

三总线结构的计算机总线系统由(1)组成。

- (1) A. CPU 总线、内存总线和 IO 总线 B. 数据总线、地址总线和控制总线
C. 系统总线、内部总线和外部总线 D. 串行总线、并行总线和 PCI 总线

【答案】B

【解析】本题考查计算机系统基础知识。

总线上传输的信息类型分为数据、地址和控制，因此总线由数据总线、地址总线和控制总线组成。

数据总线：传送数据信息，CPU 一次传输的数据与数据总线带宽相等

控制总线：传送控制信号和时序信号，如读/写、片选、中断响应信号等

地址总线：传送地址，它决定了系统的寻址空间

计算机采用分级存储体系的主要目的是为了解决(2)的问题。

- (2) A. 主存容量不足 B. 存储器读写可靠性
C. 外设访问效率 D. 存储容量、成本和速度之间的矛盾

【答案】D

【解析】本题考查计算机系统基础知识。

计算机系统中，高速缓存一般用 SRAM，内存一般用 DRAM，外存一般采用磁存储器。SRAM 的集成度低、速度快、成本高；DRAM 的集成度高，但是需要动态刷新。磁存储器速度慢、容量大、价格便宜。因此，组成分级存储体系以解决存储容量、成本和速度之间的矛盾。

存储系统由存放程序和数据的各类存储设备及有关的软件构成，是计算机系统的重要组成部分，用于存放程序和数据。存储系统分为内存储器和外存储器，两者按一定的结构有机地组织在一起，程序和数据按不同的层次存放在各级存储器中，而整个存储系统具有较好的速度、容量和价格等方面的综合性能指标。

属于 CPU 中算术逻辑单元的部件是(3)。

- (3) A. 程序计数器 B. 加法器 C. 指令寄存器 D. 指令译码器

【答案】B

【解析】本题考查计算机系统基础知识。

程序计数器、指令寄存器和指令译码器都是 CPU 中控制单元的部件，加法器是算术逻辑运算单元的部件。

算术逻辑单元是运算器的重要组成部分，负责处理数据，实现对数据的算术运算和逻辑运算。所以本题正确的选项是 B

CPU 中其它部件作用：

程序计数器是用于存放下一条指令所在单元的地址的地方。在程序执行前，必须将程序的起始地址，即程序的一条指令所在的内存单元地址送入程序计数器，当执行指令时，CPU 将自动修改程序计数器的内容，即每执行一条指令程序计数器增加一个量，使其指向下一个待指向的指令。程序的转移等操作也是通过该寄存器来实现的。

地址寄存器一般用来保存当前 CPU 所访问的内存单元的地址，以方便对内存的读写操作。

累加器是专门存放算术或逻辑运算的一个操作数和运算结果的寄存器

ALU 是 CPU 的执行单元，主要负责运算工作。

指令寄存器一般用来保存当前正在执行的一条指令。

数据寄存器主要是用来保存操作数和运算结果等信息的，其目的是为了节省读取操作数所需占用总线和访问存储器的时间。

地址寄存器一般用来保存当前 CPU 所访问的内存单元的地址，以方便对内存的读写操作。作为程序员，应该要能控制其所编写程序的执行过程，这就需要利用程序计数器来实现，因此程序员能访问的是程序计数器

内存按字节编址从 A5000H 到 DCFFFH 的区域其存储容量为(4)。

- (4) A. 123KB B. 180KB C. 223KB D. 224KB

【答案】D

【解析】本题考查计算机系统基础知识。

从地址 A5000H 到 DCFFFH 的存储单元数目为 37FFFH (即 224×1024) 个，由于是字节编址，从而得到存储容量为 224KB。

内存按字节编址从 A5000H 到 DCFFFH，得出地址空间为：DCFFFH-A5000H+1=38000H，将 38000H 换算为二进制为：11 1000 0000 0000 0000=1110 0000x2¹⁰=224KB。

以下关于 RISC 和 CISC 的叙述中，不正确的是(5)。

- (5) A. RISC 通常比 CISC 的指令系统更复杂
B. RISC 通常会比 CISC 配置更多的寄存器
C. RISC 编译器的子程序库通常要比 CISC 编译器的子程序库大得多

D. RISC 比 CISC 更加适合 VLSI 工艺的规整性要求

【答案】A

【解析】本题考查计算机系统基础知识。

计算机工作时就是取指令和执行指令。一条指令往往可以完成一串运算的动作，但却需要多个时钟周期来执行。随着需求的不断增加，设计的指令集越来越多，为支持这些新增的指令，计算机的体系结构会越来越复杂，发展成 CISC 指令结构的计算机。而在 CISC 指令集的各种指令中，其使用频率却相差悬殊，大约有 20% 的指令会被反复使用，占整个程序代码的 80%。而余下的 80% 的指令却不经常使用，在程序设计中只占 20%，显然，这种结构是不太合理的。

RISC 和 CISC 在架构上的不同主要有：

①在指令集的设计上，RISC 指令格式和长度通常是固定的（如 ARM 是 32 位的指令）、且寻址方式少而简单、大多数指令在一个周期内就可以执行完毕；CISC 构架下的指令长度通常是可变的、指令类型也很多、一条指令通常要若干周期才可以执行完。由于指令集多少与复杂度上的差异，使 RISC 的处理器可以利用简单的硬件电路设计出指令解码功能，这样易于流水线的实现。相对的 CISC 则需要通过只读存储器里的微码来进行解码，CISC 因为指令功能与指令参数变化较大，执行流水线作业时有一定的限制。

②RISC 架构中只有载入和存储指令可以访问存储器，数据处理指令只对寄存器的内容进行操作。为了加速程序的运算，RISC 会设定多组的寄存器，并且指定特殊用途的寄存器。CISC 构架则允许数据处理指令对存储器进行操作，对寄存器的要求相对不高。

CISC 计算机指复杂指令集计算机，是 20 世纪六、七十年代发展起来的系列计算机。这种计算机所支持的指令系统趋于多用途、强功能化。指令系统围绕着缩小与高级语言的语义差距以及有利于操作系统的优化而设计。指令系统的复杂化使得设计周期变长，正确性难于保证，不易维护。而且在复杂的指令系统中，只有少数基本指令是经常使用的，需要大量硬件支持的复杂指令利用率却很低。所以在 70 年代末，随着 VLSI 技术的发展产生了 RISC 计算机。

RISC 计算机指精简指令集计算机，这种计算机有下列特点。

- （1）指令系统中只包含使用频率较高但不复杂的指令。
- （2）指令长度固定，指令格式少，寻址方式少。
- （3）只有存取数指令访问主存，其他指令都在寄存器之间运算。
- （4）大部分指令在一个机器周期内完成，采用流水技术。

- (5) CPU 中增加了通用寄存器的数量。
- (6) 硬联逻辑控制，不用微程序控制技术。
- (7) 采用优化的编译，以有效地支持高级语言。

以下叙述中，正确的是(6)。

- (6) A. 编译正确的程序不包含语义错误
- B. 编译正确的程序不包含语法错误
- C. 除数为 0 的情况可以在语义分析阶段检查出来
- D. 除数为 0 的情况可以在语法分析阶段检查出来

【答案】B

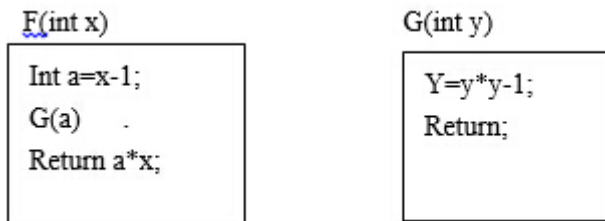
【解析】本题考查程序语言基础知识。

用户编写的源程序不可避免地会有一些错误，这些错误大致可分为静态错误和动态错误。动态错误也称动态语义错误，它们发生在程序运行时，例如变量取零时作除数、引用数组元素下标越界等错误。静态错误是指编译时所发现的程序错误，可分为语法错误和静态语义错误，如单词拼写错误、标点符号错、表达式中缺少操作数、括号不匹配等有关语言结构上的错误称为语法错误。而语义分析时发现的运算符与运算对象类型不合法等错误属于静态语义错误。

程序在编译的过程中，包含了词法分析、语法分析和语义分析等阶段，其中词法分析从左到右逐字符读入源程序，识别出一个个单词符号，常见的词法错误有输入的关键字错误等；语法分析是在词法分析的基础上将单词符号序列分解成各类，诸如“程序”、“语句”、“表达式”等语法单位；语义分析是审查源程序有无语义错误，为代码生成阶段收集类型信息，这个阶段常见的错误有死循环和除数为 0。

其中词法错误和语法错误都可以在编译程序时，检查出，而动态语义错误需要运行程序，所以无法在编译程序时检查出，而要等到程序执行时，才能发现

已知函数 $f()$ 、 $g()$ 的定义如下所示，执行表达式“ $x=f(5)$ ”的运算时，若函数调用 $g(a)$ 是引用调用(call by reference)方式，则执行“ $x=f(5)$ ”后 x 的值为 (7)；若函数调用 $g(a)$ 是值调用(call by value)方式，则执行“ $x=f(5)$ ”后 x 的值为 (8)。



- (7) A. 20 B. 25 C. 60 D. 75
- (8) A. 20 B. 25 C. 60 D. 75

【答案】D A

【解析】本题考查程序语言基础知识。

若实现函数调用时，将实参的值传递给对应的形参，则称为是传值调用。这种方式下形式参数不能向实参传递信息。引用调用的本质是将实参的地址传给形参，函数中对形参的访问和修改实际上就是针对相应实际参数变量所作的访问和改变。

根据题目说明，调用函数 f 时，实参的值为 5，也就是在函数 f 中，x 的初始值为 5，接下来先通过“a = x-1”将 a 的值设置为 4，再调用函数 g(a)。函数 g() 执行时，形参 y 的初始值为 4，经过“y = y*y-1”运算后，y 的值就修改为 15。

在引用调用方式下，g 函数中 y 是 f 函数中 a 的引用（可视为形参 y 与实参 a 是同一对象），也就是说函数 f 中 a 的值被改为 15，因此，返回函数 f 中再执行“a*x”运算后得到 75 (x=5, a=15)，因此空 (7) 应填入的值为 75。

在值调用方式下，g 函数中 y 只获得 f 函数中 a 的值（形参 y 与实参 a 是两个不同的对象），也就是说在函数 g 中修改 y 的值与函数 f 中 a 的值已经没有关系了，因此，返回函数 f 再执行“a*x”运算后得到 20 (x=5, a=4)，因此空 (8) 应填入的值为 20。

传值调用：在按值调用时，过程的形式参数取得的是实际参数的值。在这种情况下，形式参数实际上是过程中的局部量，其值的改变不会导致调用点所传送的实际参数的值发生改变，也就是数据的传送是单向的

引用调用：在按引用调用时，过程的形式参数取得的是实际参数所在的单元地址。在过程中，对该形式参数的引用相当于对实际参数所在的存储单元的地址引用。任何改变形式参数值的操作会反映在该存储单元中，也就是反映在实际参数中，因此数据的传送是双向的

本题的第一问：采用的是引用调用方式执行，x=5，g(a) 中 y=y*y-1=15，即 a 这时的值被修改为 15，最好 a*x=5*15=75

本题的第二问：采用的是传值调用方式执行，x=5，g(a) 中 y=y*y-1=15，即 a 这时的值仍然为 4，最好 a*x=5*4=20

算术表达式“(a-b)*(c+d)”的后缀是(9)。

- (9) A. ab-cd+* B. abcd-*+ C. ab-*cd+ D. ab-c+d*

【答案】A

【解析】本题考查程序语言基础知识。

后缀式（逆波兰式）是波兰逻辑学家卢卡西维奇发明的一种表示表达式的方法。这种表示方式把运算符写在运算对象的后面，例如把 a+b 写成 ab+，所以也称为后缀式。算术表达式“a*(b-c)+d”的后缀式是“ab-cd+*”。

第一步：按照运算符的优先级对所有的运算单位加括号：式子变成：((a-b)*(c+d))

第二步：把运算符移动到对应的括号后面：((ab)-(cd)+)*

第三步：去掉括号：ab-cd+*

网络系统中，通常把 (10) 置于 DMZ 区。

- (10) A. 网络管理服务器 B. Web 服务器
C. 入侵检测服务器 D. 财务管理服务器

【答案】B

【解析】本题考查防火墙的基础知识。

DMZ 是指非军事化区，也称周边网络，可以位于防火墙之外也可以位于防火墙之内。非军事化区一般用来放置提供公共网络服务的设备。这些设备由于必须被公共网络访问，所以无法提供与内部网络主机相等的安全性。

分析四个备选答案，Web 服务器是为一种为公共网络提供 Web 访问的服务器；网络管理服务器和入侵检测服务器是管理企业内部网和对企业内部网络中的数据流进行分析的专用设备，一般不对外提供访问；而财务服务器是一种仅针对财务部门内部访问和提供服务的设备，不提供对外的公共服务。

DMZ 是英文“demilitarized zone”的缩写，中文名称为“隔离区”，也称“非军事化区”。它是为了解决安装防火墙后外部网络不能访问内部网络服务器的问题，而设立的一个非安全系统与安全系统之间的缓冲区，这个缓冲区位于企业内部网络和外部网络之间的小网络区域内，在这个小网络区域内可以放置一些必须公开的服务器设施，如企业 Web 服务器、FTP 服务器和论坛等。另一方面，通过这样一个 DMZ 区域，更加有效地保护了内部网络，因为这种网络部署，比起一般的防火墙方案，对攻击者来说又多了一道关卡。

以下关于拒绝服务攻击的叙述中，不正确的是(11)。

(11) A. 拒绝服务攻击的目的是使计算机或者网络无法提供正常的服务

B. 拒绝服务攻击是不断向计算机发起请求来实现的

C. 拒绝服务攻击会造成用户密码的泄漏

D. DDoS 是一种拒绝服务攻击形式

【答案】C

【解析】本题考查拒绝服务攻击的基础知识。

拒绝服务攻击是指不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序使系统响应减慢直至瘫痪，从而影响正常用户的使用。当网络服务系统响应速度减慢或者瘫痪时，合法用户的正常请求将不被响应，从而实现用户不能进入计算机网络系统或不能得到相应的服务的目的。

DDoS 是分布式拒绝服务的英文缩写。分布式拒绝服务的攻击方式是通过远程控制大量的主机向目标主机发送大量的干扰消息的一种攻击方式。

拒绝服务攻击即攻击者想办法让目标机器停止提供服务或资源访问，是黑客常用的攻击手段之一。这些资源包括磁盘空间、内存、进程甚至网络带宽，从而阻止正常用户的访问。其实对网络带宽进行的消耗性攻击只是拒绝服务攻击的一小部分，只要能够对目标造成麻烦，使某些服务被暂停甚至主机死机，都属于拒绝服务攻击。拒绝服务攻击问题也一直得不到合理的解决，究其原因是因为这是由于网络协议本身的安全缺陷造成的，从而拒绝服务攻击也成为了攻击者的终极手法。攻击者进行拒绝服务攻击，实际上让服务器实现两种效果：一是迫使服务器的缓冲区满，不接收新的请求；二是使用 IP 欺骗，迫使服务器把合法用户的连接复位，影响合法用户的连接。DDos 是分布式 Dos 的缩写，也是拒绝服务攻击的一种形式。从原理可以看出拒绝服务攻击 Dos 不会造成密码的泄露。

(12) 不是蠕虫病毒。

(12) A. 熊猫烧香

B. 红色代码

C. 冰河

D. 爱虫病毒

【答案】C

【解析】本题考查计算机病毒的基础知识。

“蠕虫”(Worm)是一个程序或程序序列，它是利用网络进行复制和传播，传染途径是通过网络、移动存储设备和电子邮件。最初的蠕虫病毒定义是在 DOS 环境下，病毒发作时会在

