例题1

9.2 试题精解

例题1（2005年5月试题7）

三个可靠度R均为0.8的部件串联构成一个系统，如图9-1所示。

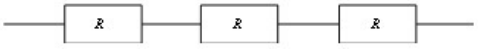

图9-1 串联系统

则该系统的可靠度为_____.

A.0.240 B.0.512 C.0.800 D.0.992

试题分析

此题是一个串联系统可靠性计算的试题，可靠性R=0.8?0.8?0.8=0.512.

试题答案

B

例题2

例题2（2005年5月试题10）

两个公司希望通过Internet进行安全通信，保证从信息源到目的地之间的数据传输以密文形式出现，而且公司不希望由于在中间节点使用特殊的安全单元增加开支，最合适的加密方式是（10），使用的会话密钥算法应该是（11）.

（10）A.链路加密 B.节点加密 C.端-端加密 D.混合加密

（11）A.RSA B.RC-5 C.MD5 D.ECC

试题分析

数据传输加密技术的目的是对传输中的数据流加密，以防止通信线路上的窃听、泄漏、篡改和破坏。如果以加密实现的通信层次来区分，加密可以在通信的三个不同层次来实现，即链路加密（位于OSI网络层以下的加密）、节点加密、端到端加密（传输前对文件加密，位于OSI网络层以上的加密）。

一般常用的是链路加密和端到端加密两种方式。链路加密侧重于在通信链路上而不考虑信源和信宿，是对保密信息通过各链路采用不同的加密密钥提供安全保护。链路加密是面向节点的，对于网络高层主体是透明的，它对高层的协议信息（地址、检错、帧头帧尾）都加密，因此数据在传输中是密文，但在中央节点必须解密得到路由信息。端到端加密则指信息由发送端自动加密，并进入

TCP/IP数据包回封，然后作为不可阅读和不可识别的数据穿过互联网，当这些信息一旦到达目的地，将自动重组、解密，成为可读数据。端到端加密是面向网络高层主体的，它不对下层协议进行信息加密，协议信息以明文形式传输，用户数据在中央节点不需解密。故第10问选择C.

RSA:适用于数字签名和密钥交换。Rivest-Shamir-Adleman（RSA）加密算法是目前应用最广泛的公钥加密算法，特别适用于通过Internet传送的数据。这种算法以它的三位发明者的名字命名：Ron Rivest,Adi Shamir和Leonard Adleman.RSA算法的安全性基于分解大数字时的困难（就计算机处理能力和处理时间而言）。在常用的公钥算法中，RSA与众不同，它能够进行数字签名和密钥交换运算。

MD5:MD5是由Ron Rivest设计的可产生一个128位的散列值的散列算法。MD5设计经过优化后用于Intel处理器。这种算法的基本原理已经泄露。

试题答案

（10）C（11）A

上一节　本书简介　下一节

例题3

例题3（2005年11月试题3）

某计算机系统的可靠性结构是如图9-2所示的双重串并联结构，若所构成系统的每个部件的可靠度为0.9,即R=0.9,则系统的可靠度为　_____.

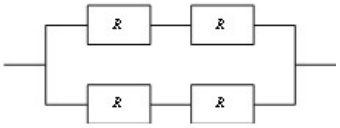

图9-2　先串联后并联系统

A.0.9997B.0.9276C.0.9639D.0.6561

试题分析

由于此题描述的系统是"先串后并",所以我们先求出一条路径上系统的可靠性R1:

R1=RxR=0.81.

然后把两个RX系统并联得：

RR=1-（1-R1）^{2}=1-0.0361=0.9639

所以此题选C.

试题答案

C

上一节　本书简介　下一节

例题4

例题4（2005年11月试题22-23）

某公司服务器上存储了大量的数据，员工使用服务器前首先必须登录。为了保证安全，使用认证技术（22）。为保证传输效率，使用（23）加密算法对传输的数据进行加密。

（22）A.对登录系统的用户身份进行认可B.保护数据在传输中的机密性

C.保证数据在传输中不被非法修改D.防止登录信息被泄漏出去

（23）A.RSA B.ECC C.MD4 D.3DES

试题分析

本题考查有关密码和计算机安全的基础知识。

为保证服务器上数据的安全，可对登录系统的用户身份进行认可，阻挡假冒者或入侵者。

RSA是一种公开密钥算法，它的主要缺点是：要想达到好的安全性，它要求密钥至少有1024位长度（相比之下，对称密钥算法只需要128位），这使得它在加密大量数据时速度非常慢，所以实践中它被广泛用于密钥分发。目前，应用较多的是使用512位密钥的RSA算法。

