1．授课内容

序号	教学内容	教学要求
1	数论： 1. 认识数论，数论研究范畴； 2. 带余除法与辗转相除，最大公因数的求法； 3. 二元一次不定方程及多元一次不定方程； 4. 背包问题及公钥算法，构造背包公钥算法（第一步）；	1. 理解带余除法的意义（与后面整数环的概念呼应）； 2. 掌握辗转相除及回带的计算方法； 3. 掌握二元一次不定方程的解法； 4. 初步理解公开密钥体制的含义及其构建原理，掌握基于背包问题构造公钥体制的思路。
2	数论： 1.同余方程初步，背包算法构造； 2.素数与合数，整数唯一分解； 3.剩余系与欧拉函数； 4.欧拉函数的计算；	1.掌握一次同余方程的概念及解法； 2.基于不定方程和同余方程完成背包公钥体制的构建； 3.理解整数唯一分解定理； 4.掌握欧拉函数的概念及计算方法。
3	数论： 1.欧拉定理与费马小定理； 2.RSA 算法的数学原理； 3.RSA 算法实现中的若干问题；	1.理解欧拉定理与费马小定理； 2.了解 RSA 算法的背景； 3.理解 RSA 算法的流程、数学原理及安全性分析； 4.了解 RSA 算法在实际使用中的安全和计算问题。
4	数论： 1.一次同余方程与同余方程组； 2.一般同余方程的概念； 3.快速模幂、零知识证明。	1.了解中国剩余定理，及同余方程组的解法； 2.了解一般同余方程的形式及求解思路； 3.基于上述数学原理，了解快速模幂的计算方法及原理； 4.了解零知识证明的概念。
5	数论： 1.认识素数，素数的数量； 2.关于素数的著名猜想； 3.梅森素数与完全数。	1.理解无穷多素数定理的证明； 2.了解素数计数定理的含义； 3.了解哥德巴赫猜想、孪生素数猜想等关于素数的著名数学猜想； 4.了解梅森素数与完全数的含义。
6	数论： 1.模数的阶，及其计算； 2.原根，及其计算； 3.D-H 算法、ElGamal 算法的数学原理。 4.素数的判断。	1.理解阶的概念，了解阶的计算方法； 2.理解原根的概念，了解原根的计算方法； 3.了解 D-H 算法的数学原理，了解离散对数问题及其在构建公钥体制中的作用； 4.了解常见的几种素性判别法：整除判别法、威尔逊判别法、莱美判别法、普罗兹判别法。
7	近世代数： 1.近世代数的介绍，代数结构的概念； 2.集合上的二元运算； 3.群的概念及举例； 4.子群的概念及举例。	1.了解代数结构的概念； 2.理解集合上二元运算的概念； 3.理解群的概念，掌握群的判断方法； 4.理解子群的概念。
8	近世代数： 1.循环群及其生成元； 2.置换与对称群； 3.古典密码的群描述； 4.群上离散对数。	1.理解循环群、生成元、阶的概念； 2.了解置换的定义，以及基于置换集合构建的群（对称群）； 3.了解希尔密码、置换密码、代换密码的原理，以及用群的方式如何描述；