屏幕上出现一条类似虫子的东西，胡乱吞吃屏幕上的字母并将其改形，蠕虫病毒因此而得名。

常见的蠕虫病毒有红色代码、爱虫病毒、熊猫烧香、Nimda 病毒、爱丽兹病毒等。

冰河是木马软件，主要用于远程监控。冰河木马后经其他人多次改写形成多种变种，并被用于入侵其他用户的计算机的木马程序。

熊猫烧香是一种经过多次变种的“蠕虫病毒”变种，2006 年 10 月 16 日由 25 岁的中国湖北武汉新洲区人李俊编写，这是名副其实的病毒，拥有感染传播功能，2007 年 1 月初肆虐网络，它主要通过下载的档案传染，受到感染的机器文件因为被误携带间接对其它计算机程序、系统破坏严重。2013 年 6 月病毒制造者张顺和李俊伙同他人开设网络赌场案，再次获刑。

“红色代码”病毒是 2001 年一种新型网络病毒，其传播所使用的技术可以充分体现网络时代网络安全与病毒的巧妙结合，将网络蠕虫、计算机病毒、木马程序合为一体，开创了网络病毒传播的新路，可称之为划时代的病毒。

冰河是一种木马软件。

2000 年 5 月 4 日，一种名为“我爱你”的电脑病毒开始在全球各地迅速传播。这个病毒是通过 Microsoft Outlook 电子邮件系统传播的，邮件的主题为“I LOVE YOU”，并包含一个附件。一旦在 Microsoft Outlook 里打开这个邮件，系统就会自动复制并向地址簿中的所有邮件地址发送这个病毒。

“我爱你”病毒，又称“爱虫”病毒，是一种蠕虫病毒，它与 1999 年的梅丽莎病毒非常相似。据称，这个病毒可以改写本地及网络硬盘上面的某些文件。用户机器染毒以后，邮件系统将会变慢，并可能导致整个网络系统崩溃。

甲公司接受乙公司委托开发了一项应用软件，双方没有签订任何书面合同。在此情形下，(13) 享有该软件的著作权。

(13) A. 甲公司 B. 甲、乙公司协商 C. 乙公司 D. 甲、乙公司均不

【答案】A

【解析】

委托开发软件著作权关系的建立，通常由委托方与受委托方订立合同而成立。委托开发软件关系中，委托方的责任主要是提供资金、设备等物质条件，并不直接参与开发软件的创作开发活动。受托方的主要责任是根据委托合同规定的目标开发出符合条件的软件。关于委托开发软件著作权的归属，《计算机软件保护条例》第十二条规定：“受他人委托开发的软件，

其著作权的归属由委托者与受委托者签定书面协议约定，如无书面协议或者在协议中未作明确约定，其著作权属于受委托者。”根据该条的规定，确定委托开发的软件著作权的归属应当掌握两条标准：

①委托开发软件系根据委托方的要求，由委托方与受托方以合同确定的权利和义务的关系而进行开发的软件，因此软件著作权归属应当作为合同的重要条款予以明确约定。对于当事人已经在合同中约定软件著作权归属关系的，如事后发生纠纷，软件著作权的归属仍应当根据委托开发软件的合同来确定。

②对于在委托开发软件活动中，委托者与受委托者没有签定书面协议，或者在协议中未对软件著作权归属作出明确的约定，其软件著作权属于受委托者，即属于实际完成软件的开发者。

接受他人委托开发的软件，其著作权的归属由委托人与受托人签订书面合同约定；无书面合同或者合同未作明确约定的，其著作权由创作方享有。

甲、乙软件公司于2013年9月12日就其财务软件产品分别申请“大堂”和“大唐”商标注册。两财务软件相似，且经协商双方均不同意放弃使用其申请注册的商标标识。此情形下，(14) 获准注册。

- (14)A. “大堂”
C. “大唐”

- B. “大堂”与“大唐”都能
D. 由甲、乙抽签结果确定谁能

【答案】D

【解析】

我国商标注册采取“申请在先”的审查原则，当两个或两个以上申请人在同一种或者类似商品上申请注册相同或者近似商标时，商标主管机关根据申请时间的先后，决定商标权的归属，申请在先的人可以获得注册。对于同日申请的情况，使用在先的人可以获得注册。如果同日使用或均未使用，则采取申请人之间协商解决，协商不成的，由各申请人抽签决定。类似商标是指在同一种或类似商品上用作商标的文字、图形、读音、含义或文字与图形的整体结构上等要素大体相同的商标，即易使消费者对商品的来源产生误认的商标。甲、乙两公司申请注册的商标，“大堂”与“大唐”读音相同、文字相近似，不能同时获准注册。在协商不成的情形下，由甲、乙公司抽签结果确定谁能获准注册。

“相同商标”是指文字、数字、图形、三维标志或颜色组合等商标的构成要素的发音、视觉、含义或排列顺序及整体结构上虽有一定区别，但又使人难以区分，容易产生混淆的商

标。

“大堂”和“大唐”按照商标的显著性要求，属于相同商标，对于相同商标同时申请，又无法提供谁先使用的证明，就需要商量确定。如果双方都不放弃，就采用抽签的方式。

假设系统采用 PV 操作实现进程同步与互斥，若 n 个进程共享两台打印机，那么信号量 S 的取值范围为 (15)。

- (15) A. $-2 \sim n$ B. $-(n-1) \sim 1$ C. $-(n-1) \sim 2$ D. $-(n-2) \sim 2$

【答案】D

【解析】本题考查的是操作系统 PV 操作方面的基本知识。

系统采用 PV 操作实现进程同步与互斥，若有 n 个进程共享两台打印机，那么信号量 S 初值应为 2。当第 1 个进程执行 P(S) 操作时，信号量 S 的值减去 1 后等于 1；当第 2 个进程执行 P(S) 操作时，信号量 S 的值减去 1 后等于 0；当第 3 个进程执行 P(S) 操作时，信号量 S 的值减去 1 后等于 -1；当第 4 个进程执行 P(S) 操作时，信号量 S 的值减去 1 后等于 -2；……；当第 n 个进程执行 P(S) 操作时，信号量 S 的值减去 1 后等于 $-(n-2)$ 。可见，信号量 S 的取值范围为 $-(n-2) \sim 2$ 。

在 PV 操作中，信号量用于表示系统中现有资源的数量，有两台打印机，故信号量初值为 2。前两个进程请求能够满足。当有进程运行时，其他进程访问信号量，信号量就会减一， n 个进程同时请求两台打印机时为 $2-n$ ，当信号量值为负数时，代表这类资源系统已经分配完毕。此时，对负数取绝对值能得到当前等待进程数量。

假设段页式存储管理系统中的地址结构如下图所示，则系统(16)。

31	2221	12 11	0
段号	页号	页内地址	

- (16) A. 最多可有 2048 个段，每个段的大小均为 2048 个页，页的大小为 2K
B. 最多可有 2048 个段，每个段最大允许有 2048 个页，页的大小为 2K
C. 最多可有 1024 个段，每个段最大大小均为 1024 个页，页的大小为 4K
D. 最多可有 1024 个段，每个段最大允许有 1024 个页，页的大小为 4K

【答案】D

【解析】本题考查操作系统页式存储管理方面的基础知识。

从题目给出的段号、页号、页内地址位数情况，可以推算出每一级寻址的寻址空间。

如：已知页内地址是从第 0 位到第 11 位，共 12 个位，所以一个页的大小为： $2^{12}=4K$ 。

页号是从第 12 位到第 21 位，共 10 个位，所以一个段中有 $2^{10}=1024$ 个页。

段号是从第 21 位到第 31 位，共 10 个位，所以一共有 $2^{10}=1024$ 个段。

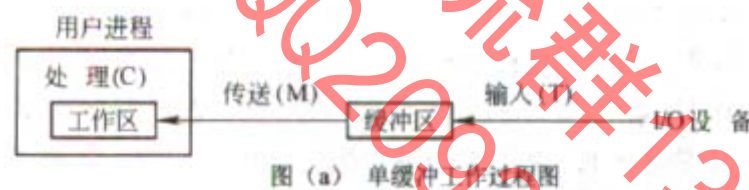
假设磁盘块与缓冲区大小相同，每个盘块读入缓冲区的时间为 $10\mu s$ ，由缓冲区送至用户区的时间是 $5\mu s$ ，系统对每个磁盘块数据的处理时间为 $2\mu s$ 。若用户需要将大小为 10 个磁盘块的 Doc1 文件逐块从磁盘读入缓冲区，并送至用户区进行处理，那么采用单缓冲区需要花费的时间为(17) μs ；采用双缓冲区需要花费的时间为(18) μs 。

- (17) A. 100 B. 107 C. 152 D. 170
(18) A. 100 B. 107 C. 152 D. 170

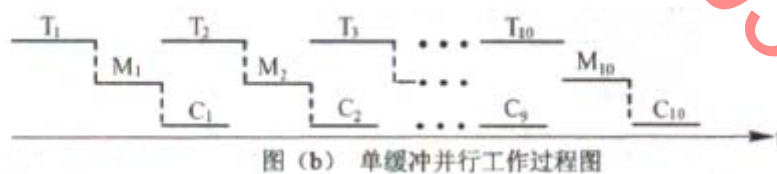
【答案】C B

【解析】

在块设备输入时，假定从磁盘把一块数据输入到缓冲区的时间为 T ，缓冲区中的数据传送到用户工作区的时间为 M ，而系统处理（计算）的时间为 C ，如图（a）所示：



当第一块数据送入用户工作区后，缓冲区是空闲的可以传送第二块数据。这样第一块数据的处理 C_1 与第二块数据的输入 T_2 是可以并行的，依次类推，如图（b）所示。系统对每一块数据的处理时间为： $\max(C, T)+M$ 。因为，当 $T>C$ 时，处理时间为 $M+T$ ；当 $T<C$ 时，处理时间为 $M+C$ 。本题每一块数据的处理时间为 $10+5=15$ ，Doc1 文件的处理时间为 $15 \times 10+2$ 。

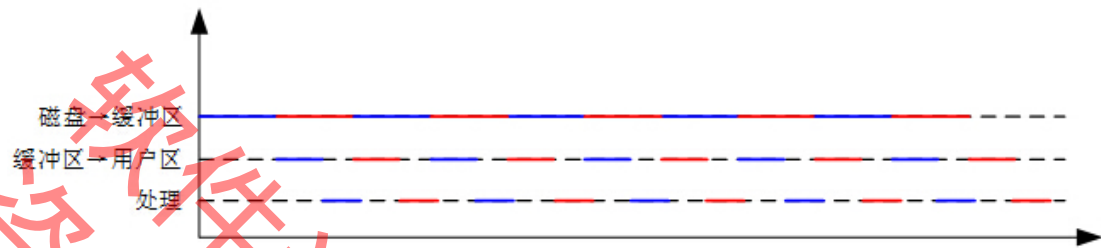


但在解题过程中，我们可以发现需要用到计算机组成原理中的流水线知识。因为进行处理时，每个数据要经过 3 个步骤：读入缓冲区、送用户区、处理。这三个步骤中，有两个步骤是需要用到缓冲区的，这两个步骤执行时，缓冲区都不可以开始下一个磁盘区的处理工作，所以三个步骤可合并为两个：读入缓冲区并送用户区、处理。此时，可应用流水线的方式来提升效率。所以用户将大小为 10 个磁盘块的 File1 文件逐块从磁盘读入缓冲区，并送用户

区进行处理，采用单缓冲时需要花费的时间为：

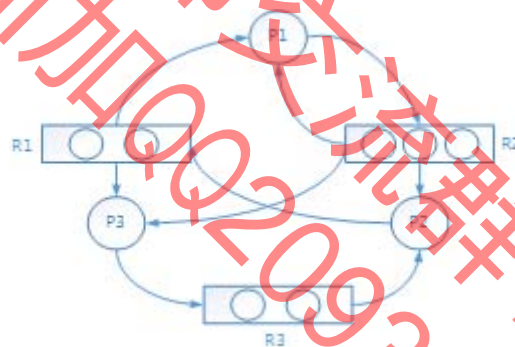
$$(10+5+2) + (10-1) * (10+5) = 152\mu s$$

若增加一个缓冲区，情况如图所示。



从图可知，使用双缓冲区时，从磁盘向缓冲区中传送数据的工作可通过两个缓冲区持续交替进行，所以计算方式为： $10*10+5+2=107\mu s$ 试题答案

在如下所示的进程资源图中，(19)。



(19) A. P1、P2、P3 都是阻塞节点

B. P1 是阻塞节点、P2、P3 是非阻塞节点

C. P1、P2 是阻塞节点、P3 是非阻塞节点

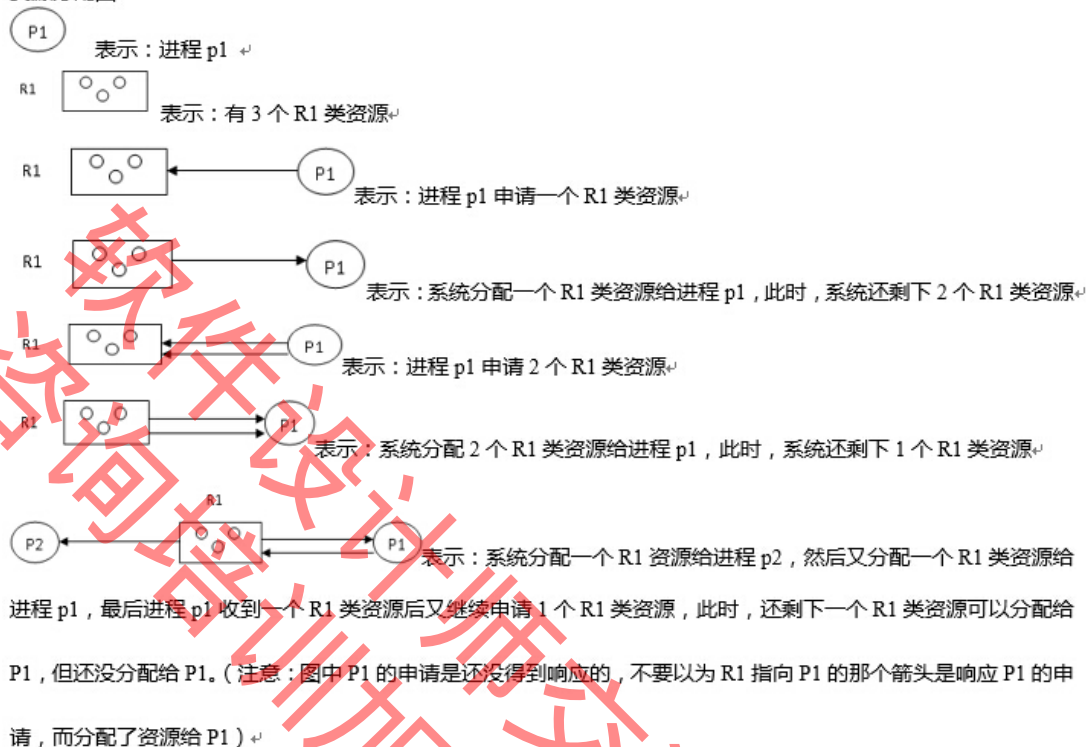
D. P1、P2 是非阻塞节点、P3 是阻塞节点

【答案】C

【解析】

图中 R1 资源只有 2 个，P2 进程申请该资源得不到满足，故 P2 进程是阻塞节点；R2 资源只有 3 个，为 P1、P2、P3 各分配一个，P1 再申请该资源得不到满足，故 P1 进程也是阻塞节点；R3 资源只有 2 个，分配 1 个给 P2 进程，还有 1 个可用，P3 申请该资源可以得到满足，故 P3 是非阻塞节点。

资源分配图



图为一个资源分配图，图中有 3 个节点，3 个资源，从资源到节点的箭头表示系统分配一个资源给节点，从节点到资源的箭头表示节点申请一个资源，特别要注意的是先分配后申请的关系，图中系统先从 R2 分配一个资源给 P1，P1 再从 R2 申请一个资源。理解上面的关系后这道题目就不难了，可以看到，R1 分配了一个资源给 P1，又分配了一个资源给 P3，P2 再从 R1 申请资源，故 P2 阻塞，R2 分配了 3 个资源给 P1、P2、P3，但 P1 还从 R2 申请资源，故 P1 也阻塞，R3 只分配一个资源给 P2，R3 有 2 个资源，故可以满足 P3 的申请，故 P3 不阻塞。

