《信息安全支撑技术》知识点串讲

第一节 密码技术

1. 密码学发展阶段：古典、近代、现代和公钥密码学及特点。
2. 密码系统组成：**明文、加密、密钥、解密、密文**。
3. **柯克霍夫**原则：密钥保密，算法公开。
4. 对称密码算法

（1）加密密钥和解密密钥相同，或实质上等同。

（2）典型算法：DES、3DES、**AES、IDEA**、RC5、Twofish、CAST-256。

（3）AES 算法：128/192/256bits 三种密钥长度。

（4）优点：**高效**。不足：交换密钥问题及密钥管理复杂。

5. 非对称密码算法：

（1）典型算法：**RSA**、**ECC**、ElGamal

（2）原理：基于数学难题实现，**大整数分解**、**离散对数**、**背包问题**。

（3）优点：解决**密钥传递**问题、密钥管理简单、提供数字签名等其他服务。缺点：计算复杂、**耗用资源大**。

6. 哈希函数：

（1）作用：完整性校验；

（2）主要算法：MD5、SHA-1、**SHA-256\384\512**。

（3）特点：具有**单向性**、定长输出、抗碰撞性（强弱之分）。

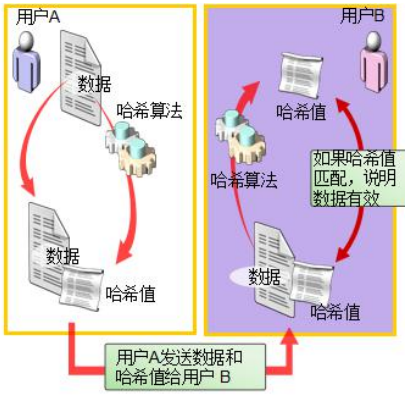
7. 消息鉴别码：

（1）**消息认证、完整性校验、抗重放攻击**（时间或顺序号验证）；

（2）消息认证方式：**MAC**、**HMAC**。

8. 数字签名：

（1）原理：见图。



（2）作用：身份鉴别、不可抵赖、消息完整性。

9.数字证书：

（1）一段电子数据，是经证书权威机构 CA 签名的、包含拥有者身份信息和密钥的电子文件。

（2）数字证书格式：国际标准 **X.509** 定义一个规范的数字证书格式，版本 v3。

（3）证书生命周期：证书申请、生成、存储、发布、使用、冻结、更新、废止等。

10.PKI 体系构成及作用

（1）KMC 或 KMS（**密码系统**）

（2）CA（**认证权威**）
（3）RA（**注册权威**）
（4）LDAP(**证书管理目录服务**）
（5）CRL&OCSP（**黑名单库或在线认证**）
（6）终端实体（持有 USB-Key 和程序）

11.区块链（了解，考试不考）

（1）区块链是分布式数据存储、点对点传输、密码技术等计算机技术的新型应用模式，解决了去中心化的共识机制的建立和应用。
（2）区块链的基本特征：去中心化、开放性、自治性、信息不可篡改、基于场景的匿名性。
（3）区块链技术：分布式账本、非对称加密和授权技术、共识机制、智能合约。

第二节 标识和身份鉴别技术

1. **标识**：实体身份的唯一性表达。
2. **鉴别**：确认实体是它所声明的，提供了关于某个实体身份的保证，某一实体确信与之打交道的实体正是所需要的实体。
3. 鉴别系统的构成：**验证者、被验证者、可信赖第三方**。
4. 鉴别的类型：**单向**鉴别、**双向**鉴别、**第三方**鉴别。
5. 鉴别的方式：

（1）基于实体**所知**：知识、密码、PIN 码等。
（2）基于实体**所有**：身份证、**钥匙**、**智能卡**、令牌等。
（3）基于实体**特征**：**指纹**，笔迹，**声音**，视网膜等。
（4）分类：**单因素、双因素、多因素**认证

