

中国十大品牌教育集团 中国十佳网络教育机构



- 自考名师全程视频授课，图像、声音、文字同步传输，享受身临其境的教学效果；
- 权威专家在线答疑，提交到答疑板的问题在 24 小时内即可得到满意答复；
- 课件自报名之日起可反复观看，不限时间、地点、次数，直到当期考试结束后一周关闭；
- 付费学员赠送 1G 超大容量电子信箱；及时、全面、权威的自考资讯全天 24 小时滚动更新；
- 一次性付费满 300 元，即可享受九折优惠；累计实际交费金额 500 元或支付 80 元会员费，可成为银卡会员，购课享受八折优惠；累计实际交费金额 1000 元或支付 200 元会员费，可成为金卡会员，购课享受七折优惠（以上须在同一学员代码下）；

英语/高等数学预备课：英语从英文字母发音、国际音标、基本语法、常用词汇、阅读、写作等角度开展教学；数学针对有高中入学水平的数学基础的同学开设。通过知识点精讲、经典例题详解、在线模拟测验，有针对性而快速的提高考生数学水平。[立即报名！](#)

基础学习班：依据全新考试教材和大纲，由辅导老师对教材及考试中所涉及的知识进行全面、系统讲解，使考生从整体上把握该学科的体系，准确把握考试的重点、难点、考点所在，为顺利通过考试做好知识上、技巧上的准备。[立即报名！](#)

真题串讲班：教育部考试中心已经启动了自考的国家题库建设，熟练掌握自考历年真题成为顺利通过考试的保障之一。自考 365 网校与权威自考辅导专家合作，推出真题串讲班网上辅导课程。通过对课程的整体情况分析 & 近 3 次考试的真题讲解，全面梳理考试中经常出现的知识点，并对重点难点问题配合典型例题扩展讲解。串讲班课程在考前一个月左右开通。[立即报名！](#)

习题班：自考 365 网校与北大燕园合作推出，每门课程均涵盖该课程全部考点、难点，在线测试系统按照考试难度要求自动组卷、全程在线测试、提交后自动判定成绩。我们相信经过反复练习定能使您迅速提升应试能力，使您考试梦想成真！[立即报名！](#)

自考实验班：针对高难科目开设，签协议，不及格返还学费。全国限量招生，报名咨询 010-82335555 [立即报名！](#)

全国 2009 年 1 月高等教育自学考试

电子商务安全导论试题

课程代码：00997

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。错选、多选或未选均无分。

1. 美国的橘黄皮书中给计算机安全的不同级别制定了标准，由低到高排列正确的是（ ）
A. C1、B1、C2、B2
B. B1、B2、C1、C2
C. A、B2、C2、D
D. C1、C2、B1、B2
2. 保证身份的精确性，分辨参与者所声称身份的真伪，防止伪装攻击，这样的业务称为（ ）
A. 认证业务
B. 保密业务
C. 控制业务
D. 完整业务
3. EES 采用的新加密算法是（ ）
A. RSA
B. Skipjack
C. DES
D. Diffie—Hellman
4. IDEA 加密算法首先将明文分为（ ）

- A.16 位数据块
C.64 位数据块
- 5.在签名人合作下才能验证的签名为 ()
A.无可争辩签名
C.盲签名
- 6.消息用散列函数处理得到 ()
A.公钥
C.私钥
- 7.在计算机机房设计中,设备间应采用 UPS 不间断电源,UPS 功率大小应根据网络设备功率进行计算,并应具有余量是 ()
A.5%~10%
C.15%~20%
- B.32 位数据块
D.128 位数据块
- B.双联签名
D.RSA 签名
- B.消息摘要
D.数字签名
- B.10%~20%
D.20%~30%
- 8.按 VPN 的服务分类,不属于业务类型的是 ()
A.Storage VPN
C.Access VPN
- 9.下列不是防火墙控制技术的是 ()
A.包过滤型
C.VPN
- 10.为数据库加密字段的存储、检索、索引、运算、删除、修改等功能的实现提供接口的技术是 ()
A.数字签名
C.双密钥机制
- 11.下列不属于 Internet 的接入控制技术主要对付的入侵者是 ()
A.伪装者
C.违法者
- 12.下列不属于 Kerberos 存在的局限性的是 ()
A.时间同步
C.密钥的分配
- 13.下列属于证书申请方式的是 ()
A.E-mail 申请
C.邮寄申请
- 14.将公钥体制用于大规模电子商务安全的基本要素是 ()
A.公钥对
C.数字证书
- 15.通常 PKI 的最高管理是通过 ()
A.政策管理机构来体现
C.应用接口来体现
- 16.SSL 协议主要用于交流购买信息,传送 ()
A.电子现金
C.电子商贸信息
- 17.为了确保数据的完整性,SET 协议是通过 ()
A.单密钥加密来实现
C.密钥分配来实现
- B.Intranet VPN
D.Extranet VPN
- B.包检验型
D.应用层网关型
- B.消息摘要
D.加密桥技术
- B.病毒
D.地下用户
- B.重放攻击
D.口令猜测攻击
- B.电话申请
D.短信申请
- B.密钥
D.公钥证书
- B.证书作废系统来体现
D.证书中心 CA 来体现
- B.电子信用卡
D.客户信息
- B.双密钥加密来实现
D.数字化签名来实现