在数据库逻辑结构设计阶段，需要(20)阶段形成的(21)作为设计依据。

(20) A. 需求分析 B. 概念结构设计 C. 物理结构设计 D. 数据库运行与维护

(21) A. 程序文档、数据字典和数据流图 B. 需求说明文档、数据文档和数据流图

C. 需求说明文档、数据字典和数据流图 D. 需求说明文档、数据字典和程序文档

【答案】A C

【解析】本题考查数据库系统基础知识。

数据库设计主要分为用户需求分析、概念结构、逻辑结构和物理结构设计四个阶段。其中，在用户需求分析阶段中，数据库设计人员采用一定的辅助工具对应用对象的功能、性能、

限制等要求所进行的科学分析，并形成需求说明文档、数据字典和数据流程图。

用户需求分析阶段形成的相关文档用以作为概念结构设计的设计依据。

逻辑结构设计是在概念结构设计的基础上进行的数据模型设计的基础上进行的数据模型设计，可以是层次、网状模型和关系模型。由于当前的绝大多数 DBMS 都是基于关系模型的，E-R 方法又是概念结构设计的主要方法，如何在全局 E-R 图基础上进行关系模型的逻辑结构设计成为这一阶段的主要内容。

但本题中第 2 个选项中并没有涉及概念阶段的成果，所以结合第 2 问进行选择，应该选择需求分析阶段，而需求阶段形成的产物为：需求说明文档、数据字典和数据流程图

给定关系模式 $R(A, B, C, D)$ 、 $S(C, D, E)$ ，与 $\pi_{1,3,5}(\sigma_{2='软件工程'}(R \bowtie S))$ 等价的 SQL 语句如下：

SELECT _____ (22) FROM R, S WHERE _____ (23) ;

(22) A. A, C, S. C B. A, B, E C. A, R. C, E D. A, R, C, S. D

(23) A. B='软件工程' OR R. C=S. C AND R. D=S. D

B. B='软件工程' OR R. C=S. C AND R. D=S. D

C. B='软件工程' OR R. C =S. C OR R. D =S. D

D. B='软件工程' AND R. C =S. C AND R. D=S. D

【答案】C D

【解析】

试题 (22) 的正确答案为选项 C。 $\pi_{1,3,5}(\sigma_{2='软件工程'}(R \bowtie S))$ 的含义是从 $R \bowtie S$ 结果集中选取 B='软件工程'的元组，再进行 R.A、R.C 和 S.E 投影。

试题 (23) 的正确答案为选项 D。自然联结 $R \bowtie S$ 中的公共属性为 C、D，所以在 SQL 中可以用条件“WHERE R.C =S.C AND R.D =S.D”来限定；对于选取运算 $\sigma_{2='软件工程'}$ 在 SQL 中可以用条件“WHERE B='软件工程'”来限定。

该关系代数表示的意思是：先关系 R 与关系 S 进行自然连接运算，形成新的结果集，然后新的结果集中进行选择运算，选择运算的条件是 第 2 列的值为“软件工程”，接下来再选择运算的结果集上再进行投影运算，选择 1 3 5 列。

由于 R 与 S 关系中，存在重复的列 C、D，因此需要在加上关系的名称，表示该列来自哪个关系，如： R.C。

自然连接运算，要求在结果集中消除重复的列，即 R 与 S 关系中 C、D 列，只能保留一个关系中的 C、D 列，所以自然连接运算后的关系列一个有：5 列 即 A、B、R.C（或者 S.C）、R.D（或者 S.D）、E。

第二问是要指定连接的条件：选择运算的连接条件为：第 2 列的值为软件工程，B=' 软件工程'， 同时需要进行自然连接运算，因此条件中需要 R.C=S.C AND R.D=S.D，因此：该题要选 B=' 软件工程' AND R.C=S.C AND R.D=S.D

下列查询 B=“信息”且 E=“北京”的 A、B、E 的关系代数表达式中，查询效率最高的是(24)。

- (24) A. $\pi_{1,2,7}(\sigma_{2='信息'\wedge 3=5\wedge 4=6\wedge 7='北京'}(R \times S))$
- B. $\pi_{1,2,7}(\sigma_{3=5\wedge 4=6}(\sigma_{2='信息'}(R) \times \sigma_{5='北京'}(S)))$
- C. $\pi_{1,2,7}(\sigma_{3=5\wedge 4=6\wedge 2=''}(R \times \sigma_{7=''}(S)))$
- D. $\pi_{1,2,7}(\sigma_{3=5\wedge 4=6\wedge 7='北京'}(\sigma_{2='信息'}(R) \times S))$

【答案】B

【解析】

关系代数表达式查询优化的原则如下：

①提早执行选取运算。对于有选择运算的表达式，应优化成尽可能先执行选择运算的等价表达式，以得到较小的中间结果，减少运算量和从外存读块的次数。

②合并乘积与其后的选择运算为连接运算。在表达式中，当乘积运算后面是选择运算时，应该合并为连接运算，使选择与乘积一道完成，以避免做完乘积后，需再扫描一个大的乘积关系进行选择运算。

③将投影运算与其后的其他运算同时进行，以避免重复扫描关系。

④将投影运算和其前后的二目运算结合起来，使得没有必要为去掉某些字段再扫描一遍关系。

⑤在执行连接前对关系适当地预处理，就能快速找到要连接的元组。方法有两种：索引连接法、排序合并连接法。

⑥存储公共子表达式。对于有公共子表达式的结果应存于外存（中间结果），这样，当

从外存读出它的时间比计算的时间少时，就可节约操作时间。

显然，根据原则①尽量提早执行选取运算。

提早执行选取运算。对于有选择运算的表达式，优化的原则可能先执行选择运算的等价表达式，以得到较小的中间结果，减少运算量和从外存读块的次数

合并乘积与其后的选择运算为连接运算。在表达式中，当乘积运算后面是选择运算时，应该合并为连接运算，使选择与乘积一道完成，以避免完成乘积后，再对一个大的乘积关系进行选择运算

将投影运算与其后的其他运算同时进行，以避免重复扫描关系

将投影运算和其后的二目运算结合起来，使得没有必要为去掉某些字段再扫描一遍关系

在执行连接前对关系做适当的预处理，就能快速找到要连接的元组。方法有两种：即索引连接法和排序合并连接法

存储公共子表达式。公共子表达式的结果应存于外存（中间结果），这样，当从外存读出它的时间比计算时间少时，就可节约操作时间

在数据库系统中；数据的(25)是指保护数据库，以防止不合法的使用所造成的数据泄漏、更改或破坏。

- (25) A. 安全性 B. 可靠性 C. 完整性 D. 并发控制

【答案】A

【解析】本题考查数据库系统概念方面的基本概念。

数据控制功能包括对数据库中数据的安全性、完整性、并发和恢复的控制。其中：

①安全性 (security)是指保护数据库受恶意访问，即防止不合法的使用所造成的数据泄漏、更改或破坏。这样，用户只能按规定对数据进行处理，例如，划分了不同的权限，有的用户只能有读数据的权限，有的用户有修改数据的权限，用户只能在规定的权限范围内操纵数据库。

②完整性 (integrality)是指数据库正确性和相容性，是防止合法用户使用数据库时向数据库加入不符合语义的数据。保证数据库中数据是正确的，避免非法的更新。

③并发控制 (concurrency control)是指在多用户共享的系统中，许多用户可能同时对同一数据进行操作。DBMS 的并发控制子系统负责协调并发事务的执行，保证数据库的完整性不受破坏，避免用户得到不正确的数据。

④故障恢复 (recovery from failure)。数据库中的 4 类故障是事务内部故障、系统故

障、介质故障及计算机病毒。故障恢复主要是指恢复数据库本身，即在故障引起数据库当前状态不一致后，将数据库恢复到某个正确状态或一致状态。恢复的原理非常简单，就是要建立冗余 (redundancy) 数据。换句话说，确定数据库是否可恢复的方法就是其包含的每一条信息是否都可以利用冗余地存储在别处的信息重构。冗余是物理级的，通常认为逻辑级是没有冗余的。

//-----
数据控制功能包括对数据库中的数据的安全性、完整性、并发和恢复的控制

数据库的安全性保护: 数据库的安全性是指保护数据库以防止不合法的使用所造成的数据泄露、更改或破坏。用户只能按规定对数据进行处理。例如，划分不同的权限，有的用户只能有读数据的权限，有的用户有修改数据的权限。用户只能在规定的权限范围内操纵数据库

数据的完整性: 数据库的完整性是指数据库的正确性和相容性，是防止合法用户使用数据库时向数据库加入不符合语义的数据。保证数据库中数据是正确的，避免非法的更新

并发控制: 在多用户共享的系统中，许多用户可能同时对同一数据进行操作。并发操作带来的问题是数据的不一致性，主要有丢失更新、不可重复读和读脏数据 3 类，其主要原因是事务的并发操作破坏了事务的隔离性。DBMS 的并发控制子系统负责协调并发事务的执行，保证数据库的完整性不受破坏，避免用户得到不正确的数据

故障恢复: 数据库中的 3 类故障是事务内部故障、系统故障以及介质故障

PPP 中的安全认证协议是(26)，它使用三次握手的会话过程传送密文。

(26) A. MD5

B. PAP

C. CHAP

D. HASH

【答案】C

【解析】

PPP 认证是可选的。PPP 扩展认证协议 (Extensible Authentication Protocol, EAP) 可支持多种认证机制，并且允许使用后端服务器来实现复杂的认证过程，例如通过 Radius 服务器进行 Web 认证时，远程访问服务器 (RAS) 只是作为认证服务器的代理传递请求和应答报文，并且当识别出认证成功/失败标志后结束认证过程。通常 PPP 支持的两个认证协议是：

①口令验证协议 (Password Authentication Protocol, PAP)：提供了一种简单的两次握手认证方法，由终端发送用户标识和口令字，等待服务器的应答，如果认证不成功，则终止连接。这种方法不安全，因为采用文本方式发送密码，可能会被第三方窃取；

②质询握手认证协议 (Challenge Handshake Authentication Protocol, CHAP)：采用

三次握手方式周期地验证对方的身份。首先是逻辑链路建立后认证服务器就要发送一个挑战报文(随机数),终端计算该报文的 Hash 值并把结果返回服务器,然后认证服务器把收到的 Hash 值与自己计算的 Hash 值进行比较,如果匹配,则认证通过,连接得以建立,否则连接被终止。计算 Hash 值的过程有一个双方共享的密钥参与,而密钥是不通过网络传送的,所以 CHAP 是更安全的认证机制。在后续的通信过程中,每经过一个随机的间隔,这个认证过程都可能被重复,以缩短入侵者进行持续攻击的时间。值得注意的是,这种方法可以进行双向身份认证,终端也可以向服务器进行挑战,使得双方都能确认对方身份的合法性。

//-----

点对点协议(PPP)目前支持两个认证协议: 密码验证协议(PAP)和质询握手验证协议(CHAP)。在 RFC 1334 指定和同步和异步接口支持两个。

PAP 使用双向握手为远程节点提供一个简单的设立身份的方法。PPP 链路建立阶段完成后,用户名和密码通过链路(在明文)进行不断重复发送,直到鉴权完成或连接终止为止。

PAP 不是一个安全的认证协议。在链路中以明文形式发送密码,并且此处不提供防止重放或跟踪错误进攻的保护措施。远程节点是由登录尝试的频率和定时控制。

CHAP: 挑战握手认证协议, 全称: Challenge Handshake Authentication Protocol。CHAP 通过三次握手验证被认证端的身份,在初始链路建立时完成,为了提高安全性,在链路建立之后周期性进行验证。CHAP 比 PAP 更安全,因为 CHAP 不在线路上发送明文,而是发送经过 MD5 过的随机数序列。CHAP 支持单向和双向认证。

ICMP 协议属于因特网中的(27)协议, ICMP 协议数据单元封装在(28)中传送。

- (27) A. 数据链路层 B. 网络层 C. 传输层 D. 会话层
- (28) A. 以太帧 B. TCP 段 C. UDP 数据报 D. IP 数据报

【答案】B D

【解析】

ICMP (Internet control Message Protocol)与 IP 协议同属于网络层,用于传送有关通信问题的消息,例如,数据报不能到达目标站,路由器没有足够的缓存空间,或者路由器向发送主机提供最短通路信息等。ICMP 报文封装在 IP 数据报中传送,因而不保证可靠的提交。

//-----

ICMP 协议是一种面向无连接的协议,用于传输出错报告控制信息。是 TCP/IP 协议族的

一个子协议，属于网络层协议，主要用于在主机与路由器之间传递控制信息，包括报告错误、交换受限控制和状态信息等。当遇到 IP 数据无法访问目标、IP 路由器无法按当前的传输速率转发数据包等情况时，会自动发送 ICMP 消息。ICMP 报文在 IP 帧结构的首部协议类型字段 (Protocol 8bit) 的值=1。

网络层数据是封装在 IP 数据包中进行传输的

DHCP 客户端可从 DHCP 服务器获得 (29)。

- (29) A. DHCP 服务器的地址和 Web 服务器的地址
B. DNS 服务器的地址和 DHCP 服务器的地址
C. 客户端地址和邮件服务器地址
D. 默认网关的地址和邮件服务器地址

【答案】B

【解析】 本题考查 DHCP 协议的工作原理。

DHCP 客户端可从 DHCP 服务器获得本机 IP 地址、DNS 服务器的地址、DHCP 服务器的地址、默认网关的地址等，但没有 Web 服务器、邮件服务器地址。

//-----

DHCP (Dynamic Host Configuration Protocol, 动态主机配置协议) 是一个局域网的网络协议，使用 UDP 协议工作，主要有两个用途：给内部网络或网络服务提供商自动分配 IP 地址，给用户或者内部网络管理员作为对所有计算机作中央管理的手段

在 DHCP 数据包中可以包含客户机 MAC 地址、DHCP 服务器 IP、默认网关地址、DHCP 租约时间、分配给客户端的 IP 地址和子网掩码以及一些其它的管理配置信息

分配给某公司网络的地址块是 210. 115. 192. 0/20，该网络可以被划分为 (30) 个 C 类子网。

- (30) A. 4 B. 8 C. 16 D. 32

【答案】C

【解析】

由于分配给公司网络的地址块是 210. 115. 192. 0/20, 留给子网掩码的比特数只有 4 位，所以只能划分为 16 个 C 类子网，这 16 个 C 类子网的子网号为 11000000~11001111, 即 192~207, 所以 210. 115. 210. 0 不属于该公司的网络地址。

//-----

C 类 IP 地址默认的子网掩码为 24 位，即对 210.115.192.0/20 需要向主机位借 4 位用于来表示网络，即用于表示子网位的位数为 4 位，一个有 $2^4=16$ 个子网

在项目初始阶段，软件开发首先需要(31)。

(31) A. 理解要解决的问题

B. 确定解决方案

C. 确定参与开发的人员

D. 估算开发成本

【答案】A

【解析】本题考查软件工程的基础知识。

在项目开发初始阶段，首先需要理解待解决的问题是什么，才能确定其他方面的内容。

//-----

项目初始阶段的管理：软件开发项目管理的首要阶段需要确定项目的目标范围，包括开发商和客户双方的协议合同、软件产品主要需要实现的功能和这些功能所量化的范围、项目开发的周期等方面。同时，软件所配备的硬件运行环境、性能、稳定性、限制条件都必须同客户明确表明，以满足客户的要求。项目组要系统地阐述项目的范围，确定所要实现的软件系统的资料、功能、性能、目标及预期达到的效果，提出问题及充分描述问题，并进行成本的粗略估计，通过技术评估、经济分析，论证项目在资源、时间、效果、资金、实施方法和技术等方面的可行性。

