 网络应用与电子商务 363. 电子商务：一般意义上的电子商务是指以开放的InterNet网络环境为基础，在计算机支持下进行的商务活动.广义上的电子商务是指以计算机与通信网络为基础平台，利用电子工具实现的在线商业交易和行政作业活动的全过程。 364. 电子商务的分类：按支付方法分：支付型电子商务和非支付型电子商务.按服务类型分：企业对企业(BTOB)、企业对消费者(BTOC)、消费者对消费者(CTOC)。 365. 电子商务的优越性：行销成本低、经营规模不受场地限制、支付手段高度电子化、便于收集和管理客户信息、特别适合信息商品的销售。 366. 电子商务系统结构：包括CA认证系统、支付网关系统、业务应用系统和用户终端系统。 367. 电子商务系统的功能层次模型：电子商务系统可以分为网络基础平台、安全基础结构、支付体系和业务处理4个层次。 368. 电子商务中应解决的重要问题：数据传输的安全性、数据的完整性、身份认证、交易的不可抵赖性、网上支付。 369. 电子商务应用中的关键技术：加密技术、安全技术、电子支付、安全电子交易。 370. 加密技术：包括私密密钥加密技术(对称密钥加密)和公开密钥加密技术两大类。 371. 私密密钥加密技术：典型的如DES算法，它是电子商务系统中应用最为广泛的对称密钥加密算法，它使用64位密钥长度，其中8位用于奇偶校验，56位被用户使用. 372. 公开密钥加密技术：典型的如RSA算法，它是一种支持变长密钥的公开密钥加密算法，它的缺点是要求加密的报文块

长度必须小于密钥长度。数字签名和身份验证是RSA算法在电子商务中的典型应用。 373. 安全向散列函数：是使用单向散列函数对要传输的信息块生成一个信息摘要(指纹)，它并不是一种加密机制。 374. 单向散列函数的特性：单向散列函数能处理任意大小的信息，其生成的信息摘要数据块长度是固定的，而且对一个源数据反复执行该函数得到的结果是相同的.单向散列函数生成的信息摘要是不可预见的，产生的信息摘要的大小与原始数据信息块的大小没有任何联系，信息摘要看起来与原始数据也没有明显的关系，而且原始数据信息的一个微小变化都会对新产生的信息摘要产生很大的影响.它具有不可逆性，没有办法通过生成的信息摘要重新生成原始数据信息。 375. 安全技术：是指在电子商务系统中，为保证传输信息的完整性、安全性，完成交易各方的身份认证，防止交易过程中抵赖行为的发生而形成的数字信封技术、数字签名技术和身份认证技术的总称。 376. 数字信封技术：数字信封技术综合了私密密钥加密技术和公开密钥加密技术的优点，它使用私密密钥对信息进行加密，使用接收方提供的公开密钥对私密密钥进行加密，接收方收到信息后，首先利用自己的私钥对对方的私密密钥进行解密，再用解密后的发送方私密密钥对密文进行解密。简单地说：数字信封技术是使用私密密钥加密技术对要发送的信息进行加密、使用公开密钥加密技术对私钥进行加密的一种加密技术。它可以形象的描述为：内私钥、外公钥。(即内层用私钥加密技术加密信息、外层用公开密钥加密技术加密私钥)。它保证了数据传输的安全性。 377. 数字签名技术：在日常生活中，签名是保证文件或资料真实性的一种方法，在电子商务系统中，通常使

用数字签名技术来模拟文件或资料中的亲笔签名。数字签名技术使用公开加密密钥算法和单向散列函数来实现。它的具体实现方法为：首先使用安全单向散列函数对要进行数字签名的信息进行处理，生成信息摘要.其次对生成的信息摘要使用公开密钥算法进行数字签名(加密).第三，将信息本身与加密后的信息摘要传送到接收方，接收方用同样的安全单向散列函数生成信息摘要并对接收到的信息摘要进行解密处理，如果两个信息接要是相同的，则可以确认该信息来自确定的发送方。数字签名技术保证了数据传输过程中的完整性，同时，完成了对传送方的身份认证，有效的防止了交易过程中抵赖行为的发生。 378. 安全数据传输和身份认证流程：是一种采用了数字信封技术以保证数据传输的安全性，采用数字签名技术以保证数据的完整性，提供身份验证，防止抵赖行为发生的数据传输和身份认证过程。它结合了数字信封和数字签名两种技术。具体流程为： a.发送方对要发送的信息进行数字签名，并将数字签名附在要发送的信息之后。 b.发送方对要发送的信息和数字签名用私密密钥加密法进行加密，c.发送方法利用接收方公钥对生成的私密密钥进行加密，形成数字信封。 d.将生成的数字信封和经加密的信息传送到接收方，接收方进行反向操作即可以完成认证。 379. 电子支付：包括电子现金、电子支票、电子信用卡三个部分。 380. 电子安全交易(SET)：是由VISA、 MasterCard所开发的开放式支付规范，是为了信用卡在公共InterNet网络上支付的安全而设立的，它采用了数字信封技术、数字签名技术、信息摘要技术以及又重签名技术，保证了信息传输和处理的安全。 381. SET协议所涉及的当事者：持卡人、发卡机构、商家、银行、

支付网关。 382. 浏览器、电子邮件和WEB服务器的安全性(略) 383. 网络技术的发展：网络技术的发展经历了从封闭到开放、从专用到公用、从数据到多媒体的过程。 384. 网络的新应用：包括广度计算和新的集中式服务趋势。 385. 宽带网技术：宽带网包括了IP/ATM、CIPOA、IP/SDH、POS、IP光网络等技术。 386. Ipv6：IP协议是InterNet 协议集的中心，1981年制订的Ipv4，有力地支持了Internet技术的发展，但是，由于网络用户的不断增加，32位IP地址已越来越不能满足用户对网络的要求，在这种情况下推出的Ipv6，以128位地址的高容量，更好地适应了网络的要求。 编辑推荐： 2011年计算机等级考试三级网络复习资料汇总 2011年计算机三级网络技术考试要点汇总 百考试题网校2010年全国计算机三级网络技术考后名师专访 2011年计算机三级网络技术基础笔记汇总 2011年计算机三级网络技术课后填空题汇总 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