这些问题可以是实际应用中遇到的安全难题，或是对密码技术的改进。其次，赋予学生更多的自主权，让他们主动发现问题并探索问题的解决思路。教师可以提供相关资料和资源，并引导学生对比分析资料发掘问题；同时，要求学生按照参考文献等线索，积极搜索问题的解决方案，以培养他们独立研究及解决问题的能力。最后，涉及复杂的工程实践问题，将学生分为小组，通过互相交流与讨论总结，学生可以从不同角度审视问题，培养批判性思维和协作精神。在整个启发式教学过程中，教师充当引导者的角色，引导学生思考问题的不同层面，帮助他们找到问题的关键点和解决途径。通过提问、讨论、反思和总结，促使学生逐步形成安全领域的思维模式，提升问题解决的能力。这种教学方法不仅关注知识传授，更注重培养学生的自主学习、解决问题和团队合作能力，使他们在日后的工作和生活中都能够受益。

以密码模块中的随机数生成问题为例，如图 2 所示，先引入问题“如何选取随机数？”引导学生从安全性和效率两方面分组讨论真随机数和伪随机数的优劣，深刻理解密码方案安全性和效率的折衷思想。然后探讨“密码学的伪随机数的安全需求？”让学生分成两组，分别回顾 DSA 数字签名和分组密码运行模式中随机数不安全可能导致的安全风险。继而探讨“不可预测的伪随机生成器如何构造？”推荐国密标准《密码随机数生成模块设计指南》、《随机数发生器总体框架》和《软件随机数发生器设计指南》供学生课前阅读并实践软件随机数发生器，课堂上由学生分享发生器构造的原理，并总结实践过程中应注意的问题。再次，引出问题“如何判断随机数生成器的好坏？”，推荐国密标准《随机性检测规范》和《密码产品随机数检测要求》供学生课后阅读，利用检测工具对常用的 random 函数和 secure random 函数进行测试，比较测试结果，反思和总结密码模块中如何高效实现安全的伪随机数生成器。

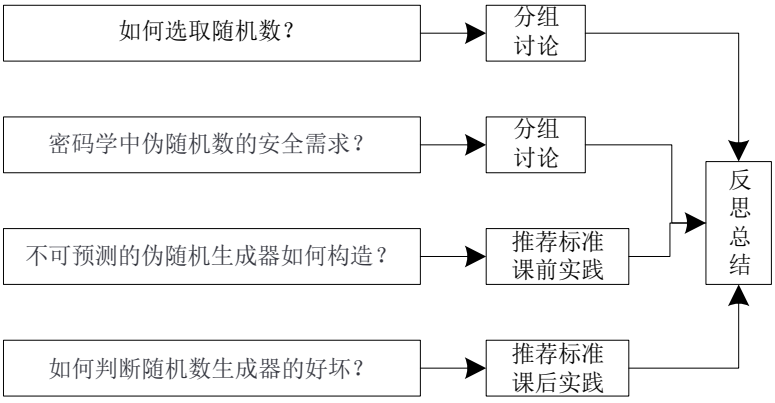

图 2 问题驱动课堂示例

3．2 丰富的教学手段

本课程借助雨课堂工具和本校的教学云平台实施线上/线下教学，进一步增强了师生间的互动交流，使教师授课的重点由传统的知识传递，转移到注重学生自我知识构建。在具体教学安排上，新型的智慧教学手段贯穿课前、课中和课后三个阶段。

（1） 课前预习

在上课前，教师把相关资料上传到教学云平台，包括课件、视频资料、参考书籍等等。同时，根据知识点的难易程度，布置预习任务。对于一些基础原理的难点内容，让学生阅读相关参考书并观看一些视频资料，晦涩难懂的内容记录下来，在课堂上由教师或

其它同学解惑。对于需要实践的内容，让学生提前调研标准，并发散思维进行实践，提炼实践中发现的问题以备课堂上分组讨论。对于前沿的知识内容，让学生分组调研相关文献并进行对比分析，然后梳理总结技术原理，制作讲稿及演示方案，在课堂汇报。

（2） 课堂知识内化

教师通过“雨课堂”授课，学生通过扫码加入课堂。教师通过精心制作的视频、音频、动画等精讲本章需要掌握的知识点，增加学习的趣味性。此外，利用雨课堂的提问工具进行师生的互动交流：少量客观题为课程知识点外延内容的调研，旨在提醒学生集中注意力，激发学生的学习兴趣；大部分客观题和主观题对应知识点相关的课堂练习，帮助学生巩固知识点，同时也在课程每章结束的时候，回顾章节知识点；投票题目主要针对易混淆的知识点进行辨析，启发学生思考。学生预习以及听讲过程中的疑惑，则可以通过弹幕发送给教师；教师可以利用“雨课堂”的数据统计反馈，掌握学生的学习情况，及时调整讲课的节奏及内容等。