软件项目管理所涉及的范围覆盖了整个软件(32)。

(32) A. 开发过程

B. 运行与维护过程

C. 定义过程

D. 生存期

【答案】D

【解析】本题考查软件项目管理的基础知识。

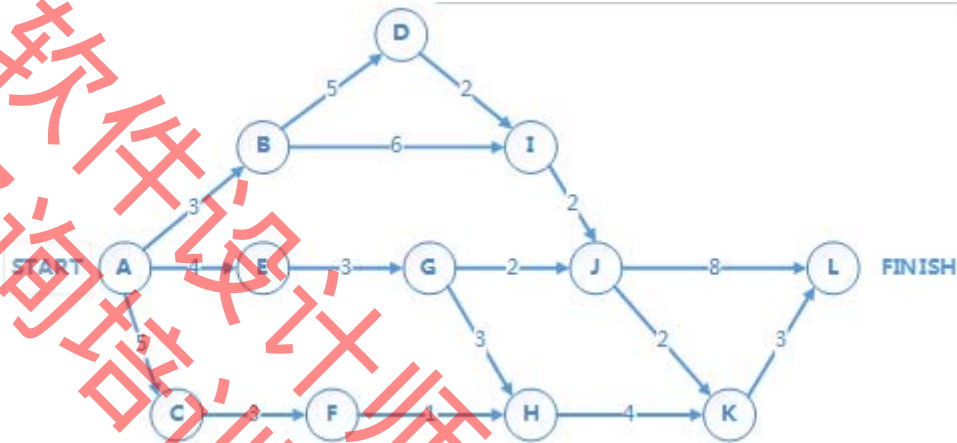
软件项目管理管理整个软件项目的生存期，包括开发过程和维护过程，涉及到人员管理、产品管理、过程管理和项目管理几个方面。

//-----

软件项目管理的对象是软件项目。为了使软件项目开发获得成功，必须对软件开发项目的工作范围、可能遇到的风险、需要的资源、要实现的任务、经历的里程碑、花费的工作量（成本）以及进度的安排等做到心中有数。这种管理的范围覆盖了整个软件工程过程，即开始于技术工作开始之前，在软件从概念到实现的过程中持续进行，最后终止于软件工程过程

结束

下图是一个软件项目的活动图，其中顶点表示项目里程碑，连接顶点的边表示包含的活动，则里程碑(33)在关键路径上。活动 GH 的松弛时间是(34)。



- (33) A. B B. E C. C D. K
(34) A. 0 B. 1 C. 2 D. 3

【答案】A D

【解析】本题考查活动图的基础知识。

根据关键路径法，计算出关键路径为 A—B—D—I—J—L，其长度为 20。因此里程碑 B 在关键路径上，而里程碑 E、C 和 K 不在关键路径上。包含活动 GH 的最长路径是 A—E—G—H—K—L，长度为 17，因此该活动的松弛时间为 $20-17=3$ 。

以下关于瀑布模型的叙述中，正确的是(35)。

- (35) A. 适用于需求被清晰定义的情况
B. 可以快速构造系统的可运行版本
C. 唯一一个适合大规模项目开发的模型
D. 已不能适应当前软件开发的过时模型

【答案】A

【解析】本题考查软件开发过程的基础知识。

软件开发过程以系统需求作为输入，以要交付的产品作为输出，涉及活动、约束和资源使用的一系列工具和技术。瀑布模型、快速原型化模型、增量模型、螺旋模型等都是典型的软件开发过程模型。在 20 世纪 80 年代之前，瀑布模型一直是唯一被广泛采用的生命周期模

型，该模型规定了软件开发从一个阶段瀑布般的转换到另一个阶段。其优点是：

- ①可强迫开发人员采用规范化的方法；
- ②严格地规定了每个阶段必须提交的文档；
- ③要求每个阶段交出的所有产品都必须是经过验证的。

缺点是：

- ①每个阶段开发几乎完全依赖于书面的规格说明，因此可能导致开发出的软件产品不能真正满足用户需求；
- ②适用于项目开始时需求就确定的情况。

//-----

瀑布模型是将软件生存周期各个活动规定为依线性顺序连接的若干阶段的模型。规定了各个阶段由前至后、相互衔接的固定次序，如同瀑布流水，逐级下落。

瀑布模型为软件的开发和维护提供了一种有效的管理模式，根据这一模式制定开发计划，进行成本预算，组织开发力量，以项目的阶段评审和文档控制为手段有效地对整个开发过程进行指导，所以它是以文档为驱动、适合于软件需求很明确的软件项目模型。但是瀑布模型在大量的软件开发实践中也逐渐暴露出它的严重缺点，它是一种理想的线性开发模式，缺乏灵活性，特别是无法解决软件需求不明确或不准确的问题

某开发小组欲开发一个大型软件系统，需求变化较小，此时最不宜采用(36)过程模型。

- (36) A. 瀑布 B. 原型 C. 增量 D. 螺旋

【答案】B

【解析】本题考查软件开发过程的基础知识。

瀑布模型、增量模型和螺旋模型都适宜大型软件系统的开发，原型模型更常用于小规模软件系统的开发。

//-----

原型模型是在需求不是很明确的情况下，快速开发出一个“原型”（可以运行，要反映最终系统部分重要特性），原型模型有利于增进软件开发人员和用户对系统服务需求的理解，适合需求不明确，动态变化的项目

本题需求基本上明确，而且项目较大，向增量、螺旋、瀑布模式都可以适应。

在各种不同的软件需求中，(37)描述了产品必须要完成的任务，可以在用例模型中予以

说明。

- (37) A. 功能需求 B. 业务需求 C. 质量需求 D. 设计约束

【答案】A

【解析】本题考查软件需求的基础知识。

软件需求是为了解决用户的问题和实现用户的目标，用户所需要的软件必须满足的能力和条件。从不同的角度，软件需要有不同的分类。

业务需求描述使用软件系统要达到什么目标；

系统需求，为了满足需求，系统或系统成分必须满足或具有的条件或能力；

功能需求规模软件必须实现的功能性需求，即软件产品必须要完成的任务；

质量需求，也称为非功能需求，在满足功能需求的基础上，要求软件系统还必须具有的特性；

设计约束，规定软件开发过程中的设计决策或限制问题解决方案的设计决策。

//-----

软件需求包括：功能需求、非功能需求和设计约束

功能需求：所开发的软件必须具备什么样的功能

非功能需求：是指产品必须具备的属性或品质，如可靠性、性能、响应时间、容错性和扩展性等

设计约束：也称为限制条件、补充规约，这通常是对解决方案的一些约束说明

以下关于结构化开发方法的叙述中，不正确的是(38)。

- (38) A. 总的指导思想是自顶向下，逐层分解
B. 基本原则是功能的分解与抽象
C. 比面向对象开发方法更适合于开发大规模的、特别复杂的项目
D. 特别适合解决数据处理领域的问题

【答案】C

【解析】本题考查结构化开发方法的基础知识。

结构化开发方法由结构化分析、结构化设计和结构化程序设计构成，是一种面向数据流的开发方法。结构化方法总的指导思想是自顶向下、逐层分解，基本原则是功能的分解与抽象。它是软件工程中最早出现的开发方法，特别适合于数据处理领域的问题，但是不适合解决大规模的、特别复杂的项目，而且难以适应需求的变化。

//-----

结构化方法总的指导思想是自顶向下、逐层分解，它的基本原则是功能的分解与抽象。是软件工程中最早出现的开发方法，特别适合于数据处理领域的问题，但是不适合解决大规模的、特别复杂的项目，且难以适应需求的变化。

模块 A、B 和 C 都包含相同的 5 个语句，这些语句之间没有联系，为了避免重复，把这 5 个语句抽取出来组成一个模块 D，则模块 D 的内聚类型为(39)内聚。以下关于该类内聚的叙述中不正确的是(40)。

- (39) A. 功能 B. 通信 C. 逻辑 D. 巧合
- (40) A. 从模块独立性来看, 是不好的设计 B. 是最弱的一种内聚类型
- C. 是最强的一种内聚类型 D. 不易于软件的修改和维护

【答案】 D C

【解析】 本题考查软件设计的基础知识。

模块独立性是创建良好设计的一个重要原则,一般采用模块间的耦合和模块的内聚两个准则来进行度量。内聚是指模块内部各元素之间联系的紧密程度,内聚度越高,则模块的独立性越好。内聚性一般有以下几种:

①巧合内聚，指一个模块内的各处理元素之间没有任何联系。

逻辑内聚，指模块内执行几个逻辑上相似的功能，通过参数确定该模块完成哪一个功能。

②时间内聚，把需要同时执行的动作组合在一起形成的模块。

③通信内聚,指模块内所有处理元素都在同一个数据结构上操作,或者指各处理使用相同的输入数据或者产生相同的输出数据。

④顺序内聚,指一个模块中各个处理元素都密切相关于同一功能且必须顺序执行,前一个功能元素的输出就是下一个功能元素的输入。

⑤功能内聚，是最强的内聚，指模块内所有元素共同完成一个功能，缺一不可。

上述提到的这几种内聚类型从弱到强,巧合内聚是最弱的一种内聚类型。从模块独立性来看,希望是越强越好,弱内聚不利于软件的修改和维护。

偶然聚合：模块完成的动作之间没有任何关系，或者仅仅是一种非常松散的关系

逻辑聚合：模块内部的各个组成在逻辑上具有相似的处理动作，但功能用途上彼此无关

时间聚合：模块内部的各个组成部分所包含的处理动作必须在同一时间内执行

过程聚合：模块内部各个组成部分所要完成的动作虽然没有关系，但必须按特定的次序执行

通信聚合：模块的各个组成部分所完成的动作都使用了同一个数据或产生同一输出数据

顺序聚合：模块内部的各个部分，前一部分处理动作的最后输出是后一部分处理动作的输入

功能聚合：模块内部各个部分全部属于一个整体，并执行同一功能，且各部分对实现该功能都必不可少

聚合程度：偶然聚合最低，功能聚合最高

在分层体系结构中，(41)实现与实体对象相关的业务逻辑。在基于 JAVA EE 技术开发的软件系统中，常用(42)技术来实现该层。

(41) A. 表示层 B. 控制层 C. 模型层 D. 数据层

(42) A. HTML B. JSP C. Servlet D. EJB

【答案】C D

【解析】本题考查软件设计的基础知识。

在分层体系结构中，表示层是应用系统的用户界面部分，负责用户与应用程序的交互；控制层接收用户请求，选择适当的逻辑层构件处理并接收处理结果，选择适当的界面展示给用户；模型层访问数据层的数据对象，并根据要求进行查询或更新数据，实现业务逻辑功能，Java EE 体系结构中，常用 EJB 技术实现；数据层负责数据的存储。

//-----

在 MVC 模型中，模型层主要负责数据和业务逻辑

EJB 组件用于封装业务逻辑，使得开发人员无需再担心数据访问、事务处理支持、安全性、高速缓存和并发等琐碎任务的编程。

在进行软件设计时，以下结构设计原则中，不正确的是(43)。

- (43) A. 模块应具有较强的独立性，即高内聚和低耦合
- B. 模块之间的连接存在上下级的调用关系和同级之间的横向联系
- C. 整个系统呈树状结构，不允许网状结构或交叉调用关系出现
- D. 所有模块都必须严格地分类编码并建立归档文件

【答案】B

【解析】本题考查软件设计的基础知识。

存在一些好的设计原则，如模块设计应该考虑独立性要强些，模块内高内聚，模块之间

的耦合程度要低；系统的模块之间应该呈树状结构，模块之间存在上下级调用关系，但不允许同级之间的横向联系，也不希望有复杂的网状结构或交叉调用关系：对所有模块必须严格分类编码并建立归档文件。

//-----

为了保证系设计工作的顺利进行，结构设计应遵循如下原则：

- (1) 所划分的模块其内部的凝聚性要强，模块之间的联系要少，即模块具有较强的独立性
- (2) 模块之间的连接只能存在上下级之间的调用关系，不能有同级之间的横向联系
- (3) 整个系统呈树状结构，不允许网状结构或交叉调用关系出现
- (4) 所有模块（包括后继 IPO 图）都必须严格地分类编码并建立归档文件。

在软件开发过程中，详细设计的内容不包括(44)设计。

- (44) A. 软件体系结构 B. 算法 C. 数据结构 D. 数据库物理结构

【答案】A

【解析】本考题考查的知识点为软件开发中的详细设计基础知识。

软件体系结构在概要设计阶段设计，而数据结构、相关的算法以及数据库物理结构则在详细设计阶段设计。

//-----

详细设计的基本任务

- (1) 对每个模块进行详细的算法设计。用某种图形、表格和语言等工具将每个模块处理过程的详细算法描述出来
- (2) 对模块内的数据结构进行设计
- (3) 对数据库进行物理设计，即确定数据库的物理结构
- (4) 其他设计。

代码设计：为了提高数据的输入、分类、存储和检索等操作，节约内存空间，对数据库中的某些数据项的值要进行代码设计

输入输出格式设计，用户界面设计。

以下关于文档的叙述中，正确的是(45)。

- (45) A. 仅仅指软件开发过程中产生的文档
- B. 必须是满足一定格式要求的规范文档

- C. 编写文档会降低软件开发的效率
- D. 高质量文档可以提高软件系统的可维护性

【答案】D

【解析】本题考查软件文档的基础知识。

软件由程序、数据和相关文档构成。因此文档是软件的不可或缺的重要组成部分。软件文档不仅包括软件开发过程中产生的文档，还包含在维护过程中的文档。软件文档既包括有一定格式要求的规范文档，在开会过程或其他活动中产生的一些记录文件也是重要的文档。尽管在开发过程中编写文档需要占用开发时间，但是相对于没有文档而言，编写文档使得开发人员对各个阶段的工作都进行周密思考，全盘权衡，从而减少返工。并且可以在开发早期发现错误和不一致性，便于及时加以纠正，因此可以提高软件开发效率。高质量的文档对于提高软件开发质量具有重要的意义，可以提高软件系统的可维护性。

//-----

文档是软件可维护性的决定因素，软件系统的文档可以分为用户文档和系统文档两类。用户文档主要描述系统功能和使用方法，并不关心这些功能是怎样实现的；系统文档描述系统设计、实现和测试等各方面的内容。

在软件维护阶段，将专用报表功能改成通用报表功能，以适应将来可能的报表格式变化，则该维护类型为(46)维护。

- (46) A. 正确性 B. 适应性 C. 完善性 D. 预防性

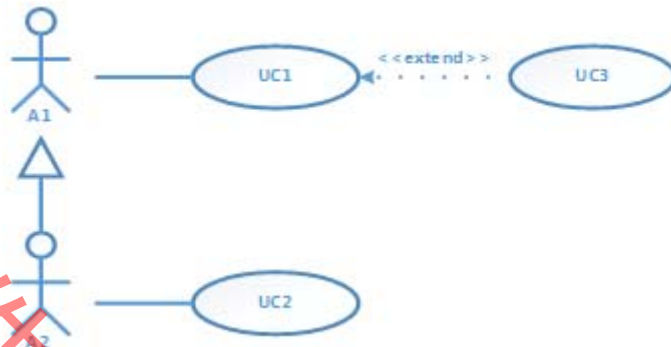
【答案】D

【解析】本题考查软件维护的基础知识。

软件维护一般包括四种类型：

- ①正确性维护，是指改正在系统开发阶段已发生而系统测试阶段尚未发现的错误。
 - ②适应性维护，是指使应用软件适应新型技术变化和管理需求变化而进行的修改。
 - ③完善性维护，是指为扩充功能和改善性能而进行的修改，主要是指对已有的软件系统增加一些在系统分析和设计阶段中没有规定的功能与性能特征。
 - ④预防性维护，是指为了改进应用软件的可靠性和可维护性，为了适应未来的软硬件环境的变化，主动增加预防性的新功能，以使应用系统适应各类变化而不被淘汰。
- 将专用报表功能改成通用报表功能，以适应将来可能的变化，是一种预防性维护。

