安 徽 理 工 大 学

学 期 授 课 计 划

周　数____10____
讲　课____40____学时
习题课____　____学时
实　验____8____学时
总　计____48____学时

教师姓名 方贤进　2017/2018 学年　第 1 学期
课程名称 现代密码学　系别　信息安全　班级信息安全 15-1.2 班

月份	周次	章节和内容摘要	讲授时数	习题课时数	实验时数	课外作业及测验题目	备注
11	11	**Δ课程导入内容**	1				
11	11	**第 1 章　密码学概论**	2				
11		1.1 信息安全与密码学					
11		1.2 密码学发展史					
11	12	**第 2 章　密码学基础**	2				
11		2.1 密码学分类					
11		2.2 保密系统模型					
11		2.3 认证系统模型					
11	13	**第 3 章　古典密码体制**	4				
11		3.1 置换密码					
11		3.2 代换密码					
11		3.3 古典密码体制分析					
11	14	**第 4 章　分组密码**	6				
11		4.1 分组密码的定义					
11		4.2 分组密码的发展史					
12	15	4.3 DES 算法					
12		4.4 AES 算法					
12		4.5 分组密码算法的运行模式					
12	15	**第 5 章　序列密码**	4				
12		5.1 序列密码简介					
12		5.2 线性反馈移位寄存器					
12	16	5.3 m 序列及其生成算法					
12		5.4 m 序列密码的破译					
12		5.5 A5 算法					
12	16	**第 6 章　HASH 函数与消息认证码**	5				
12		6.1 hash 函数的定义					
12		6.2 hash 函数的通用结构					
12		6.3 MD5 算法及其它 hash 函数					
12		6.4 消息认证					
12		6.5 生日攻击					
12	17	**第 7 章　公钥密码体制**	8				
12		7.1 公钥密码体制的基本概念					
12		7.2 RSA 算法					

1		7.3 椭圆曲线加密算法					
1	19	**第 8 章 数字签名技术**	4				
1		8.1 数字签名简介					
1		8.2 基于 RSA 数字签名					
1		8.3 基于 ECC 数字签名					
1	20	**第 10 章 密钥管理**	4				
1		10.1 密钥管理的简介					
1		10.2 密钥的生命周期					
1		10.3 公钥证书					
1		10.4 密钥分配					
1		10.5 密钥协商					
1		10.6 密钥托管					
1		10.7 密钥分割					
		设计性实验	8				
12	14	设计性实验一：多表代换 Vigenere 加密算法及秘钥破解算法的实现			2		
12	15	验证性实验二：AES 加密、解密算法的实现			2		
12	16	验证性实验三：利用 RSA 算法实现加解密、数字签名			2		
12	17	设计性实验四：椭圆曲线加密算法的设计与实现			2		
		总学时	48		8		
教学参考书籍		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。 3. 马春光. 现代密码学教程，哈尔滨工程大学自编讲义。 4. 所有材料可从课程建设网站：http://star.aust.edu.cn/~xjfang/crypto/获取。					

教研室主任_____（签名） 院或系部主任_____（签名）2017 年 10 月 23 日

注：本表一式三份，于授课前填写好，分别交所在院系、教务处各一份，本人留存一份。