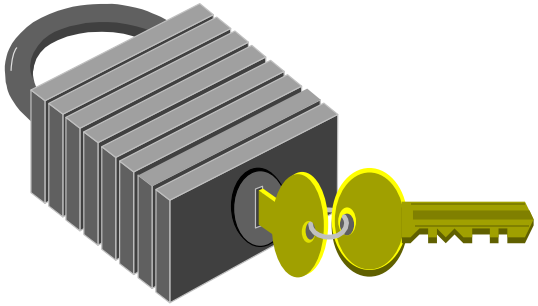

密码学复习提纲

任课教师：胡丽琴
网络空间安全学院

密码学概念及安全性基础

- 密码学的四个发展阶段：
  - 古典密码术
  - 机器密码时代
  - 传统密码学
  - 公钥密码学
- 古典学密码体制对现代密码学的研究具有十分重要的意义，实现古典密码体制的两种基本方法：代替和置换
- 按照对明文的操作，古典密码分为替换密码和置换密码
- 柯可霍夫原则：
  - 密码系统的安全性不能取决于算法，而应取决于密钥。

密码学概念及安全性基础

- 密码学的基本原理(含流程图)及有关步骤说明
- 基本原理
  - 发送方将要传输的明文通过加密算法与加密密钥加密成密文
  - 接收方接收密文，将密文通过解密算法与解密密钥解密成明文
  - 通过这种方式保护了消息的机密性，敌手即使截获密文也无法恢复出明文

密码学概念及安全性基础

- 两类重要密码体制，即对称密码体制和非对称密码体制的主要特点
- 对称密码算法：加密密钥＝解密密钥，加密算法与解密算法类似
- 公钥加密算法：加密密钥≠解密密钥，加密算法与解密算法差别很大
- 对称密码算法：效率高，密钥管理复杂
- 公钥加密算法：效率低，配合公钥数字证书可解决密钥管理问题

密码学概念及安全性基础

- 对称密码按照对明文处理的方式不同可以分为两类：流密码与对称密码。掌握各类密码的典型密码算法。
  - RC4，ZUC，DES，AES，SMS4，IDEA等
- 公钥密码体制的安全基础是某些数学上的计算困难性问题。根据公钥密码体系的安全性基础来分类，现在被认为安全、实用、有效的公钥密码体系有三类。请说明这三类问题的具体含义，各基于什么困难问题。

流密码

- 流密码基本概念与构造原理
  - 流密码的基本思想是什么？
  - 流密码和分组密码是任何区分的？
  - 流密码的典型密码算法
- LFSR(线性反馈移位寄存器)的基本概念与原理
- 密码流生成方法

分组密码

- 现代对称密码的设计基础：扩散和混淆
- 数据加密标准DES、AES、SMS4等算法原理与基本特性（如分组大小、密钥长度、循环次数、轮/圈变换由哪4个变换组成等）
- DES和AES进行比较，各有什么特点和优缺点
- 优点：“DES”：运算速度快，资源消耗较少；“AES”：运算速度快，安全性高，资源消耗少
- 缺点：“DES”：安全性低

Hash函数

- Hash函数的概念和基本性质
  - 概念：将任意长度的消息映射成某一固定长度的消息的一种函数

Hash函数

- Hash函数的基本性质
  - 单向性：对于给定的Hash值y，要找到x使得，$h(x)=y$在计算上是不可行的/计算上是困难的。
  - 弱抗碰撞性：已知消息 x，寻找另一个不同的消息 x'，使得$h(x) = h(x')$ 是计算上不可行的，使得在计算上是困难的。
  - 强抗碰撞性：寻找两个不同的消息 x 和 x'，使得 $h(x) = h(x')$ 是计算上不可行的。

Hash函数

- MD5、SHA-1等典型Hash函数算法的基本特性
  - 算法结构
  - 输出位数，即消息摘要长度
  - 安全性
- Hash函数是不是加密算法？为什么？
- Hash函数在信息安全领域的应用有哪些？

公钥密码

- 对称密码算法和公钥密码算法区别及在应用中的优缺点
  - 对称密码算法：加密密钥＝解密密钥，加密算法与解密算法类似
  - 公钥加密算法：加密密钥≠解密密钥，加密算法与解密算法差别很大
  - 对称密码算法：效率高，密钥管理复杂
  - 公钥加密算法：效率低，配合公钥数字证书可解决密钥管理问题

公钥密码

- 公钥密码算法用于加密与签名的主要不同之处
- 区别：公钥加密的接收方收到的是密文，数字签名的接收方收到的是(明文，签名)
- 公钥加密最后的输出是解密后的明文，数字签名最后的输出是是否验证通过
- 公钥加密用公钥加密，用私钥解密；数字签名用私钥签名，用公钥验证

公钥密码

- RSA与ElGamal加密与签名算法的整个步骤
- 熟练掌握RSA与ElGamal加密算法的应用方法(实例计算)
- 椭圆曲线上的基本运算及概念（点加法、倍点等）
- 熟练掌握椭圆曲线密码加解密算法的应用(实例计算)

数字签名

- 数字签名的概念，基本特性，由哪几部分组成?
- 数字签名的应用过程
- 熟练掌握典型公开密钥密码体制的数字签名算法(RSA、ElGamal)原理、计算方法与应用

密钥管理理

- 密钥管理基本内容和概念
- 理解密钥分配与密钥协商的目标与特点
- 掌握数字证书的概念与基本内容
  - 概念、组成、标准、格式等
- 掌握Diffie-Hellman密钥交换算法及安全性基础，并能熟练运用该算法建立一个双方共享的密钥(描述或实例计算)。