以下用例图中，A1 和 A2 为(47)。A1 和 A2 的关系为(48)。



(47) A. 参与者 B. 人 C. 系统 D. 外部系统

(48) A. 关联 B. 泛化 C. 包含 D. 扩展

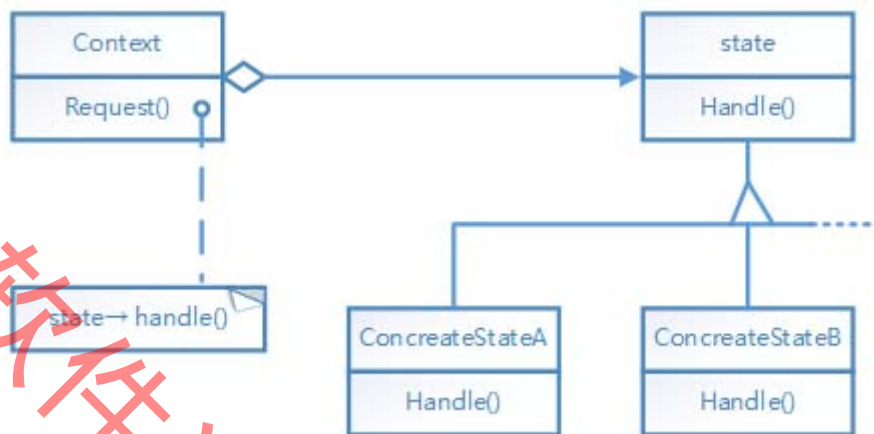
【答案】A B

【解析】本题考查面向对象技术和 UML 的基本概念和基础知识。

上述图是 UML 用例图。用例图根据系统和系统的环境之间的交互，描述可观察到的、用户发起的功能。A1 和 A2 是参与者，空心箭头表示两者之间是泛化的关系。



下图为某设计模式的类图，类 State 和 Context 的关系为(49)，类(50)是客户使用的主要接口。



- (49) A. 继承 B. 实现 C. 聚合 D. 组合
- (50) A. Context B. ConcreteStateA C. ConcreteStateB D. State

【答案】C A

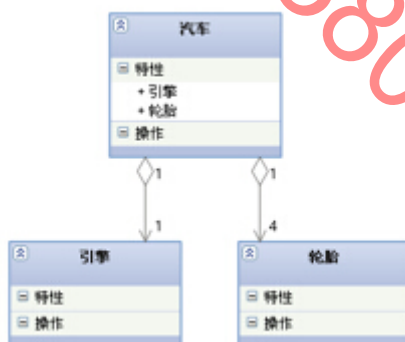
【解析】本题考查面向对象技术和UML的基本概念和基础知识。

上述图是UML状态模式的类图。类图描述了系统中各类对象以及它们之间的各种关系。在该类图中，类State和Context的关系为聚合关系，客户访问类Context。

聚合关系：是整体与部分的关系，如车和轮胎是整体和部分的关系。

聚合关系是关联关系的一种，是强的关联关系；关联和聚合在语法上无法区分，必须考察具体的逻辑关系。

箭头及指向：带空心菱形的实心线，菱形指向整体



Context与State类之间是聚合关系，即整体与部分的关系，用户的主要接口应该是整体，即Context类

软件测试的对象不包括(51)。

- (51) A. 软件代码 B. 软件需求规格说明书
- C. 软件测试报告 D. 软件开发人员

【答案】D

【解析】本题考查软件测试的对象。

根据软件的定义，软件包括程序、数据和文档。软件开发人员不属于上述三者之一，不是软件测试的对象。

以下测试内容中，属于系统测试的是(52)。

①单元测试 ②集成测试 ③安全性测试

④可靠性测试 ⑤兼容性测试 ⑥可用性测试

(52) A. ①②③④⑤⑥ B. ②③④⑤⑥ C. ③④⑤⑥ D. ④⑤⑥

【答案】C

【解析】本题考查系统测试的概念。

根据软件测试策略和过程，软件测试可以划分为单元测试、集成测试、系统测试等阶段。其中，系统测试是将经过集成测试的软件，作为计算机系统的一个部分，与系统中其他部分结合起来，在实际运行环境下对计算机系统进行的一系列严格有效地测试，以发现软件潜在的问题，保证系统的正常运行。安全性测试、可靠性测试、兼容性测试、可用性测试都属于系统测试的范畴。

系统测试是为验证和确认系统是否达到其原始目标，而对集成的硬件和软件系统进行的测试。系统测试是在真实或模拟系统运行的环境下，检查完整的程序系统能否和系统（包括硬件、外设、网络和系统软件、支持平台等）正确配置、连接，并满足用户需求。

常见的系统测试主要有以下内容：

(1) 恢复测试。监测系统的容错能力

(2) 安全性测试。检测系统的安全机制、保密措施是否完善，主要是为了检验系统的防范能力

(3) 压力测试。也称为强度测试，是对系统在异常情况下的承受能力的测试，是检查系统在极限状态下运行时，性能下降的幅度是否在允许的范围内

(4) 性能测试。检查系统是否满足系统设计方案说明书对性能的要求

(5) 可靠性、可用性和可维护性测试

(6) 安装测试

以下关于软件测试原则的叙述中，不正确的是(53)。

(53)A. 测试贯穿于全部软件生命周期，并不是实现完成后才开始

B. 测试用例本身不需要测试

C. 测试用例需要逐步完善、不断修订

D. 当缺陷成群集中出现时，测试时应该更多关注这些缺陷群

【答案】B

【解析】本题考查软件测试的原则。

软件测试应遵循的原则包括：测试贯穿于全部软件生命周期；应当把“尽早和不断地测试”作为开发者的座右铭；程序员应该避免检查自己的程序，测试工作应该由独立的专业的软件测试机构来完成；设计测试用例时，应该考虑到合法的输入和不合法的输入，以及各种边界条件；测试用例本身也应该经过测试；设计好测试用例后还需要逐步完善和修订；一定要注意测试中的错误集中发生现象，应对错误群集的程序段进行重点测试；对测试错误结果一定要有一个确认的过程；制定严格的测试计划，并把测试时间安排得尽量宽松，不要希望在极短的时间内完成一个高水平的测试；回归测试的关联性一定要引起充分的注意，修改一个错误而引起更多错误出现的现象并不少见；妥善保存一切测试过程文档；穷举测试是不能实现的。

根据上述描述，测试用例也是需要经过测试的。因此应选择选项 B。

软件测试的原则：

所有的软件测试都应追溯到用户的需求

尽早地和不断地进行软件测试

完全测试是不可能的，测试需要终止：

输入量太大

输出结果太多

路径组合太多

测试无法显示软件潜在的缺陷

充分注意测试中的群集现象

程序员应避免检查自己的程序（除单元测试以外）

尽量避免测试的随意性

以下关于测试工作在软件开发各阶段作用的叙述中，不正确的是(54)。

(54)A. 在需求分析阶段确定测试的需求分析

- B. 在概要设计和详细设计阶段制定集成测试计划和单元测试计划
- C. 在程序编写阶段制定系统测试计划
- D. 在测试阶段实施测试并提交测试报告

【答案】C

【解析】本题考查软件测试和软件开发的关系。

软件测试和软件开发的关系为：项目规划阶段，负责从单元测试到系统测试的整个测试阶段的规划；需求分析阶段，确定测试需求分析、系统测试计划的制定，评审后成为管理项目；详细设计和概要设计阶段，确保集成测试计划和单元测试计划完成；编码阶段，由开发人员进行自己负责部分的测试代码，当项目较大时，由专人进行编码阶段的测试任务；测试阶段（单元、集成、系统测试），依据测试代码进行测试，并提交相应的测试状态报告和测试结束报告。

根据上述描述，系统测试计划是在需求分析阶段完成的。本题中选项C不正确。

系统测试是将确认的软件、计算机硬件、外设和网络等其他因素结合在一起，进行信息系统的各种集成测试和确认测试，其目的是通过与系他的需求想比较，发现所开发的系统与用户需求不符或矛盾的地方。系统测试是根据系统方案说明书来设计测试用例的，而不是程序代码，所以系统测试计划也应该是在系统需求分析就开始

在引入自动化测试工具以前，手工测试遇到的问题包括(55)。

- ①工作量和时间耗费过于庞大 ②衡量软件测试工作进展困难
- ③长时间运行的可靠性测试问题 ④对并发用户进行模拟的问题
- ⑤确定系统的性能瓶颈问题 ⑥软件测试过程的管理问题

(55) A. ①②③④⑤⑥ B. ①②③④⑤ C. ①②③④ D. ①②③

【答案】A

【解析】本题考查在引入自动化测试之前手工测试的缺点。

手工测试全部依靠人手工完成，因此工作量大且耗时，难以衡量测试工作的进展。手工测试无法模拟软件的长时间运行和大量并发用户的访问，因此难以胜任可靠性测试和性能测试。当测试规模较大时，纯人工的测试过程的管理也会面临困难。

在进行可用性测试时关注的问题应包括(56)。

- ①安装过程是否困难 ②错误提示是否明确

③GUI 接口是否标准 ④登录是否方便

⑤帮助文本是否上下文敏感

(56) A. ①②

B. ①②③

C. ①②③④

D. ①②③④⑤

【答案】D

【解析】本题考查可用性测试的基础知识。

可用性测试一般是在一定环境条件下（可用性实验室），让用户执行测试，观察用户的反映，找到系统的缺陷和需要改进的地方

可用性测试可以从下面几个方面考虑

能否成功的完成一个任务

对于普通用户，完成典型任务需要多长时间

完成典型任务需要访问的的页面数

系统是否提供了层次结构明确、表达清楚的导航功能

对整个系统的感觉如何（形式）

信息是否正确、精确（内容）

帮助系统是否准确并且容易使用

系统是否提供搜索、网站地图等功能

页面下载时间用户能否接受

根据上述描述，题目中这 5 项都属于可用性测试关注的问题，应选择选项 D。

以下叙述中，不正确的是(57)。

(57) A. 黑盒测试可以检测软件行为、性能等特性是否满足要求

B. 黑盒测试可以检测软件是否有人机交互上的错误

C. 黑盒测试依赖于软件内部的具体实现，如果实现发生了变化，则需要重新设计用例

例

D. 黑盒测试用例设计可以和软件实现同步进行

【答案】C

【解析】本题考查黑盒测试的基础知识。

黑盒测试是把程序看作一个不能打开的黑盒子，在完全不考虑程序内部结构和内部特性的情况下，在程序接口进行测试，它只检查程序功能是否按照需求规格说明书的规定正常使用，程序是否能适当地接收输入数据而产生正确的输出信息。黑盒测试着眼于程序外部结构，

不考虑内部逻辑结构，主要针对软件界面和软件功能进行测试。黑盒测试能发现功能错误或者遗漏、输入输出错误以及初始化和终止错误。

由于黑盒测试不考虑程序内部结构，其用例设计可以和软件实现同步，且该方法不依赖于软件内部的具体实现，当实现变化后，只要对外接口不变，则无需重新设计用例。

黑盒测试也称为功能测试，在完全不考虑软件的内部结构和特性的情况下，测试软件的外部特性。进行黑盒测试主要为了发现以下发现以下几类错误：

- (1) 是否有错误的功能或遗漏的功能
- (2) 界面是否有误？输入是否正确接收？输出是否正确？
- (3) 是否有数据结构或外部数据库访问错误？
- (4) 性能是否能够接受？
- (5) 是否有初始化或终止错误？

本题中选项 C 不正确。

以下关于等价类划分法的叙述中，不正确的是(58)。

(58)A. 如果规定输入值 a 的范围为 $1 \sim 99$ ，那么得到两个等价类，即有效等价类 $\{a | 1 \leq a \leq 99\}$ ，无效等价类 $\{a | a < 1 \text{ 或者 } a > 99\}$

B. 如果规定输入值 s 的第一个字符必须为数字，那么得到两个等价类，即有效等价类 $\{s | s \text{ 的第一个字符是数字}\}$ ，无效等价类 $\{s | s \text{ 的第一个字符不是数字}\}$

C. 如果规定输入值 x 取值为 1, 2, 3 三个数之一，那么得到 4 个等价类，即有效等价类 $\{x | x=1\}$ 、 $\{x | x=2\}$ 、 $\{x | x=3\}$ ，无效等价类 $\{x | x \neq 1, 2, 3\}$

D. 如果规定输入值 i 为奇数，那么得到两个等价类，即有效等价类 $\{i | i \text{ 是奇数}\}$ ，无效等价类 $\{i | i \text{ 不是奇数}\}$

【答案】A

【解析】本题考查黑盒测试方法中的等价类划分法。

划分等价类的 6 条原则：

(1) 在输入条件规定了取值范围或值的个数的情况下，可以确立一个有效等价类和两个无效等价类

(2) 在输入条件规定了输入值的集合或者规定了“必须如何”的条件的情况下，可以确立一个有效等价类和一个无效等价类

(3) 在输入条件是一个布尔量的情况下，可确定一个有效等价类和一个无效等价类

(4) 在规定了输入数据的一组值（假定 n 个），并且程序要对每一个输入值分别处理的情况下，可确立 n 个有效等价类和一个无效等价类

(5) 在规定了输入数据必须遵守的规则的情况下，可确立一个有效等价类（符合规则）和若干个无效等价类（从不同角度违反规则）

(6) 在确知已划分的等价类中，各元素在程序处理中的方式不同的情况下，则再将该等价类进一步地划分为更小的等价类

在等价类划分法中，如果规定了输入数据取值范围或值的个数的情况下，可以确定一个有效等价类和两个无效等价类；如果规定了一组输入数据（假设包括 n 个输入值），并且程序要对每一个输入值分别进行处理的情况下，可确定 n 个有效等价类（每个值确定一个有效等价类）和一个无效等价类（所有不允许的输入值的集合）；如果输入条件规定了输入值的集合或规定了“必须如何”的条件下，可以确定一个有效等价类和一个无效等价类（该集合有效值之外）；如果规定了输入数据必须遵守的规则或限制条件的情况下，可确定一个有效等价类（符合规则）和若干个无效等价类（从不同角度违反规则）。

本题中，选项 A 属于规定了输入数据的取值范围，因此应该得到一个有效等价类 $\{a \mid 1 \leq a \leq 99\}$ 和两个无效等价类 $\{a \mid a < 1\}$ 、 $\{a \mid a > 99\}$ 。

以下几种白盒覆盖测试中，覆盖准则最强的是(59)。

(59) A. 语句覆盖 B. 判定覆盖 C. 条件覆盖 D. 条件组合覆盖

【答案】D

【解析】本题考查白盒测试的逻辑覆盖法。

条件组合覆盖，是指设计足够的测试用例，使得每个判定中条件的各种可能值的组合都至少出现一次。满足条件组合覆盖的测试用例是一定满足判定覆盖、条件覆盖和判定/条件覆盖的

根据逻辑覆盖法定义，语句覆盖针对的是语句，是最弱的覆盖准则；判定覆盖和条件覆盖分别针对的是判定和条件，强度次之；判定条件覆盖要同时考虑判定和判定中的条件，满足判定条件覆盖同时满足了判定覆盖和条件覆盖；条件组合覆盖则要考虑同一判定中各条件之间的组合关系，是最强的覆盖准则。

根据上述描述，覆盖准则最强的是条件组合覆盖，应选择选项 D。

对于逻辑表达式 $((a \parallel b) \parallel (c \& d))$ ，需要(60)个测试用例才能完成条件组合覆盖。

(60) A. 2

B. 4

C. 8

D. 16

【答案】D

【解析】本题考查白盒测试中逻辑覆盖法的条件组合覆盖。

条件组合覆盖的含义是：选择足够的测试用例，使得每个判定中条件的各种可能组合都至少出现一次。

本题中有 4 个条件，组合之后需要的用例数是 16, 因此选项 D 正确。

为检测系统所能承受的数据容量，应进行 (61)。

(61) A. 负载测试

B. 压力测试

C. 大数据量测试

D. 疲劳强度测试

【答案】C

【解析】本题考查负载测试、压力测试、疲劳强度测试、大数据量测试的基本知识。

负载测试是通过逐步增加系统负载，测试系统性能的变化，并最终确定在满足性能指标的情况下，系统所能承受的最大负载量的情况。

压力测试是通过逐步增加系统负载，测试系统性能的变化，并最终确定在什么负载条件下系统性能处于失效状态，并以此来获得系统能提供的最大服务级别的测试。

大数据量测试包括独立的数据量测试和综合数据量测试两类。

独立的数据量测试指针对某些系统存储、传输、统计、查询等业务进行的大数据量测试。

综合数据量测试指和压力性能测试、负载性能测试、疲劳性能测试相结合的综合测试

疲劳强度测试是采用系统稳定运行情况下能够支持的最大并发用户数，或者日常运行用户数，持续执行一段时间业务，保证达到系统疲劳强度需求的业务量，通过综合分析交易执行指标和资源监控指标，来确定系统处理最大工作量强度性能的过程。