3DES即三重DES,它共有两个密钥key1和key2,其加密过程：用key1加密，用key2解密再用key1加密；其解密过程：用key1解密，用key2加密再用key1解密。3DES主要是为了增加DES的有效密钥长度，使之更安全。

MD4是Ronald Rives设计的一系列消息摘要算法中第4个算法，属于散列算法，用于数字签名。

椭圆曲线加密算法ECC（Elliptic Curve Cryptography）也是一种公开密钥算法，该算法中160位的密钥长度被认为与RSA算法中1024位的密钥长度的安全性是等价的，它比RSA算法快得多。

考虑到对称加密算法比非对称加密算法要快得多，题干又要求保证传输效率，因此可采用3DES算法。

试题答案

（22）A （23）D

上一节 本书简介 下一节

例题5

例题5（2005年11月试题24）

不能保障公司内部网络边界的安全。

A.在公司网络与Internet或外界其他接口处设置防火墙

B.公司以外网络上用户要访问公司网时，使用认证授权系统

C.禁止公司员工使用公司外部的电子邮件服务器

D.禁止公司内部网络的用户私自设置拨号上网

试题分析

网络边界主要指本单位的网络与外界网络的出口边界，边界安全主要指针对经过边界进出访问和传输数据包时要采取的控制和防范措施。

使用防火墙或认证授权系统可以控制只有经过认证的用户才能够访问公司网络，从而能保证内部网络的安全，禁止公司内部网络用户私自设置拨号上网可以使内部网不易暴露，从而能保障内部网络安全，使不使用内部网之外的电子邮件服务器对内部网没有必然影响。

试题答案

C

例题6

例题6（2006年5月试题5）

若某计算机系统是由500个元器件构成的串联系统，且每个元器件的失效率均为10^{-7}/h，在不考虑其他因素对可靠性的影响时，该计算机系统的平均故障间隔时间为

小时。

A．$2'10^4$　B．$5'10^4$　C．$2'10^5$　D．$5'10^5$

试题分析

此题提及的平均故障间隔时间，也被称为平均无故障时间（MTBF）。提到平均无故障时间（MTBF），我们首先需要了解失效率这个概念。

- 失效率：是指单位时间内失效的元件数与元件总数的比例，通常用λ表示。当λ为常数时，可靠性与失效率的关系为：R（t）=$e^{-\lambda t}$。
- 平均无故障时间（**MTBF**）：是指两次故障间系统能够正常工作的时间平均值。MTBF=1/λ。

此外，与这个考点相关的概念还有（大家在做题时，应有这种举一返三的思想，不要停留于题目的本身）：

- 系统的可靠性：是指从系统开始运行（t=0）到某时刻t期间能够正常运行的概率，通常用R(t)表示。
- 平均修复时间（**MTRF**）：是指从故障发生到机器修复平均所需的时间，用于表示计算机的可维修性。
- 可用性（**A**）：是指计算机的使用效率，它以系统在执行任务的任意时刻能够正常工作的概率来表示。A=MTBF/（MTBF+MTRF）。

对于这个知识点，要求大家把并联系统、串联系统和冗余系统的相关计算搞清楚。下面有一个计算公式表（见表9-2）。

表9-2 可靠性和失效率计算公式表

系统类型	可 靠 性	失 效 率
串联系统	$R=R_1(R_2(\cdots(R_n$	$\lambda=\lambda_1+\lambda_2+\cdots+\lambda_n$
并联系统	$R=1((1(R_1)(1(R_2)(\cdots(1(R_n)$	$\mu=\frac{1}{\frac{1}{\lambda}\sum_{j=1}^{n}\frac{1}{j}}$
模冗余系统		$R=\sum_{m=k}^{n}C_n^m\times R_0^m(1-R_0)^{n-m}$

记住表的内容，相关题目的要求也就容易了。例如此题，我们只需要先求出500个元器件构成的串联系统的失效率λ：

$$\lambda=\lambda_1+\lambda_2+\cdots+\lambda_n=10^{-7}+10^{-7}+\ldots+10^{-7}=10^{-7}\prime 500=5\prime 10^{-5}$$