18. 下列不是 SHECA 证书管理器管理的证书是 ()
- A. 个人证书 B. 服务器证书
C. 他人证书 D. 根证书
19. CFCA 是由 ()
- A. 招商银行牵头 B. 中国人民银行牵头
C. 中国移动牵头 D. 中国电信牵头
20. Kerberos 的域内认证过程共分 3 个阶段, 共 6 个步骤。在第 1 个阶段的第 1 个步骤, 客户向 AS 发送的信息不包含 ()
- A. IDClient B. IDTGS
C. IDServer D. 时间戳 a

二、多项选择题 (本大题共 5 小题, 每小题 2 分, 共 10 分)

在每小题列出的五个备选项中至少有两个是符合题目要求的, 请将其代码填写在题后的括号内。错选、多选、少选或未选均无分。

21. 计算机病毒的主要来源有 ()
- A. 非法拷贝引起的病毒 B. 通过互联网络传入的病毒
C. 有人研制和改造的病毒 D. 一些游戏软件染有的病毒
E. 引进的计算机系统和软件中自带的病毒
22. 接入控制的实现方法有 ()
- A. DAC B. DCA
C. MAC D. MCA
E. CMA
23. Kerberos 的认证中心服务任务被分配到几个相对的服务器, 这些服务器包括 ()
- A. ASS B. Client
C. Server D. TGS
E. AS
24. PKI 技术能够有效地解决电子商务应用中信息的 ()
- A. 机密性 B. 真实性
C. 完整性 D. 不可否认性
E. 存取控制
25. SET 的技术范围包括 ()
- A. 认可信息和对象格式 B. 银行信息和对象格式
C. 购买信息和对象格式 D. 证书信息和对象格式
E. 控制信息和对象格式

三、填空题 (本大题共 5 小题, 每小题 2 分, 共 10 分)

请在每小题的空格中填上正确答案, 错填、不填均无分。

26. 在服务器面临的攻击威胁中, 攻击者通过控制一台连接于入侵目标网的计算机, 然后从网上断开, 让网络服务器误以为 _____ 就是实际的客户端, 这种威胁称为 _____。
27. 根据近代密码学的观点, 一个密码系统的安全性取决于对 _____ 的保护, 而不取决于对 _____ 的保密。
28. 在网络连接技术中, 从表面上看它类似于一种专用连接, 但实际上是在共享网络上实现的, 这种连接技术称为 _____, 它往往使用一种被称作 _____ 的技术。
29. 一个典型的 CA 系统包括安全服务器、注册机构 RA、 _____、 _____ 和数据库服务器等。

30.SSL 就是客户和商家在通信之前，在 Internet 上建立一个“秘密传输信息的信道”，保障了传输信息的_____、完整性和_____。

四、名词解释题（本大题共 5 小题，每小题 3 分，共 15 分）

- 31.主动攻击
- 32.恶性病毒
- 33.漏报率
- 34.CA 证书
- 35.公证服务

五、简答题（本大题共 6 小题，每小题 5 分，共 30 分）

- 36.简述电子商务发展的四个阶段。
- 37.简述 DES 加密算法的加密运算法则。
- 38.数字签名可以解决哪些安全鉴别问题？
- 39.设置防火墙的目的及主要作用是什么？
- 40.简述有效证书应满足的条件。
- 41.简述实现递送的不可否认性机制的方法。

六、论述题（本大题共 1 小题，共 15 分）

- 42.试述混合加密系统的实施过程。

