全国 2009 年 10 月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．电子商务安全的中心内容中，用来保证为用户提供稳定的服务的是（　D　）1-12

A．商务数据的完整性　B．商务对象的认证性

C．商务服务的不可否认性　D．商务服务的不可拒绝性

2．使用 DES 加密算法，需要对明文进行的循环加密运算次数是（　C　）2-26

A．4 次　B．8 次

C．16 次 D．32 次

3．在密钥管理系统中最核心、最重要的部分是（ D　）2-50

A．工作密钥　B．数据加密密钥

C．密钥加密密钥　D．主密钥

4．MD-4 的输入消息可以为任意长，压缩后的输出长度为（　D　）3-55

A．64 比特　B．128 比特

C．256 比特　D．512 比特

5．充分发挥了 DES 和 RSA 两种加密体制的优点，妥善解决了密钥传送过程中的安全问题的技术是（　C　）3-69

A．数字签名　B．数字指纹

C．数字信封　D．数字时间戳

6．在电子商务中，保证认证性和不可否认性的电子商务安全技术是（　A　）3-65

A．数字签名　B．数字摘要

C．数字指纹　D．数字信封

7．《电气装置安装工程、接地装置施工及验收规范》的国家标准代码是（　D　）4-71

A．GB50174—93　B．GB9361—88

C．GB2887—89　D．GB50169—92

8．下列提高数据完整性的安全措施中，不属于预防性措施的是（　D　）4-72

A．归档　B．镜像

C．RAIDD．网络备份

9．系统将通行字表划分成两部分，每部分包含几个通行字来减少暴露的危险性?（　A　）7-101

A．半个 B．一个

C．两个 D．四个

10．Kerberos 是一种网络认证协议，它采用的加密算法是（ C　）9-133

A．RSA B．PGP

C．DES D．MD5

11．数字证书采用公钥体制，即利用一对互相匹配的密钥进行（　B　）2-47

A．加密 B．加密、解密

C．解密 D．安全认证

12．通常 PKI 的最高管理是通过（　A　）9-129

A．政策管理机构来体现的 B．证书作废系统来体现的

C．应用接口来体现的 D．证书中心 CA 来体现的

13．实现递送的不可否认性的方式是（　A　）9-136

A．收信人利用持证认可　B．可信赖第三方的持证

C．源的数字签名 D．证据生成

14．SET 协议用来确保数据的完整性所采用的技术是（ D　）10-145

A．单密钥加密　B．双密钥加密

C．密钥分配 D．数字化签名

15．安装在客户端的电子钱包一般是一个（　B　）10-146

A．独立运行的程序　B．浏览器的插件

C．客户端程序　D．单独的浏览器

16．CFCA 认证系统采用国际领先的 PKI 技术，总体为几层的 CA 结构?（　C　）11-154

A．一层 B．二层

C．三层 D．四层

17．下列防火墙类型中处理效率最高的是（　A　）5-81

A．包过滤型 B．包检验型

C．应用层网关型 D．代理服务器型

18．点对点隧道协议 PPTP 是第几层的隧道协议?（　B　）5-84

A．第一层　B．第二层

C．第三层　D．第四层

19．在 Internet 接入控制对付的入侵者中，属于合法用户的是（　C　）6-93

A．黑客 B．伪装者

C．违法者　D．地下用户

20．下列选项中不属于数据加密可以解决的问题的是（　C　）6-96

A．看不懂　B．改不了

C．盗不走　D．用不了

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．将自然语言格式转换成密文的基本加密方法有（　AB　）2-23