所以平均无故障时间为：

$$MTBF=1/(5\prime 10^{-5})=2\prime 10^{4}$$

所以答案选A。

试题答案

A

例题7（2006年5月试题7-8）

相对于DES算法而言，RSA算法的 （7） ，因此，RSA （8） 。

（7）A．加密密钥和解密密钥是不相同的　　B．加密密钥和解密密钥是相同的

C．加密速度比DES要高　　D．解密速度比DES要高

（8）A．更适用于对文件加密　　B．保密性不如DES

C．可用于对不同长度的消息生成消息摘要　D．可以用于数字签名

试题分析

基于密钥的算法通常分为对称加密算法和非对称加密算法（公钥算法）。此题就是考查考生是否理解对称加密和非对称加密。题目中DES算法就是对称加密的代表作，而RSA就是非对称加密的代表作。

对称加密：

对称加密算法就是加密用的密钥和解密用的密钥是相等的。比如著名的恺撒密码，其加密原理就是所有的字母向后移动3位，那么3就是这个算法的密钥，向右循环移位就是加密的算法。那么解密的密钥也是3，解密算法就是向左循环移动3位。

显而易见的是，这种算法理解起来比较简单，容易实现，加密速度快，但是对称加密的安全性完全依赖于密钥，如果密钥丢失，那么整个加密就完全不起作用了。

比较著名的对称加密算法就是DES，其分组长度为64位，实际的密钥长度为56位，还有8位校验码。DES算法由于其密钥较短，随着计算机速度的不断提高，使用穷举法对其进行破解成为可能。

非对称加密：

非对称加密算法的核心就是加密密钥不等于解密密钥，且无法从任意一个密钥推导出另一个密钥，这样就大大加强了信息保护的力度，而且基于密钥对的原理很容易实现数字签名和电子信封。

比较典型的非对称加密算法是RSA算法，它的数学原理是大素数的分解，密钥是成对出现的，一个为公钥，一个是私钥。公钥是公开的，可以用私钥去解公钥加密过的信息，也可以用公钥去解私钥加密过的信息。

比如A向B发送信息，由于B的公钥是公开的，那么A用B的公钥对信息进行加密，发送出去，因为只有B有对应的私钥，所以信息只能为B所读取。

牢固的RSA算法需要其密钥长度为1024位，加解密的速度比较慢是它的弱点。

另外一种比较典型的非对称加密算法是ECC算法，基于的数学原理是椭圆曲线离散对数系统，这种算法的标准我国尚未确定，但是其只需要192位就可以实现牢固的加密。所以，应该是优于RSA算法的。

看完上面的概念，我们很容易便可以得出答案：A，D。

试题答案

（7）A　（8）D

例题7

例题8（2006年5月试题9）

驻留在多个网络设备上的程序在短时间内同时产生大量的请求消息冲击某Web服务器，导致该服务器不堪重负，无法正常响应其他合法用户的请求，这属于　　。

A．网上冲浪　B．中间人攻击　C．DDoS攻击　D．MAC攻击

试题分析

此题属于概念题，大家只要对网络攻击方法在概念上有一定的认知，解题还是比较容易的。下面将介绍几种常见的网络攻击方式。

中间人攻击（**MITM**攻击）：

中间人攻击（Man-in-the-Middle Attack，简称“MITM攻击”）是一种“间接”的入侵攻击，这种攻击模式是通过各种技术手段将受入侵者控制的一台计算机虚拟放置在网络连接中的两台通信计算机之间，这台计算机就称为“中间人”。然后入侵者把这台计算机模拟一台或两台原始计算机，使“中间人”能够与原始计算机建立活动连接并允许其读取或修改传递的信息，然而两个原始计算机用户却认为他们是在互相通信。通常，这种“拦截数据—修改数据—发送数据”的过程就被称为“会话劫持”（Session Hijack）。