6.实体所知：1）安全密码 2）锁定机制 3）验证码 4）输入控件 5）一次一密 6）哈希传输保护 7）挑战应答机制。
7.实体所有：1）复制技术难度；2）复制的成本方面。要求所有的实体具有唯一性。
8.实体特征：

1）原则：最小化、不干扰、长期性、稳定性。
2）方式：指纹；掌纹；虹膜；视网膜；静脉；声音；扫脸；步态等识别。
3）生物特征鉴别系统的有效性判断
   - **错误拒绝**率（FRR）
   - **错误接受**率（FAR）
   - 交叉判错率（CER）：FRR=FAR 的**交叉点**，CER 用来反映**系统准确度**。

9.身份鉴别的应用
1）单点登录：单点登录是**安全凭证**在多个系统之间传递或共享。
2）Kerberos 构成：
（1）密钥分发中心（KDC）：由 AS 和 TGS 两个部分**构成**。认证服务器（AS:Authentication Server）、票据授权服务器（TGS:Ticket Granting Server）。
（2）应用服务器
（3）客户端
3）Kerberos 过程由三个阶段组成
（1）第一次：访问 AS，获得**票据许可票据**（TGT）
（2）第二次：访问 TGS，获得**服务许可票据**（SGT）
（3）第三次：访问应用，获得**服务**。

4）常见 **AAA** 协议（AAA=认证、授权、计费；AAA=认证、授权、审计；4A）：
（1）RADIUS 协议：UDP 协议、明文发送，安全性低。
（2）TACACS+协议：延时问题，国外开发提供。
（3）**Diameter** 协议：是 RADIUS 的升级版，是一组协议。

第三节 访问控制技术

1.访问控制作用：
（1）保证用户在系统安全策略下正常工作。
（2）拒绝非法用户的非授权访问请求。
（3）拒绝合法用户越权的服务请求。

2.自主访问控制

（1）访问控制表 **ACL**：权限与客体关联，在客体上附加一个主体明细表的方法来表示访问控制矩阵的。
（2）访问能力表 **CL**：权限与主体关联，为每个用户维护一个表，表示主体可以访问的客体及权限。
（3）优点：**灵活**性高，被**大量采用**。缺点：**安全性不高**、信息在传递过程中其访问权限关系会被改变（体现的是 CL）。

3.强制访问控制：

（1）**主体**和**客体**都有一个固定的**安全属性**，系统用该安全属性来决定一个主体是否可以访问某个客体。
（2）**BLP** 模型：解决**不同级别**间保密性。
全策略：高等级权限大于等于低级权限，简单安全规则（**向下读**）、星型规则（**向上写**）。不同的权限类型不可读也不可写。
（3）**BIBA** 模型：解决**不同级别**间完整性（语义）。
简单规则：向上读，主体可以读客体，当且仅当客体的完整级别支配主体的完整级。
星型规则：向下写：主体可以写客体，当且仅当主体的完整级别支配客体的完整级。
（4）**CLARK-WILSON** 模型：**操作前和后，数据必须满足一致性条件**。
（5）CHINESE-WALL：在竞争域中的客体，**主体**只能访问其中的一个。

4. 角色访问控制模型 RBAC 模型：

根据用户所担任的角色决定用户访问权限。用户必须成为某个角色，且还必须激活这一角色，才能对一个对象进行访问或执行某种操作，激活的方式常为会话。

- ✓ RBAC0，基本模型，规定了所有 RBAC 的基本内容，四种要素，用户(U)、角色(R)、会话(S)和权限(P)
- ✓ **RBAC1**：包含 RBAC0，加入安全**等级**及角色**继承**关系
- ✓ **RBAC2**：包含 RBAC0，加入**约束条件**，例如会计和出纳不能为同一人
- ✓ **RBAC3**：结合了 RBAC1、RBAC2。

（END）

温馨提示：为了减少学习的负担和聚焦核心，知识点总结写的是关键的精要的要点，并非是知识点的全文，请一定进一步结合官方的教材进行扩充补充、理解和掌握全面，以免产生以偏概全的问题。