（3） 课后巩固

课堂上教师板书的内容通常速度快，不利于同学深刻记忆。教学云平台可以自动开启录像功能，供学生课后反复观看录像，复习和巩固知识点。此外，通过网络教学平台，每堂课布置相关的实践作业，在实践中体会和理解知识点，并在实践中进一步提出工程问题。对于这些问题，云平台也会分享与课程内容相应的拓展阅读资料和一些开源的项目，学生也可以参阅这些资料，发散思维，独立思考，提升自主解决问题的能力。同样，学生也可以通过云平台反馈问题给老师和同学，课程群展开线下探讨。最后，教师可以通过调查问卷的形式，让学生进行自评和反思，帮助学生及早发现问题并进行调整。

3．3 过程性考核

教学考核模式可以达到以考促教，以考促学的目的，因此探索多元化过程性考核的方法也是本课程建设的重要内容[8][9]。具体地，课程采取百分制计分，总成绩由三个部分内容按权重累加而成。其中，课题表现成绩占 30%；实践能力 40%；创新能力 30%。

首先，课堂表现考核促进学生参与教学的积极性。在课堂上设置知识点对应的问题，对于积极参与互动的学生给与一些激励的积分，占总成绩的 10%。另外，对于课堂分组讨论的问题，讲解流利，演示效果卓越的小组，给与激励积分，占总成绩的 20%。

其次，以实践类作业题目考察学生解决工程问题的能力。根据知识点划分，布置 2 个实践题目。如分组密码的侧信道攻击及公钥密码的侧信道攻击，教师给出公开数据集挑战，让学生运用所学知识破译密钥。代价最小者胜出给与满分，其余按照排名依次递减，总成绩占比 20%。在学期末给出一个综合的密码模块设计或者安全评估的课程设计题目，如自主分析某应用场景的安全风险并尝试设计优良的解决方案，评价学生的思辨能力和实际操作技能。以学生互评分和老师打分加权得到最终评价成绩，最优者给与满分，总成绩占比 20%。

最后，以开放式的探索型作业考察学生的创新能力。提出一些开放性问题，要求学生进行深入思考和研究。例如侧信道对应的防御措施或者随机数生成及检测方法。通过团队合作调研和讨论，有助于培养学生的批判性思维和创新能力。同样采用学生互评和老师打分两种评价方式，最优者给与满分，总成绩占比 30%。

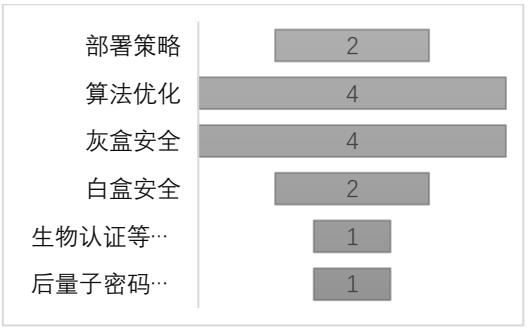

图 3 课程实践的工程应用问题

4 建设成果

本课程通过几年来的建设，目前学生对该课程有较高认同感，生源除网络空间安全学科外，吸引了电子、通信等专业学生。选课人数第一年为13人，第2年增涨到64人。课程中学生探讨的应用问题分为6大类。如图3所示，包含工程实践问题：密码模块部署的安全参数和密钥管理策略问题、密码模块的快速实现问题，灰盒或白盒安全风险评测及防御问题。也涵盖探索创新问题：生物认证等新技术的安全性探讨、量子计算和后量子密码的对决与应用思考。学生解决工程问题的能力和创新能力获得显著提升。

工程实践问题示例 --Hash 函数随机性问题：使用 SM3 对 “Beijing University Posts and Telecommunications”，的运算结果转换为二进制序列，用国密 15 项随机性检测方法检测其输出是否随机，结果见图 4。

单比特频数检测	0.8418701828800038	PASS
块内频数检测	0.8714699889033724	PASS
扑克检测	2.2713064971651 34e-12	FAIL
重叠子序列检测	0.021774910105575414	PASS
游程总数检测	0.02187603775905366	PASS
游程分布检测	7.88575391533486e-29	FAIL
块内最大“1”游程检测	0.25167441437623317	PASS
二元推导检测	0.12067630786041594	PASS
自相关检测	6.808456707489715e-85	FAIL
矩阵秩检测	0.6601830755442674	PASS
累加和检测	0.14514265181364894	PASS
近似熵检测	0.0031524460059092554	FAIL
线性复杂度检测	0.9856123220330272	PASS
Maurer通用统计检测	0.9840243050097878	PASS
离散傅里叶检测	0.17695774370450823	PASS