DD**oS**攻击：

DDoS是英文Distributed Denial of Service的缩写，意即“分布式拒绝服务”，那么什么又是拒绝服务（Denial of Service）呢？可以这么理解，凡是能导致合法用户不能够访问正常网络服务的行为都算是拒绝服务攻击。也就是说，拒绝服务攻击的目的非常明确，就是要阻止合法用户对正常网络资源的访问，从而达成攻击者不可告人的目的。虽然同样是拒绝服务攻击，但是DDoS和DoS还是有所不同，DDoS的攻击策略侧重于通过很多“僵尸主机”（被攻击者入侵过或可间接利用的主机）向受害主机发送大量看似合法的网络包，从而造成网络阻塞或服务器资源耗尽而导致拒绝服务，分布式拒绝服务攻击一旦被实施，攻击网络包就会犹如洪水般涌向受害主机，从而把合法用户的网络包淹没，导致合法用户无法正常访问服务器的网络资源。因此，拒绝服务攻击又被称之为“洪水式攻击”。常见的DDoS攻击手段有SYNFlood、ACKFlood、UDPFlood、ICMPFlood、TCPFlood、ConnectionsFlood、ScriptFlood、ProxyFlood等。

MAC/CAM攻击：

交换机主动学习客户端的MAC地址，并建立和维护端口和MAC地址的对应表以此建立交换路径，这个表就是通常我们所说的CAM表。CAM表的大小是固定的，不同的交换机的CAM表大小不同。MAC/CAM攻击是指利用工具产生欺骗MAC，快速填满CAM表，交换机CAM表被填满后，交换机以广播方式处理通过交换机的报文，这时攻击者可以利用各种嗅探攻击获取网络信息。CAM表满了后，流量以洪泛方式发送到所有接口，也就代表TRUNK接口上的流量也会发给所有接口和邻接交换机，会造成交换机负载过大、网络缓慢和丢包，甚至瘫痪。

显而易见，题目中所述的攻击方式属于DDoS攻击。

试题答案

C

例题8

例题9（2006年11月试题2）

某计算机系统由如图9-3所示的部件构成，假定每个部件的千小时可靠度R均为0.9，则该系统的千小时可靠度约为_____。

A．0.882　　B．0.951　　C．0.9　　D．0.99

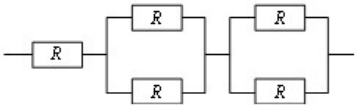

图9-3 先并联后串联系统

试题分析

两个R并联的可靠度为：1-（1-0.9）^{2}=0.99。我们可以将两个并联的R部件看成一个部件R1，R1的可靠度为0.99，所以该系统的可靠度为：0.9′0.99′0.99=0.88209。所以答案为：A。

试题答案

A

上一节　本书简介　下一节

例题9

例题10（2006年11月试题7）

以下不属于网络安全控制技术的是_____。

A．防火墙技术B．访问控制技术

C．入侵检测技术D．差错控制技术

试题分析

此题考点是网络安全，备选答案中的几种技术均为常见网络相关技术，是需要掌握的，所以我们先来了解这些技术的基本情况。

访问控制：是网络安全防范和保护的主要核心策略，它的主要任务是保证网络资源不被非法使用和访问。访问控制规定了主体对客体访问的限制，并在身份识别的基础上，根据身份对提出资源访问的请求加以控制。它是对信息系统资源进行保护的重要措施，也是计算机系统最重要和最基础的安全机制。

防火墙：是一块硬件、软件或者硬件和软件的结合体，在联网环境中发挥作用，以避免安全策略中禁止的一些通信，与建筑中的防火墙功能相似。它有控制信息基本的任务在不同信任的区域。典型信任的区域包括网际网络（一个没有信任的区域）和一个内部网络（一个高信任的区域），最终目标是提供受控连通性在不同水平的信任区域通过安全策略的执行和连通性模型之间根据最少特权原则。

入侵检测：是防火墙的合理补充，帮助系统对付网络攻击，扩展了系统管理员的安全管理能力（包括安全审计、监视、进攻识别和响应），提高了信息安全基础结构的完整性。它从计算机网络系统中的若干关键点收集信息，并分析这些信息，看网络中是否有违反安全策略的行为和遭到袭击的迹象。入侵检测被认为是防火墙之后的第

二道安全闸门，在不影响网络性能的情况下能对网络进行监测，从而提供对内部攻击、外部攻击和误操作的实时保护。

差错控制：由于通信线路上总有噪声存在，所以通常情况下噪声和信息是混在一起传输的，当噪声大到一定程度的时候，会干扰信息，使接收到的信息出现差错。差错控制是通过一些技术手段，对接收到的信息进行正确性检查并纠正，如海明校验编码就是一种具有纠错功能的编码。

