2023-2024-2《应用密码学》复习提纲

- 第一章（ 1.3, 1.4 ）

  1、密码学的基本概念、密码体制构成（五元组）、分类

  2、分析密码算法的方法、密码体制攻击方法（唯密文攻击、已知明文攻击、选择明文攻击、选择密文攻击和选择文本攻击）

- 第二章（2.3）

  1、 古典密码的基本概念

  2、 替换密码和换位密码的基本概念 （替换：摩斯密码、单字符单表替代（凯撒、仿射）、多字符多表替代（维吉尼亚、Hill）。换位：滚筒密码，列换位密码）

  3、 仿射密码，维吉尼亚密码加密和解密过程

  4、 古典密码的安全性分析

- 第四章（4.1, 4.2，4.3, 4.4, 4.7）

  1、分组密码基本概念、原理，常见的对称密码算法 DES、AES 等，国密 **SM4 算法的分组长度，密钥长度等**

  2、DES 算法、AES 算法的相关概念（密钥长度、分组长度、轮次等）

  3、多重 DES 算法密钥长度 (三重 EDE2 EEE3)

  4、DES 算法轮结构（S 盒），AES 算法整体结构、AES 算法四个基本变换（S 盒等），有限域上字节的表示、基本运算（16 进制和 2 进制的转换）

  5、分组密码算法五种基本模式（ECB、CBC、CFB、OFB、CTR）的加解过程、特点、差错传播、特性比较等

- 第五章（5.2, 5.3）

  1、序列密码分类（同步序列密码和自同步序列密码）

  2、线性反馈寄存器（线性反馈移位寄存器的反馈函数，特征多项式，周期，输出序列，m 序列）

- 第六章（6.1、6.2）

  1、 非对称密码概述（分类：基于大整数因式分解困难性问题、基于离散对数困难性问题、基于椭圆曲线离散对数困难问题等等，对称密码算法和非对称密码算法区别）

  2、 RSA （RSA 算法密钥生成、加密和解密）模幂运算（Fermat 小定理，模重复平方，欧几里得扩展算法求逆），RSA 算法安全性 RSA 加密解密实现（第 2 次实验）

  3、 对称密码和非对称密码区别

- 第七章（7.1，7.2， 7.3.1，7.5）

  1、Hash 函数概念和安全性要求、MD5 算法的概念、SHA 系列和**国密 SM3 算法**的摘要值长度

  2、SHA-1 算法（算法流程、SHA-1 数据填充和数据扩充（ASCII 码、16 进制和 2 进制的转换）

  3、消息认证（消息认证和消息认证码的基本概念、三种使用方式（206 页））

- 第八章（8.1, 8.2, 8.3.1）
  1、数字签名原理
  2、数字签名分类
  3、RSA 数字签名算法
  4、盲签名

- 第九章（9.1）
- 1、认证协议(单向认证协议和双向认证协议、有无第三方参与）的理解
- 2、认证模型和保密通信模型的理解
- 3、身份认证技术（概念及几种常见的认证技术）

- 第十章（10.1, 10.2, 10.3, 10.5.1 10.5.3）
  1、密钥组织结构和 密钥分类（基本密钥、主密钥、密钥加密密钥、会话密钥）
  2、密钥管理的内容
  3、DH 密钥协商协议 （DH 密钥协商协议、中间人攻击）
  4、STS 协议（如何防止中间人攻击）

考试题型

一、选择题（30 分，2 分/每题，15 题），
二、判断题（10 分，1 分/每题，10 题）
三、填空题（10 分，1 分/每空，10 空）
四、简答和计算（30 分，6 分/每题，5 题）
五、综合计算题（20 分，10 分/每题， 2 题）