**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（10）

密码编码学，密码分析学，密钥密码学

密码体制构成（五元组）

M，C，K，E，D

分类

执行操作方式：替换和换位

收发双方密钥是否相同：对称和非对称

分组和序列，序列还与密文在明文中的位置有关（15）

加密变换是否可逆：单向和双向

是否引入客观随机因素：确定和概率

* 1. 分析密码算法的方法

穷举法，统计分析法，，密码体制分析法

密码体制攻击方法

1. 唯密文攻击：密文+加密算法->明文->密钥
2. 已知明文攻击：密文+加密算法+明文->密钥
3. 选择明文攻击：加密算法+选择明文->密文->密钥
4. 选择密文攻击：加密算法+选择明文+密文->密钥
5. 选择文本攻击：->选择明文+选择密文

* 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）

* 1. 仿射密码，维吉尼亚密码加密和解密过程
  2. 古典密码的安全性分析

加解密适用于所有密钥空间中的元素（2）系统便于实现和使用（3）达不到理论不可破，也应当实际不可破（4）安全性不能依赖于算法保密，而应该依赖于密钥保密。

* 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

1. DES：明文分组长度**64**bit，密钥长度**64**bit，密钥中有**8**位奇偶校验位，有效密钥长度要将奇偶校验位去除，即一重des，有效密钥长度是**56**bits，3重为56\*3=162；轮次：**16**轮
2. AES有三种分组：明文128、192、256bits。密钥长度分别有：128、192、256分组。所以一共有3\*3=9种，但是！！！！NIST选中的AES限定明文分组是128bits，所以根据密钥长度决定进行的轮数！！ 密钥长度对应的轮数为：128：10轮。192：12轮。256：14轮
3. 国密**SM4**算法： 明文分组长度/密钥长度128bit
   1. DES 算法、AES 算法的相关概念（密钥长度、分组长度、轮次等）
   2. 多重 DES 算法密钥长度 (三重 EDE2 EEE3 ) 3：168，2：112
   3. 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）
   4. 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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 加解过程 | 特点 | 差错传播 | 特性比较 | 同步（独立） |
| ECB | 电子码本 | 见书 | 无差错传播 | 分组密码 | √ |
| CBC | 密码分组链接 | 有 | 分组密码 |  |
| CFB | 密码反馈 | 有 | 将分组密码作为序列密码密钥流生成器 |  |
| OFB | 输出反馈 | 同步流缺点 | √ |
| CTR | 计数器 | 无，同步流缺点 | √ |

* 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

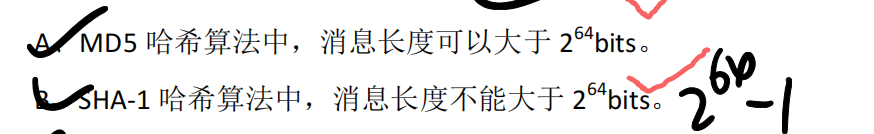
****对称****加密要求发送方和接收方在安全通信之前商定一个密钥。 优势在于加密效率高，因为加密和解密使用相同的算法和密钥。 然而，对称加密的安全性较低，因为如果密文被拦截且密钥被破解，信息就很容易被破译。 常见的对称加密算法包括DES、AES和3DES等。

非对称加密，与对称加密不同，它使用一对密钥：公钥和私钥。 公钥用于加密数据，而私钥用于解密数据。 私钥只能由一方安全保管，不能外泄，而公钥可以发给任何请求它的人。 非对称加密提供了更高的安全性，因为公钥和私钥是相互独立的，使用其中一个密钥加密的数据只能由另一个密钥解密。

* 第七章（7.1，7.2, 7.3.1，7.5）
  1. Hash 函数概念和安全性要求：见另一个

MD5 算法的概念：接收任意长度的消息作为输入，并生成128bit的哈希值

SHA 系列和国密**SM3**算法（256bit）的摘要值长度



* 1. 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）

认证分为三个子概念：消息认证（数据源认证）、实体认证，认证密钥的建立

* 1. 消息认证

消息认证：用消息的密文本身充当认证消息

消息认证码（MAC）的基本概念：以消息和密钥作为输入的公开函数产生的认证消息

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：基于对称/非对称，对称需要第三方，所以一般用非对称
    2. 数字签名分类（基于大整数因式分解数字签名、基于离散对数数字签名、基于椭圆曲线离散对数数字签名）
    3. RSA 数字签名算法
    4. 盲签名：基于大数
* 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）

口令认证（安全，静态，动态）、IC卡认证、个人特征（指纹，语音，视网膜等）、基于零知识证明

* 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

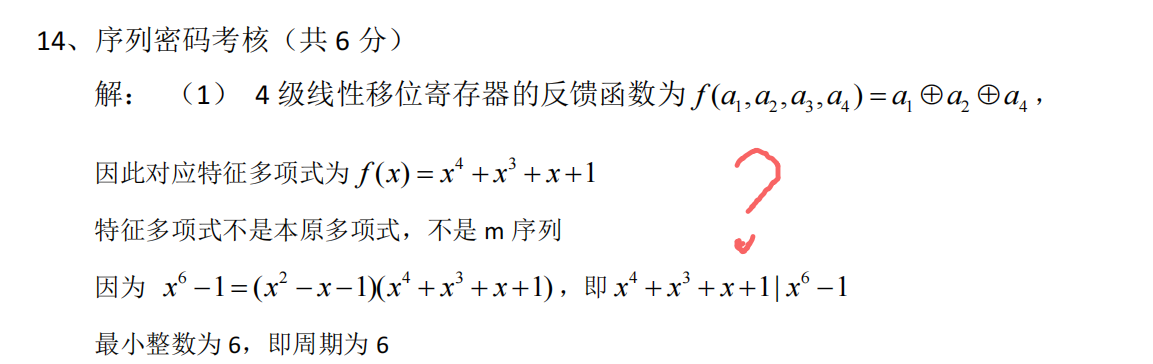
管理方式、密钥的生成、使用，存储，备份与恢复，更新，销毁

* + 1. DH 密钥协商协议 （DH 密钥协商协议、中间人攻击）
    2. 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）



**DH**