从以上分析可以得知差错控制技术不属于网络安全控制技术。所以答案为：D。

试题答案

D

例题10

例题11（2006年11月试题8-9）

“冲击波”病毒属于（8）类型的病毒，它利用Windows操作系统的（9）漏洞进行快速传播。

（8）A．蠕虫B．文件C．引导区D．邮件

（9）A．CGI脚本B．RPCC．DNSD．IMAP

试题分析

冲击波病毒的基本情况如下。

病毒类型：蠕虫病毒。

攻击对象：Windows NT 4.0，Windows 2000，Windows XP，Windows Server 2003等。

传播途径：“冲击波”是一种利用Windows系统的RPC（远程过程调用，是一种通信协议，程序可使用该协议向网络中的另一台计算机上的程序请求服务）漏洞进行传播、随机发作、破坏力强的蠕虫病毒。它不需要通过电子邮件（或附件）来传播，更隐蔽，更不易察觉。它使用IP扫描技术来查找网络上操作系统为Windows 2000/XP/2003的计算机，一旦找到有漏洞的计算机，它就会利用DCOM（分布式对象模型，一种协议，能够使软件组件通过网络直接进行通信）RPC缓冲区漏洞植入病毒体以控制和攻击该系统。

中毒症状：

（1）系统资源紧张，应用程序运行速度异常。

（2）网络速度减慢，“DNS”和“IIS”服务遭到非法拒绝，用户不能正常浏览网页或收发电子邮件。

（3）不能进行复制、粘贴操作。

（4）Word、Excel、PowerPoint等软件无法正常运行。

（5）系统无故重启，或在弹出“系统关机”警告提示后自动重启等。

从中可以得知本题的正确答案为：A，B。

试题答案

A　B

例题11

例题12（2007年5月试题4）

某系统的可靠性结构框图如图9-4所示。该系统由 4 个部件组成，其中 2、3 两部件并联冗余，再与 1、4 部件串联构成。假设部件 1、2、3 的可靠度分别为 0.90、0.70、0.70。 若要求该系统的可靠度不低于 0.75，则进行系统设计时，分配给部件 4 的可靠度至少应为_____。

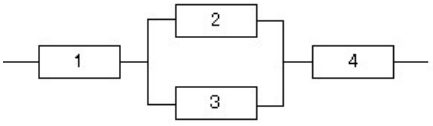

图9-4 并串混联系统

（4）A. $\frac{0.75}{0.9\times(1-0.7)^2}$　　B. $\frac{0.75}{0.9\times(1-0.7\times0.7)^2}$

C. $\frac{0.75}{0.9\times(1-(1-0.7)^2)}$　　D. $\frac{0.75}{0.9\times(0.7+0.7)}$

试题分析

当系统采用串联方式时，其可靠度R可由公式R=R1R2…Rn求得。当系统采用并联方式时，其可靠度R可由公式R=1-（1-R1）*(1-R2)…(1-Rn)求得。本题中2和3是并联，所以这段的可靠性为：1-（1-0.7）*(1-0.7)；而1和4是串联的，所以整个系统的可靠度为：R1*（1-（1-R2）*（1-R3））*R4；题中要求整个系统的可靠度不低于0.75；所以：R4≥0.75/(0.9*(1-(1-0.7)^2)。

试题答案

C

例题12

例题13（2007年5月试题7）

下列行为不属于网络攻击的是_____。

A. 连续不停 Ping 某台主机

B. 发送带病毒和木马的电子邮件

C. 向多个邮箱群发一封电子邮件

D. 暴力破解服务器密码

试题分析

网络攻击是以网络为手段窃取网络上其他计算机的资源或特权，对其安全性或可用性进行破坏的行为。

本题的B和D选项毫无疑问属于网络攻击。关键在于A和C的分析：A选项中的Ping命令是用于网络检测的工

具，Ping某台主机可测试出当前主机到某台主机的网络是否畅通。但如果有多台机器，连续不停的Ping某台主机，则可能使主机无法响应这些数量庞大的请求，从而导致主机无法正常提供服务，这也就是DDOS攻击。而C选项“向多个邮箱群发一封电子邮件”是邮件群发操作，与网络攻击无关。