大数据量测试包括独立的数据量测试和综合数据量测试，独立数据量测试是指针对系统存储、传输、统计、查询等业务进行的大数据量测试；综合数据量测试是指和压力测试、负载测试、疲劳强度测试相结合的综合测试。

本题的目标是检测系统存储的数据容量，应进行的是大数据量测试中的独立数据量测试，因此选项 C 正确。

压力测试不会使用到以下哪种测试手段， (62)。

(62) A. 重复

B. 注入错误

C. 增加量级

D. 并发

【答案】B

【解析】 本题考查压力测试的基础知识。

压力测试是通过逐步增加系统负载，测试系统性能的变化，并最终确定在什么负载条件下系统性能处于失效状态，并以此来获得系统能提供的最大服务级别的测试。重复、增加量级、并发都属于给系统增加压力的手段，而注入错误并不能增加系统压力。

本题中选项 A、C、D 都是压力测试的方法，选项 B，注入错误一般属于安全性和可靠性测试使用的方法

以下测试内容中，不属于 GUI 测试的是(63)。

- (63) A. 窗口相关操作是否符合标准 B. 菜单和鼠标操作是否正确
C. 计算结果是否正确 D. 数据显示是否正常

【答案】 C

【解析】 本题考查 GUI 测试的基本概念。

GUI（图形用户界面）测试关注的是人和机器的交互，窗口操作、菜单操作、鼠标操作、数据显示都属于交互的范畴，因此属于 GUI 测试的内容。

选项 C 计算结果是否正确应属于功能测试的范畴：程序能否适当地接收输入数据而产生正确的输出信息。

以下属于动态测试方法的是(64)。

- (64) A. 代码审查 B. 静态结构测试 C. 路径覆盖 D. 技术评审

【答案】 C

【解析】 本题考查动态测试的基本概念。

选项 C 路径覆盖测试是白盒测试常用的一种方式，属于动态测试方法

代码审查是由若干程序员和测试员组成一个审查小组，通过阅读、讨论和争议，对程序进行静态分析的过程。

静态结构测试是通过测试工具分析程序源代码的系统结构、数据结构、数据接口、内部控制逻辑等内部结构，生成函数调用关系图、模块控制流图、内部文件调用关系图、子程序表、宏和函数参数表等各类图形图表，可以清晰地标识整个软件系统的组成结构，使其便于阅读与理解，然后通过分析这些图表，检查软件有没有存在缺陷或错误

技术评审是由一组评审者按照规范的步骤对软件需求、设计、代码或其他技术文档进行仔细地检查，以找出和消除其中的缺陷

根据上述描述，代码审查、静态结构测试和技术评审都不需要运行被测软件，只有路径覆盖需要通过实际执行来确定程序的运行路径。因此应选择选项 C。

(65) A. 模块间的数据传递是否正确

C. 所有模块组合起来的性能是否能满足要求

D. 函数内局部数据结构是否有问题，会不会被异常修改

【解析】 本题考查集成测试的基础知识。

组装时需要考虑的问题:

(2) 一个模块的功能是否会对另一个模块的功能产生不利的影响

(4) 全局数据结构是否有问题

(5) 单个模块的误差累积起来, 是否会放大, 以致达到不能接受的程度

应选择选项 D。

⑤软件的可靠性投入

D. ①②③④⑤

【答案】D

【解析】本题考查软件可靠性的基本概念。

从技术的角度来看，影响软件可靠性的主要因素如下：

运行剖面（环境）。软件可靠性的定义是相对运行环境而言的，一样的软件在不同的运行剖面下，其可靠性的表现是不一样的

软件规模。也就是软件的大小，一个只有数十行代码的软件和几千万行代码的软件是不能相提并论的

软件内部结构。结构对软件可靠性的影响主要取决于软件结构的复杂程度，一般来说，内部结构越复杂的软件，所包含的软件缺陷数就可能越多

软件的开发方法和开发环境。软件工程表明，软件的开发方法对软件的可靠性有显著的影响，例如，与非结构方法相比，结构化方法可以明显减少软件的缺陷数。

软件的可靠性投入。软件在生命周期中可靠性的投入包括开发者在可靠性设计、可靠性管理、可靠性测试、可靠性评价等方面投入的人力、资金、资源和时间等。经验表明，在早期重视软件可靠性并采取措施开发出来的软件，可靠性有明显的提高

软件可靠性是软件产品在规定的条件下和规定的时间区间完成规定功能的能力。软件运行剖面越多，软件规模越大，内部结构越复杂，则表明软件出错的可能性就越大，可靠性就会越低；软件的开发方法和开发环境不合适或者落后，开发出来的软件就会遗留较多问题，会影响软件可靠性；软件可靠性投入不够，比如可靠性测试不够，也会影响到软件可靠性。根据上述描述，题目中这 5 项都会对软件可靠性产生影响。应选择选项 D。

软件可靠性管理把软件可靠性活动贯穿于软件开发的全过程，成为软件工程管理的一部分。确定软件的可靠性目标在(67)阶段。

(67) A. 需求分析 B. 概要设计 C. 详细设计 D. 软件测试

【答案】A

【解析】本题考查软件可靠性的可靠性管理。

软件可靠性管理是软件工程管理的一部分，它以全面提高和保证软件可靠性为目标，以软件可靠性活动为主要对象，是把现代管理理论用于软件生命周期中的可靠性保障活动的一种管理形式。

1、需求分析阶段

确定软件的可靠性目标

分析可能影响可靠性的因素

确定可靠性的验收标准

制定可靠性管理框架

制定可靠性文档编写规范

制定可靠性活动初步计划

确定可靠性数据收集规范

2、概要设计阶段

确定可靠性度量

制定详细的可靠性验收方案

可靠性设计

收集可靠性数据

调整可靠性活动计划

明确后续阶段的可靠性活动的详细计划

编制可靠性文档

3、详细设计阶段

可靠性设计

可靠性预测（确定可靠性度量估计值）

调整可靠性活动计划

收集可靠性数据

明确后续阶段的可靠性活动的详细计划

编制可靠性文档

4、编码阶段

可靠性测试（含单元测试）

排错

调整可靠性活动计划

收集可靠性数据

明确后续阶段的可靠性活动的详细计划

编制可靠性文档

5、测试阶段

可靠性测试（含于集成测试、系统测试）

排错

可靠性建模

可靠性评价

调整可靠性活动计划

收集可靠性活动计划

收集可靠性数据

明确后续阶段的可靠性活动的详细计划

编制可靠性文档

6. 实施阶段

可靠性测试（含于验收测试）

排错

收集可靠性数据

调整可靠性模型

可靠性评价

编制可靠性文档

根据软件可靠性管理的定义，确定软件的可靠性目标在软件的需求分析阶段。应选择选项 A。

以下关于公钥加密技术的叙述中，不正确的是(68)。

(68) A. 公钥加密的数据可以用私钥解密

B. 私钥加密的数据可以用公钥解密

C. 公钥和私钥相互关联

D. 公钥加密采用与对称加密类似的位模式操作完成对数据的加解密操作

【答案】D

【解析】本题考查公钥加密技术的基础知识。

非对称加密算法需要两个密钥：公开密钥和私有密钥。公开密钥与私有密钥是一对，如果用公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密。因为加密和解密使用的是两个不同的密钥，所以这种算法叫作非对称加密算法

公钥加密使用两个独立的密钥，因此是非对称的，即需要使用一对加密密钥与解密密钥，

这两个密钥是数学相关的。公钥加密的数据可以用私钥解密，私钥加密的数据也可以用公钥解密。与对称加密使用的位模式简单操作不同，公钥加密是基于数学函数的。

综上不难看出，候选答案 D 是不正确的。

包过滤防火墙是一种通过软件检查数据包以实现系统安全防护的基本手段，以下叙述中，不正确的是(69)。

- (69) A. 包过滤防火墙通常工作在网络层以上，因此可以实现对应用层数据的检查与过滤
- B. 包过滤防火墙通常根据数据包源地址、目的地址、端口号和协议类型等标志设置访问控制列表实现对数据包的过滤
- C. 数据包过滤用在内部主机和外部主机之间，过滤系统可以是一台路由器或是一台主机
- D. 当网络规模比较复杂时，由于要求逻辑的一致性、封堵端口的有效性和规则集的正确性等原因，会导致访问控制规则复杂，难以配置管理

【答案】A

【解析】本题考查包过滤防火墙的基础知识。

包过滤防火墙是一种通过软件检查数据包以实现系统安全防护的基本手段，数据包过滤用在内部主机和外部主机之间，过滤系统可以是一台路由器或是一台主机。通常通过查看所流经的数据包的包头来决定整个包的命运，可能会决定丢弃这个包，可能会接受这个包（让这个包通过），也可能执行其他更复杂的动作。具体来说，包过滤防火墙通常根据数据包源地址、目的地址、端口号和协议类型等标志设置访问控制列表实现对数据包的过滤。

包过滤是在 IP 层实现的，包过滤根据数据包的源 IP 地址、目的 IP 地址、协议类型（TCP 包、UDP 包、ICMP 包）、源端口、目的端口等包头信息及数据包传输方向等信息来判断是否允许数据包通过。

当网络规模比较复杂时，由于包过滤防火墙要求逻辑的一致性、封堵端口的有效性和规则集的正确性等原因，会导致访问控制规则复杂，难以配置管理。

包过滤是在网络层中根据事先设置的安全访问策略（过滤规则），检查每一个数据包的源 IP 地址、目的 IP 地址以及 IP 分组头部的其他各种标志信息（如协议、服务类型等），确定是否允许该数据包通过防火墙。

以下测试方法中，不属于典型安全性测试的是(70)。

(70) A. 安全功能验证 B. 漏洞扫描 C. 通信加密 D. 模拟攻击试验

【答案】C

【解析】本题考查包过安全性测试的基础方法。

软件系统的安全性是信息安全的重要组成部分，因此安全性测试是软件测试的重要内容之一。典型的安全测试方法包括安全性功能验证、漏洞扫描、模拟攻击试验以及网络侦听等。而通信加密是典型的安全防护手段，并不属于安全性测试的方法。

功能验证是采用软件测试当中的黑盒测试方法，对涉及安全的软件功能进行测试，主要是验证相关功能是否有效。

漏洞扫描通常是借助特定的漏洞扫描器完成的。通过漏洞扫描器，系统管理人员能够发现所维护的信息系统存在的安全漏洞，从而在信息系统网络安全保卫战中做到“有的放矢”，及时修补漏洞。

模拟攻击试验是一组特殊的黑盒测试案例，以模拟攻击来验证软件或信息系统的安全防护能力。

侦听技术实际上是在数据通信或数据交互过程，对数据进行截取分析的过程；该技术常用于网络加密的验证。

Teams are required for most engineering projects. Although some small hardware or software products can be developed by individuals, the scale and complexity of modern systems is such, and the demand for short schedules so great, that it is no longer (71) for one person to do most engineering jobs. Systems development is a team (72), and the effectiveness of the team largely determines the (73) of the engineering.

Development teams often behave much like baseball or basketball teams. Even though they may have multiple specialties, all the members work toward (74). However, on systems maintenance and enhancement teams, the engineers often work relatively independently, much like wrestling and track teams.

A team is (75) just a group of people who happen to work together. Teamwork takes practice and it involves special skills. Teams require common processes; they need agreed-upon goals; and they need effective guidance and leadership. The methods

for guiding and leading such teams are well known, but they are not obvious.

- (71) A. convenient B. existing C. practical D. real
- (72) A. activity B. job C. process D. application
- (73) A. size B. quality C. scale D. complexity
- (74) A. multiple objectives B. different objectives
C. a single objective D. independent objectives
- (75) A. relatively B. / C. only D. more than

【答案】C A B C D

【解析】

大多数工程项目需要团队完成。虽然有些小规模硬件或软件产品可以由个人完成，但是现代系统的规模大、复杂性高以及开发周期短的极高需求，使得一个人完成大多工程工作已经不再现实。系统开发是一个团队活动，团队的效率很大程度上决定工程的质量。

开发团队经常表现的像是棒球队或篮球队。即使棒球队或篮球队可能有多种不同专长，但是所有的队员都朝着一个目标努力。然而，在系统维护和增强团队，工程师们的工作就像摔跤和田径队一样经常相对独立。

团队不仅仅是一群人碰巧在一起工作。团队工作需要实践，涉及到多种特殊的技能。团队需要共同的过程，需要达成一致的目标，需要有效地指导和领导。尽管指导和领导这样的团队的方法是众所周知的，但是它们并不明显。

试题一

阅读下列 C 程序，回答问题 1 至问题 3，将解答填入答题纸的对应栏内。

【C 程序】

```
int GetMaxDay( int year, int month){  
    int maxday=0; //1  
    if( month>=1&&month<=12){ //2,3  
        if (month==2){ //4  
            if( year%4==0){ //5  
                if (year%100==0){ //6  
                    if(year%400==0) //7  
                        maxday= 29; //8  
                    else //9  
                        maxday= 28;  
                }  
            else //10  
                maxday= 29;  
        }  
    else  
        maxday = 28; //11  
    }  
    else{ //12  
        if (month==4||month==6||month==9||month==11) //13, 14, 15, 16  
            maxday = 30; //17  
        else //18  
            maxday = 31;  
    }  
}  
return maxday; //19  
}
```

【问题 1】

请针对上述 C 程序给出满足 100%DC（判定覆盖）所需的逻辑条件。

【参考答案】

编号	条 件
1	month >= 1 && month <= 12
2	month < 1 month > 12
3	month == 2
续表	
编号	条 件
4	month != 2 && (month >= 1 && month <= 12)
5	year % 4 == 0 && month == 2
6	year % 4 != 0 && month == 2
7	year % 100 == 0 && month == 2
8	year % 100 != 0 && year % 4 == 0 && month == 2
9	year % 400 == 0 && month == 2
10	year % 400 != 0 && year % 100 == 0 && month == 2
11	month == 4 month == 6 month == 9 month == 11
12	(month != 4 && month != 6 && month != 9 && month != 11) && (month >= 1 && month <= 12)

