【答案】C

【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：

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；适应性维护，是指使应用软件适应新技术变化和管理需求变化而进行的修改；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；

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。

根据题干和四种维护类型的定义，很容易判断该处理属于完善性维护。

软件测试的对象包括（50）。

①需求规格说明

②概要设计文档

③软件测试报告

④软件代码

⑤用户手册

⑥软件开发人员

(50)A.①②③④⑤⑥　　B.①②③④⑤　　C.①②④　　D.①②③④

【答案】B

【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。所以软件测试并不仅仅是程序测试，还应包括相应文档和数据的测试。

本题中①②③⑤都属于文档，而⑥不属于程序、文档、数据中任一种，因此应该选择选项B。

以下不属于系统测试的是（51）。

①单元测试

②集成测试

③安全性测试

④可靠性测试

⑤确认测试

⑥验证测试

(51)A.①②③④⑤⑥　　B.①②③④　　C.①②⑤⑥　　D.①②④⑤⑥

【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、确认测试、验收测试等阶段。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、可靠性测试都属于系统测试的范畴。

本题中只有选项 C 符合上述描述。

以下关于软件测试原则叙述中，不正确是的（52）。

(52)A.测试阶段在实现阶段之后，因此实现完成后再开始进行测试

B.测试用例需要完善和修订

C.发现错误越来的地方应该进行更多的测试

D.测试用例本身也需要测试

【答案】A

【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，测试贯穿于全部软件生命周期，而不仅仅是实现之后的一个阶段。

一条 BUG 记录应该包括（53）。

①编号

②bug 描述

③bug 级别

④bug 所属模块

⑤发现人

(53)A.①②　　B.①②③　　C.①②③④　　D.①②③④⑤

【答案】D

【解析】本题考查 Bug 记录的基本知识。

根据定义，一条完整的 Bug 记录应包括编号、详细描述、级别、所属模块、状态、发现人等信息。

根据上述描述，应选择选项 D。

（54）不属于使用软件测试工具的目的。

(54)A.帮助测试寻找问题　　B.协助问题的诊断

C.节省测试时间　　D.替代手工测试

【答案】D

【解析】本题考查使用测试工具的目的。

软件测试工具是通过一些自动化的手段将问题更容易更快速地暴露出来，这样能使 测试人员更好地找出软件错误的所在，因此其主要作用就是帮助寻找问题、协助诊断以节省测试时间，提高测试效率。软件测试工具本身不具备智能，无法替代手工测试。

以下关于验收测试的叙述中，不正确的是（55）。

(55)A.验收测试由开发方主导，用户参与

B.验收测试也需要制定测试计划

C.验收测试之前需要先明确验收方法

D.验收测试需要给出验收通过或者不通过结论

【答案】A

【解析】本题考查验收测试的基本概念。

验收测试主要是确认软件的功能、性能及其他特性是否满足软件需求规格说明书中列出的需求，是否符合软件开发商与用户签订的合同的要求。验收测试由用户主导，开发方参与。软件验收测试尽可能在现场进行实际运行测试，如果受条件限制，也可以在模拟环境中进行测试，无论何种测试方式，都必须事先明确验收方法，制定测试计划规定要做的测试种类，并制定相应的测试步骤和具体的测试用例。测试完成后要明确给出验收通过或者不通过的结论。根据上述描述，应选择选项 A。

以下关于黑盒测试的测试方法选择的叙述中，不正确的是（56）。

(56)A.在任何情况下都要采用边边界值分析法

B.必要时有等价类划分法补充测试用例

C.可以用错误推测法追加测试用例

D.如果输入条件之前不存在组合情况，则采用因果图法

【答案】D

【解析】本题考查黑盒测试中测试方法的选择。

常见的黑盒测试方法包括等价类划分法、边界值分析法、因果图法、决策表法以及错误推测法等。开发中最容易在边界取值上犯错，因此任何情况下都要采用边界值分析法进行测试，必要的时候采用等价类划分法补充用例，可以根据经验用错误推测法追加一些用例，如果输入条件之间存在组合，则应该采用因果图法。根据上述描述，选项 D 的叙述是错误的。

以下关于等价划分法的叙述中不正确的是（57）。

(57)A.如果规定输入值 string1 必须是‘\0’结束，那么得到两个等价类，即有效等价类{string1|string1 以‘\0’结束}，无效等价类{string1|string1 不以‘\0‘结束}

B.如果规定输入值 int1 取值为 1、-1 两个数之一，那么得到 3 个等价类，即有效等价类{int1|int1=1}、{int1|int1=-1}，无效等价类{int1|int1≠1 并且 int1≠-1}

