《应用密码学实验》

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	7331001	学分	0.5	总学时	16	实验学时	16
课程名称	应用密码学实验						
课程英文名称	Applied Cryptography Experiment						
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						
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必修课。本课程为学生信息安全领域知识理论的学习奠定实践论基础，目的是让学生熟悉使学生学习和掌握信息安全所涉及的密码学中的基本理论和应用，掌握密码学的基本思想、基础理论和常用算法。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的发展及其研究的主要算法

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，加深学生对国家安全，特别是网络空间安全的理论知识学习，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

应用密码学实验是信息安全专业的重要的实践课程之一。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。在实验过程中，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	传统密码体制	2	验证性实验
2	分组密码－对称密码算法 DES	2	验证性实验
3	序列密码	2	验证性实验
4	Hash 算法 MD5 及 Hash 函数应用	4	验证性实验
5	非对称密码算法 RSA 及公钥密码算法应用	4	验证性实验
6	数字签名算法	2	验证性实验

五、 实验安排与要求

应用密码学实验课程共 16 学时，其中课程实验学时 16 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
16	16

1. 课程重点

代换密码算法；置换密码算法；DES 算法对实际的数据加密和解密；RC4 算法对实际的数据加密和解密；MD5 算法的加密过程；非对称密码算法 RSA 的加密和解密过程；比特币钱包地址的生成过程；数字签名算法

2. 课程难点

DES 算法对实际的数据加密和解密；RC4 算法对实际的数据加密和解密；MD5 算法的加密过程；Hash 函数应用于比特币“挖矿”的过程；比特币钱包地址的生成过程；数字签名算法

六、 实验教学与其它相关课程的联系与分工

本课程为现代密码学课程的后续实践课，需要学生对现代密码学的理论知识良好掌握的前提下，运用掌握的编程知识实现主流密码算法在实际生产生活中的应用。

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，本课程引入了区块链技术中所涉及到的相关密码学技术。通过对区块链中密码学技术的讲解及实验，使学生对本课程可以更好地理解和掌握，培养创新能力。每次实验前一周布置下次实验的目的、内容和要求，并提出预习要求。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）以锻炼密码学思维、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程的重点和难点内容展开讨论，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

《现代密码学教程》（第 1 版），谷利泽，郑世慧，北京邮电大学出版社，2009 年 8 月，9789563520190

九、 实验考核方法及成绩评定标准

本课程成绩由平时成绩和期末成绩两部分组成，以百分制计算。平时的实验过程成绩占 50%，实验报告成绩占 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