【试题分析】

本题考查白盒测试方法及应用。

本问题考查白盒测试用例设计方法之判定覆盖法。

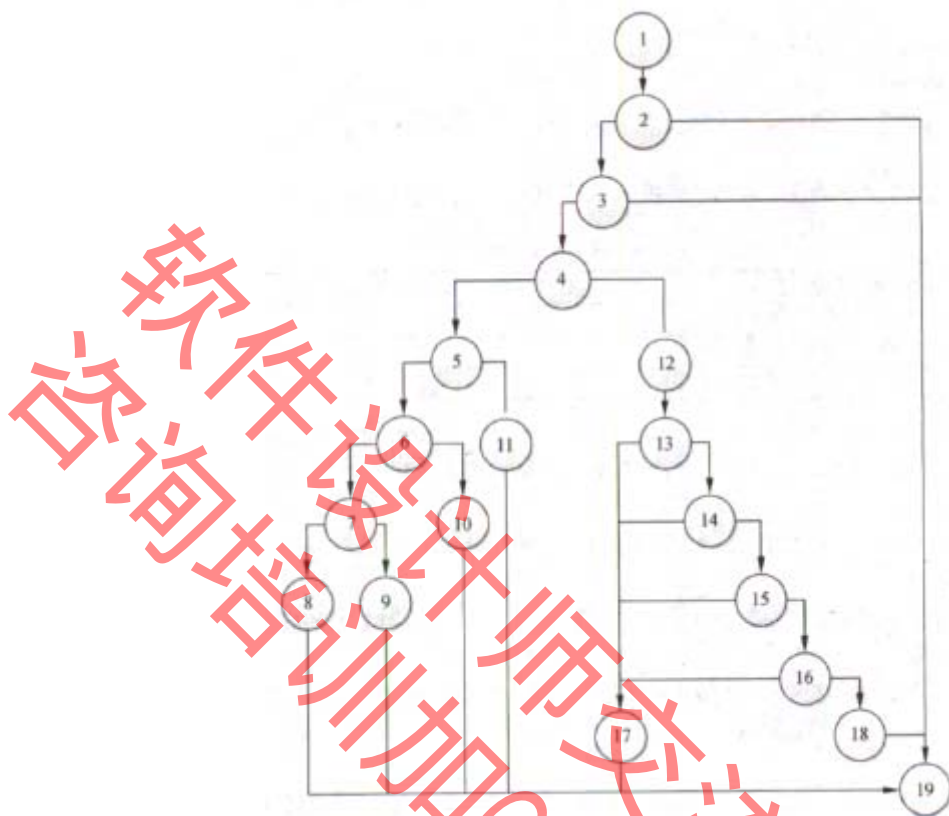
判定覆盖指设计足够的测试用例，使得被测程序中每个判定表达式至少获得一次“真”值和“假”值，从而使程序的每一个分支至少都通过一次。本题中程序有 6 个判定，所以满足判定覆盖一共需要 12 个逻辑条件。

【问题 2】

请画出上述程序的控制流图，并计算其环路复杂度 $V(G)$ 。

【参考答案】

控制流图



【试题分析】

本问题考查白盒测试用例设计方法之基本路径法。

涉及到的知识点包括根据代码绘制控制流图、计算环路复杂度。

控制流图是描述程序控制流的一种图示方式，它由节点和定向边构成。控制流图的节点代表一个基本块，定向边代表控制流的方向。其中要特别注意的是，如果判断中的条件表达式是复合条件，即条件表达式是由一个或多个逻辑运算符连接的逻辑表达式，则需要改变复合条件的判断为一系列之单个条件的嵌套判断。本题程序中，`if(month >= 1 && month <= 12)`，这条判断语句中的判定由两个条件组成，因此在画控制流图的时候需要拆开成两条判断语句。同理，`if(month=4 || month=6 || month=9 || month=11)`这条判断语句中的判定由 4 个条件组成，因此在画控制流图的时候需要拆开成 4 条判断语句。这里需要注意的是，如果复合条件之间是“&&”的关系，则拆开后反应在控制流图上是沿左子树往下，反之如果条件之间是“||”的关系，则在控制流图上是沿右子树往下。

程序的环路复杂度等于控制流图中判定节点的个数加 1，本题控制流图中判定节点个数为 10，所以 $V(G)=11$ 。

【问题 3】

请给出问题 2 中控制流图的线性无关路径。

【参考答案】

线性无关路径：

1. 1-2-19
2. 1-2-3-19
3. 1-2-3-4-12-13-14-15-16-18-19
4. 1-2-3-4-12-13-14-15-16-17-19
5. 1-2-3-4-12-13-14-15-17-19
6. 1-2-3-4-12-13-14-17-19
7. 1-2-3-4-12-13-17-19
8. 1-2-3-4-5-11-19
9. 1-2-3-4-5-6-10-19
10. 1-2-3-4-5-6-7-9-19
11. 1-2-3-4-5-6-7-8-19

【试题分析】

本问题考查白盒测试用例设计方法中的基本路径法。

涉及到的知识点是根据控制流图和环路复杂度给出线性无关路径。

线性无关路径是指包含一组以前没有处理的语句或条件的路径。从控制流图上来看，一条线性无关路径是至少包含一条在其他线性无关路径中从未有过的边的路径。程序的环路复杂度等于线性无关路径的条数，所以本题中应该有 11 条线性无关路径。

试题二（共 15 分）

阅读下列说明，回答问题 1 至问题 3，将解答填入答题纸的对应栏内。

【说明】

某商店为购买不同数量商品的顾客报出不同的价格，其报价规则如表 2-1 所示。

表 2-1 不同数量商品对应的的单价

购买数量	单价(单位:元)
头 10 件(第 1 件到第 10 件)	30
第二个 10 件(第 11 件到第 20 件)	27
第三个 10 件(第 21 件到第 30 件)	25
超过 30 件	22

如买 11 件需要支付 $10 \times 30 + 1 \times 27 = 327$ 元，买 35 件需要支付 $10 \times 30 + 10 \times 27 + 10 \times 25 + 5 \times 22 = 930$ 元

现在该商家开发一个软件，输入为商品数 $C(1 \leq C \leq 100)$ ，输出为因付的价钱 P 。

【问题 1】

请采用等价类划分法为该软件设计测试用例(不考虑 C 为非整数的情况)。

【参考答案】

序号	输入 C	输出 P
1	0（任意小于 1 的数）	N/A
2	200（任意大于 100 的数）	N/A
3	5（任意大于等于 1 小于等于 10 的数）	150
4	15（任意大于等于 11 小于等于 20 的数）	435
5	25（任意大于等于 21 小于等于 30 的数）	695
6	35（任意大于等于 30 小于等于 100 的数）	930

【试题分析】

本题考查黑盒测试法及应用。

本问题考查黑盒测试用例设计方法之等价类划分法。

等价类划分法是把程序的输入域按规则划分为若干子集，然后从每个子集中选取一具有代表性的数据作为测试用例。本题中规定了 C 的取值范围 ($1 \leq C \leq 100$)，按规则可以划分为一个有效等价类 $\{C | 1 \leq C \leq 100\}$ 和两个无效等价类 $\{C | C < 1\}$ 、 $\{C | C > 100\}$ 。表 2-1 中对 C 取不同值有不同的处理，因此上述有效等价类还可以进一步细分为 4 个等价类 $\{C | 1 \leq C \leq 10\}$ 、 $\{C | 11 \leq C \leq 20\}$ 、 $\{C | 21 \leq C \leq 30\}$ 、 $\{C | 31 \leq C \leq 100\}$ 。这样一共得到 6 个等价类，

包括 4 个有效等价类 $\{C|1 \leq C \leq 10\}$ 、 $\{C|11 \leq C \leq 20\}$ 、 $\{C|21 \leq C \leq 30\}$ $\{C|31 \leq C \leq 100\}$ 和两个无效等价类 $\{C|C < 1\}$ 、 $\{C|C > 100\}$ 。设计用例时从这 6 个等价类中任选一个代表数据即可。

【问题 2】

请采用边界值分析法为该软件设计测试用例 (不考虑健壮性测试, 既不考虑 C 不在 1 到 100 之间或者是非整数的情况)。

【参考答案】

序号	输入 C	输出 P
1	1	30
2	5 (任意大于 1 小于 10 的数)	150
续表		
序号	输入 C	输出 P
3	10	300
4	11	327
5	15 (任意大于 11 小于 20 的数)	435
6	20	570
7	21	595
8	25 (任意大于 21 小于 30 的数)	695
9	30	820
10	31	842
11	35 (任意大于 31 小于 100 的数)	930
12	100	2360

【试题分析】

本问题考查白盒测试用例设计方法之边界值分析法。

边界值分析法作为等价类划分法的一种补充, 是把等价类上的边界取值作为测试用例的一种测试方法。题目中要求不考虑健壮性测试, 也就是说不用考虑无效等价类的边界取值, 剩下 4 个等价类中有 1、10、11、20、21、30、31、100 这 8 个边界值, 然后每个等价类中再取 1 个任意值, 一共得到 12 个边界值的测试用例。

【问题 3】

列举除了等价类划分法和边界值分析法以外的三种常见的黑盒测试用例设计方法。

【参考答案】

错误推测法, 因果图法, 判定表驱动法, 正交试验法, 功能图法。

【试题分析】

本问题考查黑盒测试的基本概念。

黑盒测试方法除了等价类划分法和边界值分析法之外, 还包括错误推测法, 因果图法, 判定表驱动法, 正交试验法, 功能图法等。

试题三（共 20 分）

阅读下列说明，回答问题 1 至问题 4，将解答填入答题纸的对应栏内。

【说明】

某大型披萨加工和销售商为了有效管理披萨的生产和销售情况，欲开发一套基于 Web 的信息系统。其主要功能为销售、生产控制、采购、运送、存储和财务管理等。系统采用 Java EE 平台开发，页面中采用表单实现数据的提交与交互，使用图形（Graphics）以提升展示效果。

【问题 1】

设计两个表单项输入测试用例，以测试 XSS（跨站点脚本）攻击。系统设计时可以采用哪些技术手段防止此类攻击。

【参考答案】

XSS（跨站点脚本攻击）是一种注入式攻击，主要通过恶意脚本进行攻击，任何脚本如 <SCRIPT> 都不该被接受。

- (1) <script> alert(' Wufff! ')</script>
- (2) <b onmouseover=alert(' Wufff!')>click me!

防止的主要手段是对功能符号进行编码（转义）。

【试题分析】

本题考查 Web 应用测试相关知识及应用。Web 应用测试除了类似传统软件系统测试的性能测试、压力测试等之外，还需要测试页面、链接、浏览器、表单和可用性等，由于 Web 应用部署访问的大众化特点，对安全性尤其要重视。

此类题目要求考生阅读题目对现实问题的描述，根据对问题的分析，回答测试有关的问题。本题目说明中除了功能背景之外，给出了几个技术点，即采用 Java EE 平台，页面中采用表单实现数据的提交与交互，使用图形（Graphics）以提升展示效果。

本问题考查 Web 应用安全性测试的 XSS 攻击。

XSS 攻击测试是 Web 应用安全性测试的主要内容之一。

许多 Web 应用系统在某些情况下，接收页面上传的内容，并入新页面，作为新页面的内容。例如，在新闻网用户可以对新闻进行评论，用户可以输入如下带有 HTML 标记的内容：

```
<Script>alert("Hello World!");</Script>
```

在用户提交之后，标记将提交到服务器上，并在有新用户访问新的页面中显示，此时用户所看到的网页中包含以上标记的部分元素可能是：

```
<div>  
  <Script>alert("Hello World!");</Script>  
</div>
```

从用户的角度看，该网页中就出现了弹出窗口提示，显示“Hello World! ”。如下图所示：



即：用户输入的内容已经被浏览器成功执行。再如输入如下内容：

```
<b onmouseover=alert('Hello!')>click me!</b>
```

在用户提交之后，后续再访问时，用户所看到的网页中包含以上标记的部分元素可能是：

```
<div>  
  <b onmouseover=alert('Hello!')>click me!</b>  
</div>
```

即新用户所看到网页中显示“Click me! ”。当用户鼠标移过此文字时，就会弹出窗口（左侧为 Chrome 弹出，右侧为 IE9 直接给出的提示窗口，多次鼠标滑过操作 Chrome 提示窗口多了一行浏览器对阻止这类代码的创建新窗口的选项，firefox 类似）：



而如果这类代码都可以执行，就存在被真正恶意攻击者攻击的可能，而且可能造成各类安全问题。所以网站提交代码中的任何脚本、页面功能符号都不应该被直接接受作为功能符号在后续使用。

本题目说明中采用表单实现数据提交与交互，在提交数据时，对数据的内容中包含的特殊内容要进行测试。在测试用例时，要考虑 HTML 标记符、脚本。所以测试用例的设计主要考虑<script>、等功能符号。在页面上真正需要 HTML 标记的，在接收到服务器端时，先进行转义。

【问题 2】

简述图形测试的主要检查点。

【参考答案】

图形测试的主要检查点如下：

- (1) 颜色饱和度和对比度是否合适；
- (2) 需要突出的链接的颜色是否容易识别；
- (3) 是否正确加载所有的图形。

【试题分析】

本问题考查页面的展示效果方面的测试。

Web 页面展示效果在用户界面友好性方面非常重要，是用户界面测试的主要内容之一。

图形测试主要检查图片大小、颜色饱和度和对比度是否合适、需要突出的链接的颜色是否容易识别、是否正确加载等等。

【问题 3】

简述页面测试的主要方面。

【 参考答案】

页面测试可以从以下几个方面进行：

- (1) 页面的一致性；
- (2) 在每个页面上是否设计友好的用户界面和直观的导航系统；
- (3) 是否考虑多种浏览器的需要；
- (4) 是否建立了页面文件的命名体系；
- (5) 是否充分考虑了合适的页面布局技术，如层叠样式表、表格和帧结构等。

【试题分析】

本问题考查 Web 应用页面测试。

Web 页面测试内容包括：页面一致性、用户友好性、浏览器兼容性、布局合理性、直观的导航等。要关注页面是否一致，每个页面上是否设计友好的用户界面，导航系统是否直观，是否考虑浏览器的兼容性，元素布局是否合理，功能块布局是否合理，页面颜色搭配是否合理，字体大小是否合理等方面。另外，还要考虑页面文件的命名体系是否建立。

【问题 4】

系统实现时，对销售订单的更新所用的 SQL 语句如下：

```
PreparedStatement pstmt = connection.prepareStatement("UPDATE SalesOrder  
SET status = ? WHERE OrderID= ?")
```

然后通过 `setString(...)` 的方式设置参数值后加以执行。

设计测试用例以测试 SQL 注入，并说明该实现是否能防止 SQL 注入。

【参考答案】

设计如下测试：【注：设计类似如下用例即可，其中包含 SQL 功能符号使 SQL 变为不符合设计意图即可】

```
status: 'fulfilled' -- , OrderID: '2014' OR '1' = '1'
```

采用传递参数的形式，Java 的 JDBC 驱动会自动将其按照相应的类型处理，功能符号会进行转义。因此，该 SQL 语句是安全。

【试题分析】

本问题考查 Web 应用安全性方面的 SQL 注入，SQL 注入是 Web 应用安全性测试的重要方面之一。

许多 Web 应用系统采用某种数据库，接收用户从 Web 页面中输入，完成展示相关存储的数据（如检查用户登录信息）、将输入数据存储到数据库（如用户输入表单中数据域并点击提交后，系统将信息存入数据库）等操作。在有些情况下，将用户输入的数据和设计好的 SQL 框架拼接后提交给数据库执行，就可能存在用户输入的数据并非设计的正确格式，就给恶意用户提供了破坏的机会，即 SQL 注入。恶意用户输入不期望的数据，拼接后提交给数据库执行，造成可能使用其他用户身份，查看其他用户的私密信息，还可能修改数据库的结构，甚至是删除应用的数据库表等严重后果。SQL 注入在使用 SSL 的应用中仍然存在，甚至是防火墙也无法防止 SQL 注入。因此，在测试 Web 应用时，需要认真仔细设计测试用例，采用 Web 漏洞扫描工具等进行检查，进行认真严格的测试，以保证不存在 SQL 注入机会。

本系统实现时，对销售订单的更新所用的 SQL 语句如下：

```
PreparedStatement pstmt = connection.prepareStatement("UPDATE SalesOrder  
SET status = ? WHERE OrderID= ?");
```

然后通过 `setString(...)` 的方式设置参数值后加以执行。

在 SQL 语句中采用参数的方式传递前台传递来的值，因为不论是什么值，都会只作为

setString(...)的参数值，不会作为 SQL 语句的其他功能符，所以本 SQL 语句更新订单的方式是防止 SQL 注入的。设计如下测试 SQL 注入的测试用例：

```
status: 'fulfilled' -- , OrderID: '2014' OR '1' = '1'
```

检查执行结果，或者传递给数据库的 SQL 语句，会发现所有用例中的功能字符都会经过特定的转义后作为 status 和 OrderID 的值。和拼接 SQL 的方式不同，采用参数形式传递时，Java 的 JDBC 驱动会自动会将其按照相应的类型处理，功能符号会进行转义。因此，测试用例中的注释--、OR 等都会作为参数的值，不会作为功能符，也就不会改变 SQL 语句本身的功能结构，该 SQL 语句是安全的。