		4.了解群上离散对数问题。
9	近世代数： 1.环的定义及举例； 2.零因子与整环； 3.理想和主理想； 4.环上的多项式，多项式环。	1.理解环的定义，及与体、域的关系； 2.理解零因子和整环的概念，通过零因子深化对代数结构的理解； 3.了解理想和主理想的概念； 4.理解环上多项式的概念，能判断环上多项式构成的代数结构； 5.了解循环吗与多项式环的关系。
10	近世代数： 1.域的定义及举例； 2.有限域，GF(2)； 3.域的基本性质； 4.域上多项式。	1.理解域的定义及判断方法； 2.理解有限域，特别是 GF(2)； 3.了解域的基本性质，对比群、环的性质，深入理解代数结构的含义； 4.了解域上多项式的概念。
11	近世代数： 1.多项式的带余除法，公因式、公倍式的求法； 2.既约多项式，既约多项式分解； 3.多项式的同余，剩余类； 4.子域、扩域，数据组与多项式。	1.掌握多项式的带余除法、欧几里得算法； 2.理解多项式的同余、剩余类、既约以及多项式的既约多项式分解等概念； 3.理解子域、扩域的概念，了解数据组与多项式的关系； 4.了解 AES 算法中涉及到的运算，及其与多项式的关系。
12	近世代数： 1.有限域的加法特性； 2.域的特征，二项式运算； 3.有限域的乘法特性； 4.本原元与生成元； 5.最小多项式与本原多项式。	1.了解有限域的特征与有限域元素数量之间的关系； 2.了解有限域的乘法特性，结合循环群的概念，进一步理解阶的概念； 3.了解本原元与生成元的概念，以及最小多项式和本原多项式的概念； 4.了解椭圆曲线的概念及 ECC 的构造。
13	数理逻辑： 1.逻辑学与数理逻辑的介绍； 2.命题、命题变量、命题常量； 3.命题联结词与真值； 4.命题逻辑公式，逻辑等价式。	1.理解命题逻辑中的基本概念； 2.掌握命题逻辑公式与自然语言之间的转换； 3.掌握命题逻辑公式等值判断的方法； 4.理解永真式、矛盾式、命题公式的等值等概念； 5.了解命题逻辑公式的逻辑等价式。
14	数理逻辑： 1.命题逻辑公式的等值演算； 2.命题逻辑公式的范式； 3.命题演算系统。	1.了解等值演算、限制性公式的概念； 2.了解范式的概念； 3.理解命题演算系统的定义及演算方法； 4.通过实例了解命题演算系统的推理流程。
15	数理逻辑： 1.一阶逻辑的概念； 2.一阶逻辑语言的符号及项； 3.合式公式，换名规则与替换原则； 4.等值式与前束范式；	1.了解一阶逻辑与命题逻辑的区别； 2.了解一阶逻辑语言的符号、项等概念； 3.了解合式公式，能够使用换名规则、替换原则； 4.了解等值式，了解前束范式的概念。
16	数理逻辑： 1.一阶逻辑推理及推理定理； 2.全称量词的消除和引入；	1.了解一阶逻辑推理的概念、推理定理； 2.能够使用全称量词和存在量词的消除和引入规则对公式进行变换；

	3.存在量词的消除和引入； 4.非经典逻辑，模态逻辑。	3.了解非经典逻辑的范畴； 4.了解模态逻辑的定义和基本概念。

2．实验内容

序号	实验内容	教学要求说明
1	数论基础算法的计算机实现： 1.辗转相除法的实现及应用； 2.素性判断方法的实现。	1.掌握辗转相除法的计算机实现； 2.掌握基于辗转相除的最大公因数、最小公倍数的计算； 3.掌握一种素性判断法的计算机实现。
2	RSA 算法数学原理的计算机实现与验证： 1.快速模幂算法的实现； 2.公钥、私钥的生成； 3.加密、解密模块的实现。	1.掌握快速模幂算法的计算机实现； 2.掌握 RSA 公钥体制的实现方法； 3.掌握 RSA 密钥对的生成方法及计算机实现； 4.掌握 RSA 算法加解密算法的计算机实现。
3	有限域算法的计算机实现： 1.GF(2)上多项式的基本运算； 2.GF(2)上多项式的辗转相除法； 3.GF(2)上多项式的最大公因式、最小公倍式的计算。	1.多项式基本运算的计算机实现，包括加、减、乘、模； 2.多项式的辗转相除法的计算机实现； 3.基于辗转相除法的多项式最大公因式、最小公倍式的计算机实现。
4	AES 算法数学原理的计算机实现与验证： 1.GF(2^n)上的运算及辗转相除； 2.AES 算法中的加法、乘法及循环移位算法。	1.GF(2^n)上多项式基本运算的计算机实现； 2.AES 算法中基本运算的计算机实现； 3.AES 算法流程的部分计算机实现。