C.如果规定输入值 int2 取值范围为-10~9，那么得到两个等价类，即有效等价类{int2|-10<=int2<=9}，无效等价类{int2|int2<-10 或者 int2>9}

D.如果规定输入值 int3 为质数，那么得到两个等价类，即有效等价类{int3|int3 是质数}，无效等价类{int3|int3 不是质数}

【答案】C

【解析】本题考查黑盒测试方法中的等价类划分法。

在等价类划分法中，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，则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)；如果规定了输入数据取值范围或值的个数，可以确定一个有效等价类和两个无效等价类；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 C 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{int2|-10<=int2<=9}和两个无效等价类{int2|int2<-10}、{int2|int2>9}。

以下关于白盒测试的叙述中，不正确的是（58）。

(58)A.满足判定覆盖一定满足语名覆盖

B.满足条件覆盖一定满足判定覆盖

C.满足判定条件覆盖一定满足条件覆盖

D.满足条件组合覆盖一定满足判定条件覆盖

【答案】B

【解析】本题考查白盒测试的逻辑覆盖法。

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判定和条件，强度次之，满足判定覆盖或者条件覆盖一定满足语句覆盖;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，满足条件组合覆盖一定同时满足判定条件覆盖、判定覆盖、条件覆盖和语句覆盖。

判定覆盖和条件覆盖之间没有谁强谁弱的关系，满足条件覆盖不一定满足判定覆盖。

对于逻辑表达式((a||(b&c))||(c&&d)),需要(59)个测试用例才能完成条件组合覆盖。

(59)A.4　　B.8　　C.16　　D.32

【答案】C

【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 a、b&c、c、d4 个条件，组合之后需要的用例数是 16，因此选项 C 正确。

为了解系统在何种服务级别下会崩溃，应进行（60）。

(60)A.负载测试　　B.压力测试　　C.大数据量测试　　D.疲劳测试

【答案】B

【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。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在什么情况下崩溃，需要进行压力测试，应选择选项 B。

兼容性测试的测试范围包括（61）。

①硬件兼容性测试

②软件兼容性测试

③数据兼容性测试

④平台兼容性测试

(61)A.①②③④　　B.①②③　　C.①②　　D.①

【答案】A

【解析】本题考查兼容性测试的基本知识。

兼容性测试是测试被测软件在特定的硬件平台上，不同的应用软件之间，不同的操作系统平台上，在不同的网络等环境中能否正常的运行。兼容性测试的目的包括：被测软件在不同的操作系统平台上正常运行，包括能在同一操作系统平台的不同版本上正常运行；被测软件能与相关的其他软件或系统“和平共处”，能方便地共享数据；被测软件能在指定的硬件环境中正常运行；被测软件能在不同的网络环境中正常运行。

根据上述描述，应选择选项 A。

以下不能作为测试结束标准的是（62）。

(62)A.测试超过了预定时间

B.执行完了所有测试用例但没有发现新的故障

C.单位时间内查出的故障数目低于预定值

D.测试人员或者其它资源不足

【答案】D

【解析】本题考查测试停止准则。

常见的测试停止准则包括：测试超过了预定时间；执行了所有的测试用例，没有发现新的故障；采用特定的测试用例设计方案；查出某一预定数目的故障；单位时间内查出故障的数量少于预定值。