试题答案

C

例题13

例题14（2007年5月试题8）

多形病毒指的是_____的计算机病毒。

A. 可在反病毒检测时隐藏自己

B. 每次感染都会改变自己

C. 可以通过不同的渠道进行传播

D. 可以根据不同环境造成不同破坏

试题分析

多形病毒是一种较为高级的病毒，这种病毒在每次感染后会改变自己。该病毒以这种方式来避开杀毒软件的查杀。

试题答案

B

例题14

例题15（2007年5月试题9）

感染“熊猫烧香”病毒后的计算机不会出现_____的情况。

A. 执行文件图标变成熊猫烧香

B. 用户信息被泄漏

C. 系统运行变慢

D. 破坏计算机主板

试题分析

“武汉男生”，俗称“熊猫烧香”，这是一个感染型的蠕虫病毒，它能感染系统中exe，com，pif，src，html，asp等文件，它还能中止大量的反病毒软件进程并且会删除扩展名为gho的文件（该文件是一系统备份工具GHOST的备份文件），使用户的系统备份文件丢失。被感染的用户系统中所有.exe可执行文件全部被改成熊猫举着三根香的模样。这种病毒不会破坏计算机主板。至今为止，还只有一种计算机病毒具备破坏主板的功能，即CHI病毒。

试题答案

D

例题15

例题16（2007年11月试题7-8）

某Web网站向CA申请了数字证书。用户登录该网站时，通过验证 （7） ，可确认该数字证书的有效性，从而 （8） 。

（7）A. CA的签名　B. 网站的签名C. 会话密钥D. DES密码

（8）A. 向网站确认自己的身份　B. 获取访问网站的权限

C. 和网站进行双向认证　D. 验证该网站的真伪

试题分析

本题是考数字证书方面的题。数字证书是一段包含用户身份信息、用户公钥信息以及身份验证机构数字签名的数据。身份验证机构的数字签名可以确保证书信息的真实性，用户公钥信息可以保证数字信息传输的完整性，用户的数字签名可以保证数字信息的不可否认性。

数字证书是各类终端实体和最终用户在网上进行信息交流及商务活动的身份证明，在电子交易的各个环节，交易的各方都需验证对方数字证书的有效性，从而解决相互间的信任问题。

数字证书是一个经证书认证中心（CA）数字签名的包含公开密钥拥有者信息以及公开密钥的文件。认证中心（CA）作为权威的、可信赖的、公正的第三方机构，专门负责为各种认证需求提供数字证书服务。认证中心颁发的数字证书均遵循X.509 V3标准。X.509标准在编排公共密钥密码格式方面已被广为接受。X.509证书已应用于许多网络安全，其中包括IPSec（IP安全）、SSL、SET、S/MIME。

数字信息安全主要包括以下几个方面：

- 身份验证（Authentication）
- 信息传输安全
- 信息保密性（存储与交易）（ Confidentiality）
- 信息完整性（Integrity）
- 交易的不可否认性（Non-repudiation）

对于数字信息的安全需求，通过如下手段加以解决：

- 数据保密性----加密
- 数据的完整性----数字签名
- 身份鉴别----数字证书与数字签名
- 不可否认性----数字签名

为了保证网上信息传输双方的身份验证和信息传输安全，目前采用数字证书技术来实现，从而实现对传输信息的机密性、真实性、完整性和不可否认性。

试题答案

A　D

例题16

例题17（2007年11月试题9）

实现VPN的关键技术主要有隧道技术、加解密技术、_____和身份认证技术。

A. 入侵检测技术　B. 病毒防治技术

C. 安全审计技术　D. 密钥管理技术

试题分析

虚拟专用网络（VPN）：是利用不可靠的公用互联网络作为信息传输介质，通过附加的安全通道、用户认证和访问控制等技术实现与专用网络相类似的安全性能，从而实现对敏感信息的安全传输。VPN的关键技术：安全隧道技术、用户认证技术、访问控制技术。VPN可以提供的功能：防火墙功能、认证、加密、隧道化。L2TP、PPTP是两种链路层的VPN协议，TLS是传输层VPN协议，IPsec是网络层VPN协议。

试题答案

D

例题17

例题18（2007年11月试题33）

某大型软件系统按功能可划分为2段P1和P2.为提高系统可靠性，软件应用单位设计了如下图给出的软件冗余容错结构，其中P1和P2均有一个与其完全相同的冗余备份。若P1的可靠度为0.9,P2的可靠度为0.9,则整个系统的可靠度是_____.

