《应用密码学课设》

课程实验教学大纲

一、 课程基本信息

课程类型	☑独立设置的实验课　　☐课内实验						
课程编码	7263211	学分	3	总学时	3 周	实验学时	3 周
课程名称	应用密码学课设						
课程英文名称	Curriculum Project of Applied Cryptography						
适用专业	信息安全						
先修课程	（7001631）C 程序设计、（7241101）信息安全数学基础、（7242211）应用密码学						
开课部门	信息学院计算机系						

二、 课程性质与目标

本课程为信息安全专业的专业课程设计性实践教学环节。本课程为学生信息安全领域知识理论的学习奠定实践基础，目的是使学生学完课程后，对密码学的原理、思想和算法都有较清晰的理解，理解并学会运用密码学算法、思想和原理，掌握密码设计的基本方法和步骤环节，理解密码学在信息安全中的地位，了解密码学领域的新进展、新应用。培养基本的信息安全应用能力和处理实际问题的能力。

课程目标 1：学生应了解现代密码学关键技术的实现原理

课程目标 2：学生应掌握现代密码学重要加密算法的实现细节

课程目标 3：学生应能掌握现代密码学在现实生活中的应用

课程思政目标：本门课程在培养学生专业素质和思维能力的同时，通过将密码学中的主流密码技术和国家安全教育紧密结合，加深学生对国际前沿密码学技术、安全产品的理解。进而丰富国家安全、特别是网络空间安全的实践经验和动手能力，使学生加深对信息安全专业的热爱，培养民族使命感和责任感。

三、 实验的性质与任务

应用密码学课设是信息安全专业从理论走向实践的关键一环。通过本课程，学生可以在掌握现代密码学基本理论知识的基础上，以编程的方式实现各类具体的密码学应用，并能够较为完整地实现各类密码技术在主流应用场景下的关键功能。在课设实验过程中，学生可以将各类安全知识融会贯通。

本实验课程的主要任务是使学生掌握密码学实验的基本方法和技能，观察、分析各类密码学原语在各类密码应用中所发挥的作用和过程。在巩固所学的密码学知识的同时，更好地培养编程思维、逻辑能力和创新能力。

四、 实验教学内容与学时分配

序号	实验名称	学时	实验类型
1	密码算法加解密实验	4 天	验证性实验
2	哈希函数、认证与数字签名实验	5 天	验证性实验
3	密码算法综合应用实验	6 天	验证性实验

五、 实验安排与要求

应用密码学实验课程共 15 天学时，其中课程实验学时 15 天学时。学时分配如表 2 所示。

表 2 学时分配表

总学时	课程实验学时
15 天	15 天

1. 课程重点

通过本课程的学习，使学生能够对所学的技术原理、算法灵活运用，独立设计实现对称密钥加密、公开密钥加密以及信息内容摘要生成和验证，熟悉有关的密码编程环境、基本的函数库，掌握密码体系设计应用实现的要领。课程重点如下：古典密码算法、对称加密算法、非对称加密算法、HASH 算法、数字签名算法的编码实现、密码算法综合应用系统的编码实现。

2. 课程难点

古典密码算法，对称加密 DES 算法、非对称加密 RSA 算法、MD5 算法、数字签名 RSA 算法。

六、 实验教学与其它相关课程的联系与分工

本课程为信息安全专业的密码学课程设计课。本课程的先修课程：C 程序设计、计算机网络、信息安全导论、应用密码学。

七、 实验教学设计与教学组织

本课程所涉及到的知识理论性较强，对学生的编程能力有较高的要求。为使学生更好地理解和掌握密码学技术在生产中的具体应用。验证型实验报告内容包含实验步骤、实验结果与预期结果的差别，以及实验过程中遇到的问题及

解决办法。

鼓励学生组织学习小组，对密码学算法进行组内分工，以此来激发学生的学习热情，在充分调动学习积极性的同时加深对密码学知识的理解和感悟，提高学生的编程能力和素养，使学生更为深入地了解密码技术的实现细节。通过丰富的实际案例加深学生对相关抽象理论和算法过程的理解。通过课后撰写实验报告，使学生对课堂所学能够及时复习和巩固，对知识充分消化吸收。

此外，通过增强师生间、同学间的多种形式的讨论来提高课程的教学效果和教学质量。安排有课后答疑、课下讨论、网上讨论等环节，以多种方式帮助学生更好地掌握密码学思想，提高运用密码学技术解决实际问题的能力。

课程教学方法及具体要求如下：

1. 课堂讲授

1）在实验课随堂，先通过老师进行知识的简单梳理并进行必要的实践指导。在完成实验阶段，注重锻炼密码学思维、提高综合编程能力导向，注重理解应用密码学涉及到的各种密码学概念、理论和方法。为保证教学质量，课堂讲授中应重点突出、点面结合，既要保证完成使广大学生接受应用密码学知识体系结构的教学目标，又要针对关键问题、重点内容作较为详尽、多引入实例的透彻讲解，使学生真正领会和掌握本课程的知识要点。

2）结合生产生活中的实际案例，使同学对密码学设计方法有更为直观、深刻的认识，对于某些密码学技术的重点或难点，通过伪代码讲解来增强学生的感性认识，使学生更好、更快地掌握。

3）多媒体课件与代码演示相结合的教学手段与多种教学方法兼施并用。教学方法则采取在教师讲授基本教学内容的过程中适当穿插引入个体针对性提问、集体提问、答疑等教学形式。对个别的重点难点，鼓励学生在所讲授代码的基础上进行改进和创新，调动学生的学习热情，培养密码学思维，提高编程能力。

2. 讨论与自学

鼓励同学之间或同学与教师之间针对应用密码学课设中的重点、难点以及编程中遇到的各类困难等内容展开讨论，以澄清知识要点、扩大知识面和培养独立思考能力及创新能力。自学内容应以学生掌握相关知识结构基础上能比较方便地和理解为原则；对于有能力的同学，鼓励其将各种密码学相关算法程序进行一定量的扩展，封装成可重用模块，以提高解决实际问题的能力，培养工程能力，锻炼思维。

3. 课前预习和课后复习

实验前学生通过自学的方法做好实验的预习准备工作，最好写出预习报告。实验课完成后，在课外完成实验报告，同时完成与实验内容相关、适当数量的实验练习题(包括分析思考题)。建议学生课前预习相应教学内容；课后复习以

课堂讲授内容和实验内容为主线，对于密码学中的关键应用查阅拓展资料以更为深入地理解。

八、 实验教材、实验指导书及教学参考资料

1.实验教材

任课教师自编教材

2.参考资料

《密码学原理与实践》，Douglas R.Stinson 著 冯登国译，电子工业出版社，2009 年，9787121279713

九、 实验考核方法及成绩评定标准

本课程成绩采用百分制，总评成绩由平时成绩、实践教学成绩两部分组成，平时成绩占 30% （其中出勤成绩占 30%），实践设计成绩占 70%。

十、 大纲制(修)订说明

无

大纲执笔人：王宝成

大纲审核人：曾凡锋

开课系主任：肖珂

开课学院教学副院长：宋威

制（修）订日期：2022 年 2 月