《现代密码学》实验教学大纲

适用专业：	信息安全	课程性质：	必做
课程编号：	0602003120	实验学时：	8
课程总学时：	48	开课学期：	第 5 学期
开课单位：	计算机工程教学实验中心		

一、实验目的与要求

本课程实验教学的目的是使学生通过软件编程掌握（1）实现古典密码学中的多表代换加密（Vigenere 加密）的密文进行破译的基本方法；（2）掌握 DES 加密算法、AES 加密算法，能够在实际的应用系统或安全系统中实现；（3）掌握公钥密码体制模型、RSA 算法、ECC 算法、基于 RSA 和 ECC 的数字签名机制；能够在实际应用中利用公钥密码算法及签名机制实现加解密、数字签名、公钥基础设施平台的能力。

实验要求学生掌握 Vigenere 加密的密文采用重合指数法进行破解的方法；掌握 DES、AES 分组加密算法；掌握 RSA 算法加解密及其数字签名机制；椭圆曲线加解密算法及其数字签名机制的设计与实现。掌握软件代码的调试方法，对程序运行的正确性进行反复测试，完成实验报告。

二、实验内容与学时分配

序号	实 验 项 目	实 验 内 容	学 时	实验类别	开出要求
1	多表代换 Vigenere 加解密算法及密钥破解算法的实现	1.使用 Vigenere 加密算法在字符集{a...z}上的密钥、明文消息的编码、加密算法的编程实现，明文消息存储在文本文件 plain.txt 中；（2）利用密钥对密文进行解密算法的编程实现；（3）唯密文攻击：给出一段 Vigenere 加密后的密文 cipher.txt，要求破解得到加密密钥 key，利用 key 进行解密得到明文文件 plain.txt，验证破解是否成功。	2	设计性	必 做
2	AES 加密、解密算法的实现	（1）绘制 AES-128 算法流程图；（2）建立一个明文文本文件 plain.txt，从中读取 16 个字节（字符）作为 AES 加密的一个分组（block）；（3）设置的一个 AES 加密算法的 KEY=128bits(16 个字节或 4 个字)；（4）编程实现对一个分组 16 个字符的 AES 加密，得到密文；（5）对步骤（4）得到的密文，	2	验证性	必 做

		编程利用密钥 key 进行解密，并验证 AES 加解密程序的正确性。			
3	利用 RSA 算法实现加解密、数字签名	（1）大整数素性的判定算法以及编程实现；（2）大整数的运算（乘法、幂模）算法技巧及编程实现；（3）扩展的 Euclid 算法求一个整数关于模运算的乘法逆元；（4）RSA 算法中公钥、私钥的生成算法及编程实现；（5）用于 RSA 算法的明文消息的编码、分组方法及编程实现；（6）对一个明文分组的 RSA 加、解密算法的编程实现；（7）对一个消息 m 进行数字签名算法及验证签名的算法的编程实现。	2	验证性	必 做
4	椭圆曲线加密算法的设计与实现	（1）选定一个椭圆曲线：$E_{89}(-1,0)$：$y^2=x^3-x \pmod{89}$；（2）编程计算该椭圆曲线上所有在有限域 GF(89)上的点；（3）编程实现椭圆曲线上任意一个点 P(例如 P=(12,5))的倍点运算的递归算法，即计算 k*P(k=2,3,...)；（4）利用此递归算法找出椭圆曲线上的所有生成元 G 以及它们的阶 n，即满足 n*G=O；（5）设计实现某一用户 B 的公钥、私钥对的生成算法，即得到 public key=(n, G, PB, E_p(a, b)) secure key=nB(小于 n)。假如用户 A 发送明文消息“yes”并加密传输给用户 B，用户 B 接收消息后要能解密为明文。试用 ECC 密码体制实现此功能。	2	设计性	必做

三、实验进程安排

序号	实 验 项 目	实 验 内 容	学 时	开出要求	开出时间
1	多表代换 Vigenere 加解密算法及密钥破解算法的实现	1.使用 Vigenere 加密算法在字符集{a...z}上的密钥、明文消息的编码、加密算法的编程实现，明文消息存储在文本文件 plain.txt 中；（2）利用密钥对密文进行解密算法的编程实现；（3）唯密文攻击：给出一段 Vigenere 加密后的密文	2	必做	14 周

		cipher.txt, 要求破解得到加密密钥 key, 利用 key 进行解密得到明文文件 plain.txt, 验证破解是否成功。			
2	AES 加密、解密算法的实现	(1)绘制 AES-128 算法流程图；（2）建立一个明文文本文件 plain.txt, 从中读取 16 个字节（字符）作为 AES 加密的一个分组（block)；(3）设置的一个 AES 加密算法的 KEY=128bits(16 个字节或 4 个字)；(4）编程实现对一个分组 16 个字符的 AES 加密，得到密文；(5）对步骤（4）得到的密文，编程利用密钥 key 进行解密，并验证 AES 加解密程序的正确性。	2	必做	15 周
3	利用 RSA 算法实现加解密、数字签名	(1）大整数素性的判定算法以及编程实现；(2）大整数的运算（乘法、幂模）算法技巧及编程实现；(3）扩展的 Euclid 算法求一个整数关于模运算的乘法逆元；(4）RSA 算法中公钥、私钥的生成算法及编程实现；(5)用于 RSA 算法的明文消息的编码、分组方法及编程实现；(6）对一个明文分组的 RSA 加、解密算法的编程实现；(7）对一个消息 m 进行数字签名算法及验证签名的算法的编程实现。	2	必做	16 周
4	椭圆曲线加密算法的设计与实现	(1）选定一个椭圆曲线: $E_{89}(-1,0)$: $y^2=x^3-x \pmod{89}$; (2）编程计算该椭圆曲线上所有在有限域 GF(89)上的点;(3）编程实现椭圆曲线上任意一个点 P(例如 P=(12,5))的倍点运算的递归算法，即计算 k*P(k=2,3,...)；(4）利用此递归算法找出椭圆曲线上的所有生成元 G 以及它们的阶 n，即满足 n*G=O；(5）设计实现某一用户 B 的公钥、私钥对的生成算法，即得到 public key=(n,	2	必做	17 周

		G, PB, $E_p(a, b)$) secure key=nB(小于 n)。假如用户 A 发送明文消息“yes”并加密传输给用户 B，用户 B 接收消息后要能解密为明文。试用 ECC 密码体制实现此功能。			

四、考核方式

《现代密码学》实验成绩由实验报告、四个实验中程序的运行结果及测试分析报告二个部分组成，前者占成绩的 40%，后者占成绩的 60%。

五、使用主要仪器设备说明

PC 机，Windows OS 或 Linux OS，C/C++/java/python 等开发环境皆可以满足需要。

六、教材及参考书

1. 谷利泽，郑世慧，杨义先. 现代密码学教程. 北京邮电大学出版社，2015.3（教材）。

2．B. Schneier. Applied cryptograghy second edition: protocols, algorithms, and source code in C. NewYork: John Wiley & Sons, 1996. 中译本：吴世忠，祝世雄，张文政译。