A．替换加密 B．转换加密

C．DES 加密 D．RSA 加密

E．IDEA 加密

22．在下列计算机病毒中，属于良性病毒的有（　ABD　）4-76

A．小球病毒 B．扬基病毒

C．黑色星期五病毒　D．救护车病毒

E．火炬病毒

23．从攻击角度来看，Kerberos 的局限性体现出的问题有（　ABCDE　）7-108

A．时间同步 B．认证域之间的信任

C．口令猜测攻击 D．密钥的存储

E．重放攻击

24．SET 协议的安全保障措施的技术基础包括（　ABDE　）10-145

A．通过加密方式确保信息机密性

B．通过数字化签名确保数据的完整性

C．通过数字化签名确保数据传输的可靠性

D．通过数字化签名和商家认证确保交易各方身份的真实性

E．通过特殊的协议和消息形式确保动态交互系统的可操作性

25．数据加密的作用在于解决（　ABDE　）6-95

A．外部黑客侵入网络后盗窃计算机数据的问题

B．外部黑客侵入网络后修改计算机数据的问题

C．外部黑客非法入侵计算机内部网络的问题

D．内部黑客在内部网上盗窃计算机数据的问题

E．内部黑客在内部网上修改计算机数据的问题

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。填错、不填均无分。

26. 根据电子商务的发展过程，可以将电子商务分为以建立在_专用网_____基础上的 EDI 为代表的传统电子商务和以_因特网_____为基础的现代电子商务。1-6

27. 我国计算机应急体系在进行计算机病毒的防范时，遵循的工作原则是:“_积极预防_____、及时发现、快速反应、_确保恢复_____”。4-77

28. VPN 是一种架构在公用通信基础设施上的专用数据通信网络，利用__网络层安全协议____和建立在 PKI 上的_加密与签名技术_____来获得机密性保护。9-131

29. CFCA 手机证书支持无线_PKI_____，提供基于__WAP____和短信息两种方式的手机证书，实现在移动商务中的身份验证、信息加密、数字签名，确保使用者能在任何地点、任何时间，方便、及时、交互地进行安全接入信息与服务。11-159

30. VPN 的设计应该遵循以下原则：__安全性____、__网络优化____、VPN 管理等。5-90

四、名词解释题（本大题共 5 小题，每小题 3 分，共 15 分）

31. 无条件安全 2-5

答：

一个密码体制的安全性取决于破译者具备的计算能力，如若它对于拥有无限计算资源的破译者来说是安全的，则称这样的密码体制是无条件安全的，它意味着不论破译者拥有多大的计算资源，都不可能破译。

32. 非军事化区 5-79

答：

为了配置管理方便，内网中需要向外提供服务的服务器往往放在一个单独的网段，这个网段便是非军事化区（DMZ 区）。

33. 公证服务 9-131

答：

PKI 中支持的公证服务是指“数据认证”，也就是说，公证人要证明的是数据的有效性和正确性，这种公证取决于数据验证的方式。

34. TLS 协议 10-140

答：

TLS 是对 IETF 的标准化，制走的目的是为了在因特网上有一种统一的 SSL 标准版本。

35. 加密桥技术 6-97

答：

一种在加／解密卡的基础上开发加密桥的技术可实现在不存在降低加密安全强度旁路条件下，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，并且它的实现是与密码算法、密码设备无关的（可使用任何加密手段）。

五、简答题（本大题共 6 小题，每小题 5 分，共 30 分）

36．简述目前密钥的自动分配途径。2-50

答：

目前，典型的有两类自动密钥分配途径：集中式分配方案和分布式分配方案。

（1）所谓集中式分配是指利用网络中的“密钥管理中心(KMC)”来集中管理系统中的密钥，“密钥管理中心”接受系统中用户的请求，为用户提供安全分配密钥的服务。

（2）分布式分配方案是指网络中各主机具有相同的地位，它们之间的密钥分配取决了它们自己的协商，不受任何其他方面的限制。

37．简述散列函数的概念及其特性。3-54

答：

一、散列函数是将一个长度不确定的输入串转换成一个长度确定的输出串——称为散列值。

二、散列函数 H 应该具有如下特性：

1、给定 M，很容易计算 h；

2、给定 h，不能计算 M；

3、给定 M，要找到另一个输入串 M’并满足 H(M’)=H(M)很难。

38．目前比较常见的备份方式有哪些？4-73

答：

（1）定期磁带备份数据。

（2）远程磁带库、光盘库备份。即将数据传送到远程备份中心制作完整的备份磁带或光盘。

（3）远程关键数据并兼有磁带备份。采用磁带备份数据，生产机实时向备份机发送关键数据。

（4）远程数据库备份。就是在与主数据库所在生产机相分离的备份机上建立主数据库的一个拷贝。

（5）网络数据镜像。这种方式是对生产系统的数据库数据和所需跟踪的重要目标文件的更新进行监控与跟踪，并将更新日志实时通过网络传送到备份系统，备份系统则根据日志对磁盘进行更新。

