第一节课，密码学简介

密码学发展的历史

古典、近代、现代的不同特点

里程碑与图灵奖

国产密码发展历程

密码学相关术语和概念

公钥密码学 vs 私钥密码学

非对称加密 vs 对称加密

公钥加密 vs 私钥解密

4种攻击（COA，KPA，CPA，CCA）

第二节课，古典密码学

代换密码分类

1.1 Monoalphabetic cipher单字母单表密码

(1) 加法密码：Caesar cipher (Shift cipher)凯撒密码

(2) 加乘密码：Affine cipher仿射密码

(3) 混合密码：Mixed alphabetic cipher混合字母表密码

1.2 Polyalphabetic cipher单字母多表密码

(1) 周期多表代换：Vigenère cipher维吉尼亚密码

(2) 周期多表代换：Rotor machine转轮密码机(1870-1943)

(3) 无限多表代换：One-time pad (OTP)一次一密

1.3 Multiple letter cipher多字母密码

(1) 2字母代换：Playfair普莱菲尔密码

(2) 3字母代换：Hill密码

1.4 代换密码安全性分析

置换密码举例

2.1 无密钥置换(Keyless)：Rail Fence cipher栅栏密码

2.2 有密钥置换(Keyed)：Column Transposition Cipher列移位密码

第三节课，分组密码-数据加密标准DES

分组密码概述

1.1 什么是分组密码/块密码(Block Cipher)

1.2 分组密码的作用

分组密码设计准则

2.1 混淆(Confusion)：密文和密钥之间的统计关系复杂

2.2 扩散(Diffusion)：明文统计特性散布到密文中

分组密码设计方法

3.1 乘积(Product)

3.2 迭代(Round)

数据加密标准(DES)

4.1 简化版DES算法原理

4.2 DES算法产生及原理

4.3 DES算法安全性分析：穷举、差分、线性

第四节课，密码学数学基础-I

群环域的概念，尤其是有限域GF(p)

定义在有限域GF(2)上的多项式和n次模不可约多项式，构成了多项式有限域，记为GF(2^n)

第五节课，AES算法

AES概述

简化版AES

AES结构的子模块

AES中的密钥扩展和解密

SM4简介

简化版AES算法中加密和密钥生成的过程，其中Mix Column中关于多项式有限域的计算

第六节课，分组加密操作模式ECB，CBC，CFB，OFB，Counter

操作模式的设计结构和对应的优缺点

填充问题

第七节课，序列密码

定义概念

线性移位寄存器，序列密码中线性反馈移位寄存器的执行过程，如何设计移位寄存器可以输出m序列

第八节课，数论基础

整除性和带余除法,最大公因子

素数和模运算

欧几里得算法和扩展欧几里得算法

费马小定理和欧拉定理

素性检测

中国剩余定理

离散对数

第九节课，公钥密码体制+RSA

公钥加密的定义

RSA公钥加密算法步骤

RSA公钥加密算法正确性推导

RSA公钥加密算法面临的共模、低指数、选择密文攻击

第十节课，Rabin加密算法，ElGamal加密算法，ECC加密算法

Rabin加密算法的步骤，如何正确解密，与RSA加密算法的相似性比较

ElGamal加密算法的步骤，安全性为何基于离散对数困难问题，如何正确解密

ECC加密算法的步骤，安全性为何基于椭圆曲线离散对数问题，点加运算如何执行，与ElGamal算法的相似性比较

第十一节课，Hash

哈希函数的应用

密码学哈希函数的安全要求

穷举攻击、生日悖论

安全哈希函数的一般结构

安全哈希算法(SHA)

第十二节课，消息认证

消息认证及消息认证码

消息认证码的要求

基于哈希函数的MAC

基于分组密码的MAC

第十三节课，数字签名和公钥密码基础设施

数字签名与消息认证码的区别

RSA数字签名算法步骤和不足

子群和循环群的概念

ElGamal数字签名算法步骤

Schnorr数字签名算法步骤

公钥密码基础设施PKI的架构，CA的作用

第十四节课，安全多方计算专题

第十五节课，零知识证明介绍