测试人员或者其他资源不足属于项目管理的问题，不能作为测试结束标准，因此应选择选项 D。

以下属于静态测试方法的是（63）。

(63)A.代码审查　　B.判定覆盖　　C.路径覆盖　　D.语句覆盖

【答案】A

【解析】本题考查静态测试的基本概念。

根据定义，静态测试是指不需要实际运行被测软件而进行的测试。

根据上述描述，判定覆盖、语句覆盖和路径覆盖都需要执行被测软件，只有代码审查通过阅读代码即可实现，不需要实际执行程序，因此应选择选项 A。

单元测试的测试内容包括（64）。

①模块接口

②局部数据库结构

③模块内路径

④边界条件

⑤错误处理

⑥系统性能

(64)A.①②③④⑤⑥　　B.①②③④⑤　　C.①②③④　　D.①②③

【答案】B

【解析】本题考查单元测试的基本概念。

单元测试是对软件中可测试的最小单元——模块进行检查和验证，其测试内容包括模块接口、局部数据结构、模块内路径、边界条件和错误处理。

单个模块无法反映出整个系统的性能，因此系统性能不属于单元测试的测试内容，应选择选项 B。

一个 Web 信息系统所需要的进行的测试包括（65）。

①功能测试

②性能测试

③可用性测试

④客户端兼容性测试

⑤ 安全性测试

(65)A.①②　　B.①②③　　C.①②③④　　D.①②③④⑤

【答案】D

【解析】本题考查 Web 测试的基本概念。

Web 信息系统也是软件，因此需要进行功能测试、性能测试和可用性测试；Web 系统客户端运行在浏览器上，操作系统和浏览器的差异会引起兼容性问题，需要进行客户端兼容性测试；此外，Web 系统运行在互联网上，容易遭受攻击，需要进行安全测试。

以下不属于网络测试的测试指标的是（66）。

(66)A.吞吐量　　B.延时　　C.并发用户数　　D.丢包率

【答案】C

【解析】本题考查网络测试的基本概念。

网络测试是指针对软件运行的底层网络环境进行的测试，常见的测试指标包括网络可用性、网络带宽、吞吐量、延时、丢包率等。

并发用户数是一个整体的性能指标，它跟软件、平台、硬件配置、网络环境都相关，不属于网络测试的指标。

对于其于用户口令的用户认证机制来说，（67）不属于增强系统安全性应使用的防范措施。

(67)A.对本地存储的口令进行加密

B.在用户输入的非法口令达到规定的次数之后，禁用相应账户

C.建议用户使用英文单词或姓名等容易记忆的口令

D.对于关键领域或安全性要求较高的系统 ，应该当保证用过的用户删除或停用后，保留该用户记录，且新用户不能与该用户名

【答案】C

【解析】本题考查用户认证机制的安全防范措施。

基于用户名/口令的用户认证机制是最基本的认证机制，相应增强系统安全性的防范措施包括设置口令时效、增加口令复杂度、口令加密存储、口令锁定、保证用户名称的唯一性等，题目候选项中，候选答案A、B及D属于典型的安全防范措施，而候选答案C的方法则会降低口令的复杂度，从而使得系统更易受到口令猜测攻击，不属于增强系统安全性所应采取的措施。

对于防病毒系统的测试是系统安全测试的重要内容，下列不属于防病毒系统安全测试基本测试点的是（68）。

(68)A.能否提供对病毒特征与检测引擎的定期在线更新服务

B.能否在不更新特征库的前提下对新的未知病毒进行有效查杀

C.能否支持多种平台的病毒防范

D.能否支持对电子邮件附件的病毒防治

【答案】B

【解析】本题考查防病毒系统安全测试的基本测试点。

对于防病毒系统的测试是系统安全测试的重要内容，其测试的基本测试点包括能否支持多种平台的病毒防范、能否支持对服务器的病毒防治、能否支持对电子邮件附件的病毒防治、能否提供对病毒特征库与检测引擎的定期在线更新服务、防病毒范围是否广泛等，而基于病毒特征库对已知病毒进行查杀是防病毒系统准确查杀病毒的主要手段。

综上不难看出，候选答案B不是防病毒系统安全测试的基本测试点。

1976年Diffie与Hellman首次公开提出（69）的概念与结构，采用两个从此独立的密

钥对数据分别行行加密或解密，且加密过程基于数学函数，从而带来了加密领域的革命性进步。

(69)A.公钥加密　　B.对称加密　　C.单向 Hash 函数　　D.RSA 加密

【答案】A

【解析】本题考查公钥加密的基础知识。

与对称加密使用同一密钥对数据进行加密与解密不同，公钥加密采用两个独立的密钥对数据分别进行加密与解密，且加密过程是基于数学函数的。公钥加密较好地解决了加密机制中密钥的发布和管理问题，从而带来了加密领域的革命性进步。公钥加密的概念与结构是1976 年由 Diffie 与 Heilman 首次公开提出的。

综上不难看出，应选择候选答案 A。

集线器与网桥的区别是（70）。

(70)A.集线器不能检测发生冲突，而网桥可以检测冲突

B.集线器是物理层设备，而网桥是数据链路层设备

C.网桥只有两个端口，而集线器是一种多端口网桥

D.网桥是物理层设备，而集线器是数据链路层设备

【答案】B

【解析】

集线器是物理层设备，相当于在 10BASE2 局域网中把连接工作站的同轴电缆收拢在一个盒子里，这个盒子只起到接收和发送的功能，可以检测发送冲突，但不能识别数据链路层的帧。网桥是数据链路层设备，它可以识别数据链路层 MAC 地址，有选择地把帧发送到输出端口，网桥也可以有多个端口，如果网桥端口很多，并配置了加快转发的硬件，这就成了局域网交换机了。

In a world where it seems we already have too much to do, and too many things to think about, it seems the last thing we need is something new that we have to learn.

