

2009年自考电子商务安全导论押密试题及答案(1) 自考 PDF 转换可能丢失图片或格式, 建议阅读原文

https://www.100test.com/kao_ti2020/646/2021_2022_2009_E5_B9_B4_E8_87_AA_c67_646289.htm 全国高等教育自学考试 电子商务安全导论标准预测试卷(一)(考试时间150分钟) 第一部分 选择题 一、单项选择题(本大题共20小题, 每小题1分, 共20分) 在每小题列出的四个备选项中只有一个是符合题目要求的, 请将其代码填写在题后的括号内。 1. 在电子商务系统可能遭受的攻击中, 从信道进行搭线窃听的方式被称为() A. 植入 B. 通信监视 C. 通信窜扰 来源: 考试大 D. 中断 2. 消息传送给接收者后, 要对密文进行解密是所采用的一组规则称作() A. 加密 B. 密文 C. 解密 D. 解密算法 3. 基于有限域上的离散对数问题的双钥密码体制是() A. ELGamal B. AES C. IDEA D. RSA 4. MD-5是_____轮运算, 各轮逻辑函数不同。() A. 2 B. 3 来源: 考试大 C. 4 D. 5 5. 在以下签名机制中, 一对密钥没有与拥有者的真实身份有唯一的联系的是() A. 单独数字签名 B. RSA签名 C. ELGamal签名 D. 无可争辩签名 6. 《计算机房场、地、站技术要求》的国家标准代码是() A. GB50174- 93 B. GB9361- 88 C. GB2887-89 D. GB50169 - 92 7. 综合了PPTP和L2F的优点, 并提交IETF进行标准化操作的协议是() A. IPsec B. L2TP C. VPN D. GRE 来源: www.examda.com 8. VPN按服务类型分类, 不包括的类型是() A. Internet VPN B. Access VPN C. Extranet VPN D. Intranet VPN 9. 接入控制机构的建立主要根据_____种类型的信息。() A. 二 B. 三 C. 四 D. 五 10. 在通行字的控制措施中, 根通行字要求必须采用_____进制字符。() A. 2

B . 8 C . 10 D . 16 11.以下说法不正确的是 () 来源 : 考试大A. 在各种不用用途的数字证书类型中最重要的是私钥证书 B . 公钥证书是由证书机构签署的 , 其中包含有持证者的确切身份 C . 数字证书由发证机构发行 D . 公钥证书是将公钥体制用于大规模电子商务安全的基本要素 12.以下说法不正确的是 () A. RSA的公钥一私钥对既可用于加密 , 又可用于签名 B . 需要采用两个不同的密钥对分别作为加密一解密和数字签名一验证签名用 C . 一般公钥体制的加密用密钥的长度要比签名用的密钥长 D . 并非所有公钥算法都具有RSA的特点 13. _____是整个CA证书机构的核心 , 负责证书的签发。 () A . 安全服务器 B . CA服务器 C . 注册机构RA D . LDAP服务器 来源 : 考试大14 . 能够有效的解决电子商务应用中的机密性、真实性、完整性、不可否认性和存取控制等安全问题的是 () A. PKI B . SET C . SSL D . ECC 15.在PKI的性能中 , _____服务是指从技术上保证实体对其行为的认可。 () A . 认证 B . 数据完整性 C . 数据保密性 D . 不可否认性 16 . 以下不可否认业务中为了保护发信人的是 () A . 源的不可否认性 B . 递送的不可否认性 C . 提交的不可否认性 D . B和C 来源 : www.100test.com17 . SSL支持的HTTP , 是其安全版 , 名为 () A . HTTPS B . SHTTP C . SMTP D . HTMS 18. SET系统的运作是通过_____个软件组件来完成的。 () A . 2 B . 3 C . 4 D . 5 19 . 设在CFCA本部 , 不直接面对用户的是 () A . CA系统 B . RA系统 C . LRA系统 D . LCA系统 20. CTCA的个人数字证书 , 用户的密钥位长为 () 百考试题论坛A . 128 B . 256 C . 512 D . 1024 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