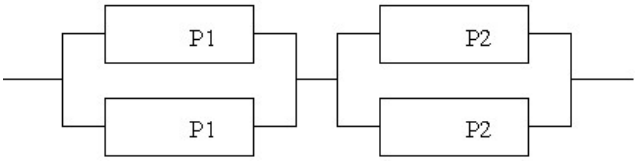

图9-5　先并联后串联系统

A. 0.6561　B. 0.81　C. 0.9801　D. 0.9

试题分析

当系统采用串联方式时，其可靠度R可由公式R=R1R2…Rn求得。当系统采用并联方式时，其可靠度R可由公式R=1-（1-R1）*（1-R2）…（1-Rn）求得。这个系统总的来说是串联，但分成两个并联部分。第一部分的可靠度为：R1=1-（1-0.9）*（1-0.9）=0.99;第二部分的可靠度也为：

R2=0.99;所以整个系统的可靠度为：R=R1*R2=0.9801 ,C答案。

试题答案

C

例题18

例题19（2008年5月试题31）

某数据处理软件包括 2 个完全相同的数据处理部件和 1 个数据存储部件，且采用下图给出的容错方案。当数据处理部件的可靠性为 0.6 时，为使整个软件系统的可靠性不小于0.66,则数据存储部件的可靠性至少应为_____.

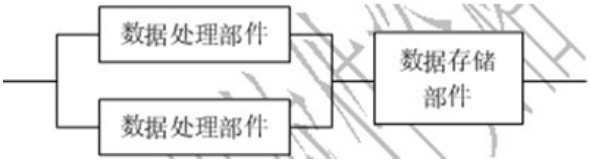

图9-6 先并联后串联系统

A. 0.6　B. 0.66　C. 0.79　D. 1.0

试题分析

本题考查系统可靠性，是常考的知识点。

计算机系统是一个复杂的系统，而且影响其可靠性的因素也非常繁复，很难直接对其进行可靠性分析；若采用串联方式，则系统可靠性为每个部件的乘积R=R1×R2×R3×……×Rn;若采用并联方式，则系统的可靠性为R=1-（1-R1）×（1-R2）×（1-R3）×……×（1-Rn）。本道题当中的数据处理部件是并联的，每个处理部件的可靠性为0.6,把这两个数据处理部件做为整体M看，则它的可靠性为：1-（1-0.6）×（1-0.6） = 0.84.由于M和数据存储部件是串联的，而M的可靠性为0.84,要求整

第 9 章：安全性、可靠性及系统性能评价　作者：希赛教育软考靠性H.利用串联公共，0.84×H≥0.66 ,解这个

例题18

试题答案

C

版权方授权希赛网发布，侵权必究

上一节　本书简介　下一节

第 9 章：安全性、可靠性及系统性能评价　作者：希赛教育软考学院　2014年02月10日

例题19

例题20（2008年12月试题8）

为了防止电子邮件中的恶意代码，应该用_____方式阅读电子邮件。

A.文本　　B.网页　　C.程序　　D.会话

试题分析

电子邮件的查看方式通常有两种即：文本方式和网页方式（有时也称为HTML方式）。用网页格式查看邮件时会运行邮件当中的脚本，这样就会执行邮件中的恶意代码，所以用文本方式阅读电子邮件能防止恶意代码。

试题答案

A

上一节　　本书简介　　下一节

例题20

例题21（2008年12月试题9）

TCP/IP 在多个层引入了安全机制，其中TLS 协议位于_____.

A. 数据链路层　B. 网络层　C. 传输层　D. 应用层

试题分析

TLS（安全传输层协议：Transport Layer Security Protocol）用于在两个通信应用程序之间提供保密性和数据完整性。该协议由两层组成： TLS 记录协议（TLS Record）和 TLS 握手协议（TLS Handshake）。该协议工作于传输层。

试题答案

C

上一节　　本书简介　　下一节

例题1

10.2 试题精解

例题1（2004年5月试题60）

某个计算机中心有28台微机，每台微机有24个应用，每个应用占用1个端口地址，则这个计算机中心所有应用的地址总数为　　.

A.24　B.28　C.52　D.672

试题分析

本题叙述模糊。如果每台微机的24个应用都相同，则为24个地址；如果都不相同，则为