图 4 SM3 输出序列的随机性检测

通过实验可以得出在该项实验中，待测序列通过了单比特频数检测、块内频数检测、重叠子序列检测、游程总数检测、块内最大“1”游程检测、二元推导检测、矩阵秩检测、累加和检测、线性复杂度检测、Maurer通用统计检测、离散傅里叶检测这 11 项随机性检测，而扑克检测、游程分布检测、自相关检测、近似熵检测这 4 项随机性检测未通过。

工程实践问题示例 -- SM4 白盒实现的计算安全性分析：改进 SM4 的白盒设计，通过 Deadpool 库进行 DCA 实验测试。采集 200 个加密内存样本，如下图 7 所示，遍历第一轮轮密钥的第一字节所有值时，每个字节的差分轨迹均没有明显的尖峰，即攻击者无法获取正确密钥。

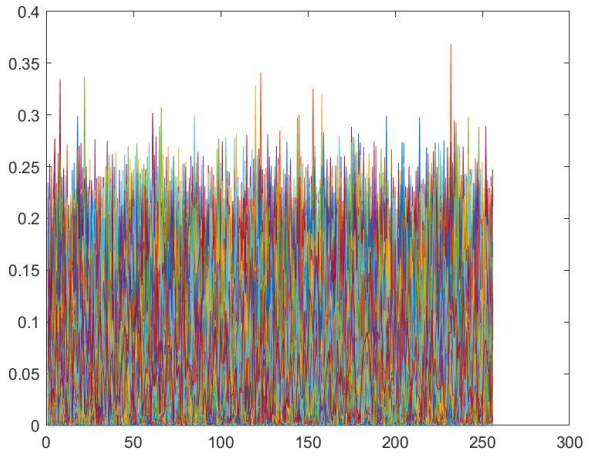

图 5 M4 白盒实现的差分计算攻击

学生在探索学习的基础上，积极参与开源社区建设、各项学科竞赛。在“华为杯”第一、二届中国研究生网络安全创新大赛上，我们学生获奖总数和一等奖总数均位居全国第一（见图 6）。

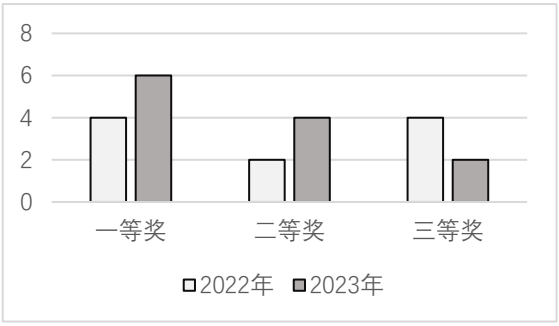

图 6 中国研究生网络安全创新大赛获奖人数

5 结束语

《密码应用与安全》课程旨在提高学生对于密码学技术的实践应用能力。我们从工科学生的培养要求出发，从课程内容、教学方法和考核方式等方面进行设计。课程在提高学生解决工程应用问题取得一定效果，受到学生广泛好评。在后续的教学实践中，我们将进行持续改进，在达到新工科培养目标的同时，力求彰显密码学作为交叉学科的特性，探索如何利用跨学科优势碰撞出精彩的成果。

参 考 文 献

[1] Verizon, 2023 Data breach investigation report[EB/OL].https://www.verizon.com/business/resources/T7b/reports/2023-data-breach-investigations-report-dbir.pdf.

[2] 童新海,吴科科,阎亚龙.密码人才培养亟需加强密码学科与专业建设[J].中国信息安全,2018(08):75-77.

[3] 邓芳，叶文，卢向群，梁美玉.新工科背景下融合OBE的《数据库系统原理》实验环节教学改革与实践[J].

计算机技术与教育学报，2021,9(2):54-58.

[4] 王丽杰，罗蕾.基于新工科的新生嵌入式系统设计课程探索[J].计算机技术与教育学报，2022,10(4):34-37.

[5] 胡钰,耿植林,普运伟等.以问题为导引的线上线下混合式教学模式探究[J].计算机教育,2022(02):73-78.

[6] 郭华,兰雨晴,高莹等.密码学课程群教学方法探索与实践[J].工业和信息化教育,2019(04):52-55.

[7] 赵银平，贺消非，郑江滨.基于OBE-CDIO理念的网络与信息安全课程教学改革[J].计算机技术与教育学报，2023,11(4):47-50.

[8] 沈树声,邓沿生,夏建中等.新工科背景下教学质量评价体系构建与实证研究[J/OL].电化教育研究,2023(08):103-107.

[9] 石娟.新工科背景下“大学计算机基础”课程教学改革研究与实践[J].计算机技术与教育学报，2022,10(1):77-80.