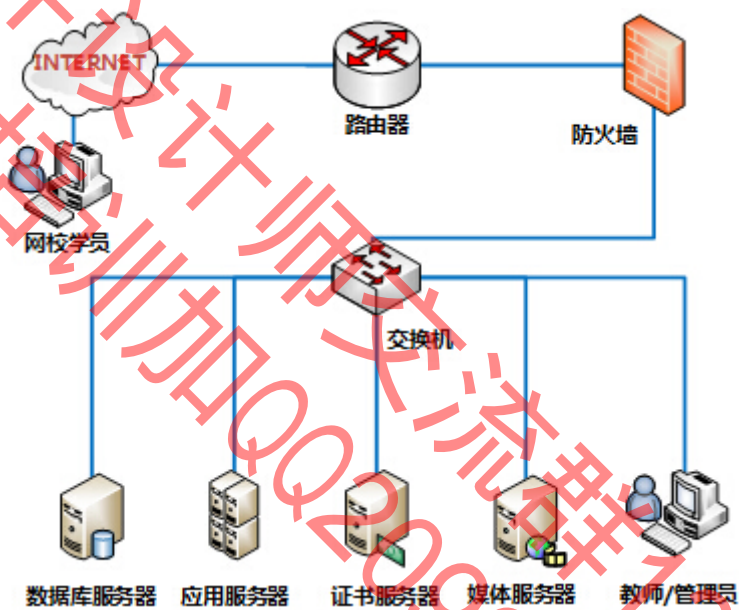
试题四（共 20 分）

阅读下列说明，回答问题 1 至问题 3, 将解答填入答题纸的对应栏内。

【说明】

某大型教育培训机构近期上线了在线网络学校系统，该系统拓扑结构如图 4-1 所示。

企业信息中心目前拟对该系统用户认证机制进行详细的安全性测试，系统注册用户分为网校学员、教师及管理员三类，其中网校学员采用用户名 / 口令机制进行认证，教师及管理员采用基于公钥的认证机制。



【问题 1】

为防止针对网校学员的口令攻击，请从口令的强度、传输存储及管理等方面，说明可采取哪些安全防护措施。相应地，对于网校学员所采用的口令认证机制进行测试时，请说明从用户名称及用户口令两个方面开展测试时应包含哪些基本的测试点。

【参考答案】

(1) 可采取的安全防护措施包括：

①口令强度：可设置最小口令长度，同时可采取要求用户在口令中使用非数字字母的字符等增加口令复杂度的手段提高口令强度。

②口令传输存储：可采用加密或 Hashing 手段，系统服务端存储的用户口令可加密或 Hashing 后存储，网络传输的用户口令可加密或 Hashing 后进行传输。

③口令管理：可设置最大口令时效强制用户定期更新口令，引入口令锁定机制以应对口令猜测攻击，引入口令历史强制用户设置新口令等。

(2) 对口令认证机制测试应包含的基本测试点：

①对用户名称测试的主要测试点在于测试用户名称的唯一性，即测试同时存在的用户名称在不考虑大小写的情况下，不能够同名。

②对用户口令测试应主要测试用户口令是否满足当前流行的控制模式。主要测试点应包括最大/最小口令时效、口令历史、最小口令长度、口令复杂度、加密选项及口令锁定等。

【试题分析】

软件系统的安全性是信息安全的一个重要组成部分，针对程序和数据的安全性测试与评估是软件安全性测试的重要内容，本题考查软件安全性测试的相关知识。

本问题考查考生对基于口令的用户认证机制相关安全测试内容的了解。

基于口令的认证是最简单的用户认证方式，口令具有共享秘密的属性，该方式也容易受到相应的口令攻击。为防范口令攻击，通常可以从口令的强度、传输存储及管理等方面采取相应的安全防护措施，具体措施可包括设置最小口令长度，同时可采取要求用户在口令中使用非数字字母的字符等增加口令复杂度的手段提高口令强度；采用加密或 Hashing 手段，系统服务端存储的用户口令可加密或 Hashing 后存储，网络传输的用户口令可加密或 Hashing 后进行传输；设置最大口令时效强制用户定期更新口令，引入口令锁定机制以应对口令猜测攻击，引入口令历史强制用户设置新口令等。

对用户名称测试的主要测试点在于测试用户名称的唯一性，即测试同时存在的用户名称在不考虑大小写的情况下，不能够同名。对用户口令测试应主要测试用户口令是否满足当前流行的控制模式，主要测试点应包括最大/最小口令时效、口令历史、最小口令长度、口令复杂度、加密选项及口令锁定等。

【问题 2】

为提高系统认证环节安全性，系统在网校教师及管理员登录认证时引入了 USB Key，请说明对公钥认证客户端进行安全测试时，USB Key 的功能与性能测试应包含哪些基本的测试点。

【参考答案】

客户端 USB Key 测试的基本测试点：

(1) 功能测试

①是否支持 AES、RSA 等常用加解密算法。

②是否提供外部接口以支持用户证书及私钥的导入。

- ③是否提供外部接口支持将数据传入 Key 内，经过公钥/私钥计算后导出。
- ④是否能实现 USB Key 插入状态实时监测，当 USB Key 意外拔出时是否能自动锁定用户状态。
- ⑤是否使用口令进行保护。

(2) 性能测试

- ①是否具备私钥不能导出的基本安全特性。
- ②Key 内加解密算法的执行效率是否满足系统最低要求。

【试题分析】

本问题考查考生对 USB Key 安全测试内容的理解。

USB Key 内置单片机或智能卡芯片有一定的存储空间，可以存储用户的私钥以及数字证书，利用 USB Key 内置的加密算法可以实现对用户身份的认证。由于用户私钥通常保存在密码锁中，理论上无法读取，因此可保证用户认证的安全性。

针对 USB Key 的测试通常包括功能与性能测试两个方面。功能测试的基本测试点包括是否支持 AES、RSA 等常用加解密算法；是否提供外部接口以支持用户证书及私钥的导入；是否提供外部接口支持将数据传入 Key 内，经过公钥/私钥计算后导出；是否能实现 USB Key 插入状态实时监测，当 USB Key 意外拔出时是否能自动锁定用户状态；是否使用口令进行保护等。性能测试的基本测试点包括是否具备私钥不能导出的基本安全特性；Key 内加解密算法的执行效率是否满足系统最低要求等。

【问题 3】

系统证书服务器主要提供证书审核注册管理及证书认证两项功能，根据系统实际情况，目前只设置人员证书，请说明针对证书服务器的功能与性能测试应包含哪些基本的测试点。

【参考答案】

证书服务器测试的基本测试点：

(1) 功能测试

- ①系统是否提供证书的申请、审核、签发与管理功能。
- ②系统是否提供证书撤销列表的发布和管理等功能。
- ③系统是否提供证书认证策略及操作管理策略、自身证书安全管理等管理服务。
- ④是否可以提供加密证书和签名证书。
- ⑤证书格式是否采用标准 X. 509 格式。

(2) 性能测试

- ①检查证书服务器的处理性能是否具备可伸缩配置及扩展能力。
- ②关键部分是否采用双机热备和磁盘镜像等安全机制。
- ③是否满足系统的不间断运行、在线故障恢复和在线系统升级的需要。
- ④是否满足需求中预测的最大数量用户正常访问需求，且是否具备 3~4 倍冗余，并需要测试证书服务器的并发处理能力。

【试题分析】

本问题考查证书服务器安全测试内容的相关知识。

按题目描述，系统证书服务器主要提供证书审核注册管理及证书认证两项功能，因此针对证书服务器的安全测试也应主要涵盖这两项主要功能的相应测试。

功能测试的基本测试点包括系统是否提供证书的申请、审核、签发与管理功能；系统是否提供证书撤销列表的发布和管理等功能；系统是否提供证书认证策略及操作管理策略、自身证书安全管理等管理服务；是否可以提供加密证书和签名证书；证书格式是否采用标准 X.509 格式等。性能测试的基本测试点包括检查证书服务器的处理性能是否具备可伸缩配置及扩展能力，关键部分是否采用双机热备和磁盘镜像等安全机制；是否满足系统的不间断运行、在线故障恢复和在线系统升级的需要；是否满足需求中预测的最大数量用户正常访问需求；且是否具备 3~4 倍冗余，并需要测试证书服务器的并发处理能力等。

试题五（共 20 分）

阅读下列说明，回答问题 1 至问题 4, 将解答填入答题纸的对应栏内。

【说明】

某嵌入式刹车控制软件，应用于汽车刹车控制器，该软件需求如下：

1. 模式选择：采集模式控制离散量信号 In-D1 并通过模式识别信号灯显示软件当前工作模式。在信号 In-D1 为低电平时进入正常工作模式（模式识别信号灯为绿色），为高电平时进入维护模式（模式识别信号灯为红色）。软件在正常工作模式下仅进行刹车控制和记录刹车次数，在维护模式下仅进行中央控制器指令响应。

2. 刹车控制：采用定时中断机制，以 5ms 为周期采集来自驻车器发出的模拟量信号 In-A1 以及来自刹车踏板发出的模拟量信号 In-A2，并向刹车执行组件发送模拟量信号 Out-A1 进行刹车控制。

模拟量信号说明：1) In-A1、In-A2 以及 Out-A1 信号范围均为[0.0V, 10.0V]，信号精度均为 0.1V;2) Out-A1 信号的计算方法为： $Out-A1 = In-A1 + 0.3 * In-A2$ ，在计算完成后需要在满足信号精度的要求下进行四舍五入及限幅处理。

3. 记录刹车次数：在 Out-A1 大于 4V 时，读出非易失存储器 NVRAM 中保存的刹车次数记录进行加 1 操作，然后保存至非易失存储器 NVRAM 中。

4. 响应中央控制器指令：接收来自中央控制器的串行口指令字 In-S1，回送串行口响应字 Out-S1。当接收的指令字错误时，软件直接丢弃该命令字，不进行任何响应。

指令字及响应字说明如表 5-1 所示。

表 5-1 指令字和相应字

序号	指令	指令字 In_S1				响应字 Out_S1 格式				
1	读取刹车次数指令	帧头	指令码	帧长	帧尾	帧头	响应码	帧长	数据	帧尾
		0x5A	0x01	0x04	0xA5	0x5A	0x01	0x06	刹车次数 (2 字节)	0xA5
2	清除刹车次数指令	帧头	指令码	帧长	帧尾	帧头	响应码	帧长	数据	帧尾
		0x5A	0x02	0x04	0xA5	0x5A	0x02	0x06	0x0000	0xA5

【问题 1】

在不考虑测量误差的情况下，根据所设计的输入填写表 5-2 中的空(1)～(4)。

表 5.2

序号	输入		输出 Out -A1
	In -A1	In -A2	预期结果
1	0.0V	0.0V	0.0V
2	3.0V	5.2V	(1)
3
4	5.3V	6.8V	(2)
5	6.9V	10.0V	9.9V
6	7.0V	10.0V	10.0v
7	7.1V	10.0V	(3)
8	10.0	10.0V	(4)

【参考答案】

(1) 4.6V (2) 7.3V (3) 10.0V (4) 10.0V

【试题分析】

本题考查软件测试的一些基本概念及依据需求进行测试用例设计的能力。

此题目要求考生认真阅读题目所给的软件需求描述的软件工作过程及通信协议，了解刹车控制软件的工作流程，结合软件测试的一些基本概念，在刹车控制软件中进行实际应用。此问题主要考查对题目描述需求的阅读理解能力，主要对需求中模拟量信号说明部分进行理解正确，即“模拟量信号说明：1) In_A1、In_A2 以及 Out_A1 信号范围均为 [0.0V, 10.0V]，信号精度均为 0.1V；2) Out_A1 信号的计算方法为： $Out_A1 = In_A1 + 0.3 \times in_A2$ ，在计算完成后需要在满足信号精度的要求下进行四舍五入及限幅处理。”

本题中空 (1) 处直接使用公式计算即可；根据公式计算空 (2) 处为 7.34，而根据需求精度为 0.1，所以需要四舍五入为 7.3；根据公式计算空 (3) 处为 10.1，满足精度要求，但是需要限幅为 10；根据公式计算空 (4) 处为 13，需要限幅为 10。

【问题 2】

请简述本软件串行输入接口测试的测试策略及测试内容。针对表 5-1 中“读取刹车次数指令”进行鲁棒性测试时应考虑哪些情况？

【参考答案】

测试策略包括测试正常和异常指令的响应。

测试内容包括读取刹车次数和清除刹车次数两种指令。

对“读取刹车次数指令”鲁棒性测试时应考虑输入接口帧头错误、指令码错误、帧长错误、帧尾错误以及整个指令长度超过 4B 的情况。

【试题分析】

本问题主要考查测试的基本概念及应用。对所有的测试而言，都必须进行正常测试和异常测试，在本题中对测试对象实例化为串行输入接口。串行输入接口在本题的需求描述中，根据表 5-1 内容，负责接收读取刹车次数和清除刹车次数两种指令，故测试内容为此两种指令。对“读取刹车次数指令”进行鲁棒性测试时应考虑的情况，其实也是接口鲁棒性测试概念的一个实例化，对接口数据包而言，至少应该包括帧头错误、数据长度错误、数据错误、校验和错误、校验码错误、帧尾错误以及其他防止指令错误手段的错误等。对本题的实例化而言，具体包括帧头错误、指令码错误、帧长错误、帧尾错误以及整个指令长度超过 4 字节的情况。

【问题 3】

某测试人员设计了如表 5-3 所示的操作步骤，对模式选择功能进行测试（表中 END 表示用例到此结束）。

表 5-3

前提条件	上电前置 In-D1 为低电平，给测试环境上电后，模式识别信号灯为绿色	
序号	In-D1 输入	模式识别信号灯预期输出
1	高电平	红色
2	低电平	绿色
3	高电平	红色
4	END	
5		

为进一步提高刹车控制软件的安全性，在需求中增加了设计约束：软件在单次运行过程中，若进入正常工作模式，则不得再进入维护模式。请参照表 5-3 的测试用例完成表 5-4，用于测试该设计约束。

表 5-4

前提条件		
序号	In-D1 输入	模式识别信号灯预期输出
1		
2		
3		
4		

【参考答案】

前提条件	上电前置 In_D1 为高电平，给测试环境上电，模式识别信号灯为红色	
顺序号	In_D1 输入	模式识别信号灯预期输出
1	低电平	绿色
2	高电平	绿色
3	END	
4		
5		

【试题分析】

本问题中如果不考虑约束，软件工作状态从组合的角度来说，表 5-2 的测试顺序完全符合要求。但是许多软件在实际使用中，由于真实情况的限制，不能从理论的情况进行组合，对一些条件必须要进行约束。比如本题中，在单次进入正常工作模式后，就不能进入维护模式，因为维护模式是一种检修模式，不能再正常工作中，进行检修，所以必须保证在正常工作模式下，对维护模式命令不响应。所以此题的前提条件应该为“上电前置 In_D1 为高电平，给测试环境上电，模式识别信号灯为红色”，即在上电后首先让工作模式为维护模式；然后再发送进入正常工作模式命令，灯变绿，进入工作模式；最后在正常工作模式下，发送进入维护模式命令，此时软件应该不响应，灯继续为绿色，表示在工作模式，完成带约束条件的状态转换测试。如果此题继续表 3-2 的测试前提条件，不管发送什么命令，灯一直不会变化，就无法判断是软件问题还是测试设备问题，无法完成测试。

【问题 4】

本项目在开发过程中通过测试发现了 17 个错误，后期独立测试发现了 31 个软件错误，在实际使用中用户反馈了 2 个错误。请计算缺陷探测率 (DDP)。

【参考答案】

$$DDP = (17+31)/(17+31+2) = 96\%$$

【试题分析】

本问题是一个简单的测试概念，缺陷探测率 (DDP) = 测试发现的软件问题 / 软件总的发现问题。对本题而言，缺陷探测率 (DDP) = $(17+31)/(17+31+2) = 96\%$ 。