

等级考试三级数据库考点分析之计算机基础知识(6) PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/137/2021_2022__E7_AD_89_E7_BA_A7_E8_80_83_E8_c98_137909.htm

考点13 信息认证 信息认证就是验证信自、发送者的真实性及信息的完整性。认证是防止对系统进行主动攻击的重要手段为。为了保证信息的可认证性，抵抗主动攻击，一个安全的认证体制应满足以下要求。(1) 消息的接收者能够检验和证实消息的合法性、真实性和完整性(2) 消息的发送者对发送的信息不能抵赖，有时也要求消息的接收者不能否认所收到的消息。(3) 除合法消自、发送者外，其他人不能伪造合法的消息。

1、数字签名

数字签名是实施身份认证的方法之一，通过签字算法来实现一个签名算法至少应满足以下3个条件。(1) 签名者事后不能否认自己的签名。(2) 接收者能验证签名，但其他人都不能仿造签名(3) 双方对签名的真伪发生争执时，有能解决争执的第一方存在

2、身份识别

身份识别涉及计算机的安全访问、使用及出入境管理等内容使用密码技术，特别是公钥密码技术，可以设计出安全性能高的识别方法。基于密码识别技术的身份识别有两种方式，即通行字方式和持证方式。通行字方式使用广泛的身份识别方式，通行字一般为数字、字母和特殊字符等组成的长度为5 - 8的字符串其认证过程如下。(1) 识别者将它的通行字传送给计算机。(2) 计算机完成通行字的单项函数值的计算。(3) 计算机把单项函数值和机密存储值相比较。持证方式是另一种身份识别方式，它是用一种持有物来启动电子设备的身份识别方式。常见的是嵌有磁条的磁松，在磁条上记录用于机器识别的个人信息。 100Test 下

载频道开通，各类考试题目直接下载。详细请访问
www.100test.com