

网络技术考前密卷250道选择题23 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/136/2021_2022__E7_BD_91_E7_BB_9C_E6_8A_80_E6_c98_136945.htm (111)我们说公钥加密比常规加密更先进，这是因为_____。

A)公钥是建立在数学函数基础上的，而不是建立在位方式的操作上的
B)公钥加密比常规加密更具有安全性
C)公钥加密是一种通用机制，常规加密已经过时了
D)公钥加密算法的额外开销少

答案：A
知识点：加密与认证技术评析：公开密钥加密又叫做非对称加密，公钥加密最初是由Diffie和Hellman于1976年提出的，这是几千年来文字加密的第一次真正革命性的进步。因为公钥是建立在数学函数基础上的，而不是建立在位方式的操作上的。更重要的是，公钥加密是不对称的，与只使用一种密钥的对称常规加密相比，它涉及到两种独立密钥的使用

。(112)CA安全认证中心的功能是_____。A)发放证书，用于在电子商务交易中确认对方的身份或表明自己的身份
B)完成协议转换，保护银行内部网络
C)进行在线销售和在线谈判，处理用户的订单
D)提供用户接入线路，保证线路的可靠性

答案：A
知识点：加密与认证技术评析：在商务活动中，参与活动的双方需要确认对方的身份，以便保证交易活动安全顺利地进行。在一个电子商务系统中，所有参与交易活动的实体也必须使用某种方式或方法表明自己的身份。通过CA安全认证系统发放的证书确认对方(或表明自身)的身份是电子商务中最常用的方法之一。(113)“数字摘要”(也称为“数字指纹”)是指_____。A)一种基于特定算法的文件，其内容和长度以及文件有关
B)一种和特定文件相关的数据，由指定

文件可以生成这些数据C)一种由特定文件得出的不可能由其他文件得出的数据D)一种由特定文件得出的或者是文件略做调整后得出的数据

答案：C

知识点：加密与认证技术

评析：数字摘要技术属于消息认证的范畴。特定文件是指合法的发送方发出的文件，特定是指文件的身份。这样的文件在做内容调整后，不影响由它得出的数字摘要的合法性，此时数字摘要会发生变化。指定的文件是指伪造方要伪造的文件。它必须满足由其生成的数字摘要和指定的摘要相同。数字摘要有以下要求：接收的输入报文数据没有长度限制；对任何输入报文数据生成固定长度的摘要；根据报文能方便地计算出摘要；难以根据指定的摘要生成一个指定的报文；难以生成两个具有相同摘要的不同的报文。得出数字摘要自然有特定的算法，但是数字摘要的长度是固定的；如果可以由指定的文件(也就是伪造的文件)得到这些数据就违反了第四条要求。报文只要略做变化，数字摘要就要发生变化。所以D也不正确。

(114)网络防火墙的作用是_____。

A)建立内部信息和功能与外部信息和功能之间的屏障
B)防止系统感染病毒与非法访问
C)防止黑客访问
D)防止内部信息外泄

答案：A

知识点：防火墙技术的基本概念

评析：防火墙是构成网络安全因素的重要手段。它的任务是对于进出网络的所有信息进行全面的检测，监视网络的使用，阻断有害信息进入网络的途径，也要防止内部保密的信息通过一个特别的点传输到系统以外，在必要的情况下发布安全警报，重新部署网络地址转换，向外发布信息。

(115)网络管理的功能有_____。

A)性能分析和故障检测
B)安全性管理和计费管理
C)网络规划和配置管理
D)以上都是

答案：D

知识点：网络管理的基本概念

评析：网络管理主要有以下的功能：性能分析、故障检测、安全性管理、计费管理、网络规划、配置管理、目录管理、网络拓扑图。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