（6）远程镜像磁盘。通过高速光纤通道线路和磁盘控制技术将镜像磁盘延伸到远离生产机的地方，镜像磁盘数据与主磁盘数据完全一致．更新方式为同步或异步。

39．按照接入方式的不同，VPN 的具体实现方式有哪几种？5-89

答：

按接入方式的不同，VPN 的具体实现即解决方案有四种：

（1）虚拟专用拨号网络(VPDN)，用户利用拨号网络访问企业数据中心，用户从企业数据中心获得一个私有地址，但用户数据可跨公共数据网络传输。

（2）虚拟专用路由网络(VPRN)，它是基于路由的 VPN 接人方式。

（3）虚拟租用线路(VLL)，是基于虚拟专线的一种 VPN，它在公网上开出各种隧道，模拟专线来建立 VPN。

（4）虚拟专用 LAN 子网段(VPLS)，是在公网上用隧道协议仿真出来一个局域网，透明地提供跨越公网的 IAN 服务。

40．通行字的安全存储有哪些方法？7-102

答：

通行字的安全存储有以下 2 种方法：

（1）对于用户的通行字多以加密形式存储，入侵者要得到通行字，必须知道加密算法和密钥，算法可能是公开的，但密钥应当只有管理者才知道。

（2）许多系统可以存储通行字的单向杂凑值，入侵者即使得到此杂凑值也难于推出通行字。

41．SSL 如何来保证 Internet 上浏览器/服务器会话中的认证性？10-139

答：

SSL 提供认证性——使用数字证书——用以正确识别对方。首先是利用服务器的数字证书来验证商家的资格。如果商家网站——服务器要进行 SSL 的安全网上交易，他必须须事先向认证中心提出商家自己的合洼证明（营业执照、法人材料等），并取得数字证书。在 SSL 交易中，客户——浏览器对服务器进行认证，以使其确信与之通信的网站——服务器具有的特定密钥；必要时服务器对浏览器用类似方法进行认证，以确信其具有合法的信用卡号等。现在网络商店使用这类认证还在普及之中，而在 Internet 银行合同签署中
已普遍采用。

六、论述题（本大题共 1 小题，共 15 分）

42．由于 RSA 的公钥/私钥对具有不同的功能，在对公钥/私钥对的要求上要考虑哪些不一致的情况？8-113

答：

RSA 的公钥一私钥对既可用于加密，又可用于签名，但实际上公钥一私钥对的功能是不一样的。因此在要求上要考虑不一致的情况：

（1）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。

（2）一般公钥体制的加密用密钥的长度要比签名用的密钥短，有的国家对出口加密用算法的密钥的长度有限制，而对签名用密钥无限制。

（3）由于实际商务的需要或其他原因，需要用不同的密钥和证书（如有多个信用卡一样），例如一般？肖息加密用的密钥比较短，加密时间可快一些；而对短消息（如单钥密码体制的加密密码）加密用的密钥可以长一些，有利于防止攻击。

（4）密钥对的使用期限不同：加密密钥使用频度比签名用密钥的使用频度大得多，因此更换周期要短。

（5）并非所有公钥算法都具有 RSA 的特点，例如 DSA 算法可以用做签名，但无须建立密钥。未来系统要能支持多种算法，因而应支持采用不同签名密钥对和不同密钥的建立。

（6）加密算法可能支持密钥托管和密钥恢复，以及可能的法律监听。但数字签名的密钥则不允许泄露给他人，其中也包括法律机构。