But use cases do solve a problem with requirements: with （71） declarative requirements it's hard to describle steps and sequences of events.

Use cases, stated simply, allow description of sequences of events that, taken

together, lead to a system doing something useful. As simple as this sounds, this is important. When confronted only with a pile of requiements, it's often （72） to make sense of what the authors of the requirements really wanted the system to do.In the preceding example, use cases reduce the ambiguity of the requirements by specifying exactly when and under what conditions certain behavior occurs; as such, the sequence of the behaviors can be regarded as a requirement. Use cases are particularly well suited to capture approaches. Although this may sound simple, the fact is that （73） requirement capture approaches, with their emphasis on declarative requirements and "shall" statements, completely fail to capture fail to capture the （74） of the system's behavior. Use cases are a simple yet powerful way to express the behavior of the system in way that all stakeholders can easily understand.

But, like anything, use cases come with their own problems, and as useful as they are, they can be （75）. The result is something that is as bad, if not worse, that the original problem. Therein it's important to utilize use cases effectively without creating a greater problem than the one you started with.

(71)A.plenty	B.loose	C.extra	D.strict
(72)A.impossible	B.possible	C.sensible	D.practical
(73)A.modern	B.conventional	C.different	D.formal
(74)A.statics	B.nature	C.dynamics	D.originals
(75)A.misapplied	B.applied	C.used	D.powerful

【答案】D　A　B　C　A

【解析】

在这个世界上，似乎我们有太多的事情要去做，有太多的事情要去思考，那么需要做的最后一件事就是必须学习新事物。

而用例恰恰可以解决带有需求的问题：如果具有严格声明的需求，则很难描述事件的步骤和序列。

简单地说，用例可以将事件序列的说明放在一起，引导系统完成有用的任务。正如听起来一样简单——这很重要。在面对很多需求的时候，通常不太可能理解需求的作者真正想要系统做什么。在前面的例子中，通过指定特定行为发生的时间和条件，用例减少了需求的不

确定性。这样的话，行为的顺序就可以当作是一种需求。用例特别适用于捕捉这类需求。尽管听起来可能很简单，但事实情况是由于常规的需求捕捉方法所侧重的是声明需求和“应该怎么样”的陈述，因此完全无法捕捉系统行为的动态方面。用例是一种简单而有效的表达系统行为的方式，使用这种方式所有参与者都很容易理解。

但是与任何事物一样，用例也存在自己的问题——在用例非常有用的同时，人们也可能误用它，结果就产生了比原来更为糟糕的问题。因此重点在于：如何有效地使用用例，而又不会产生出比原来更严重的问题。

试题一

阅读下列 java 程序，回答问题 1 至问题 3，将解答填入答题纸内对应栏内。

【Java 程序】

```
public int addAppTask(Activity activity, Intent intent,
            TaskDescription description, Bitmap thumbnail) {
    Point size = getSize();                                    //1
    final int tw = thumbnail.getWidth();
    final int th = thumbnail.getHeight();
    if (tw != size.x || th != size.y) {                        //2,3
        Bitmap bm = Bitmap.createBitmap(size.x, size.y, thumbnail
       .getConfig());  //4
        float scale;
        float dx = 0, dy = 0;
        if (tw * size.x > size.y * th) {                       //5
            scale = (float) size.x / (float) th;               //6
            dx = (size.y - tw * scale) * 0.5f;
        } else {                                               //7
            scale = (float) size.y / (float) tw;
            dy = (size.x - th * scale) * 0.5f;
        }
        Matrix matrix = new Matrix();
        matrix.setScale(scale, scale);
        matrix.postTranslate((int) (dx + 0.5f), 0);
        Canvas canvas = new Canvas(bm);
        canvas.drawBitmap(thumbnail, matrix, null);
        canvas.setBitmap(null);
        thumbnail = bm;
    }
    if (description == null) {                                 //8
        description = new TaskDescription();                   //9
    }
}                                  //10
```

【问题 1】

请简述基本路径测试法的概念。

基本路径测试法是在程序控制流图的基础上，通过分析控制构造的环路复杂性，导出基本可执行路径集合，从而设计测试用例的方法。

本题考查白盒测试法的应用。

本问题考查白盒测试用例设计方法中的基本路径测试法。

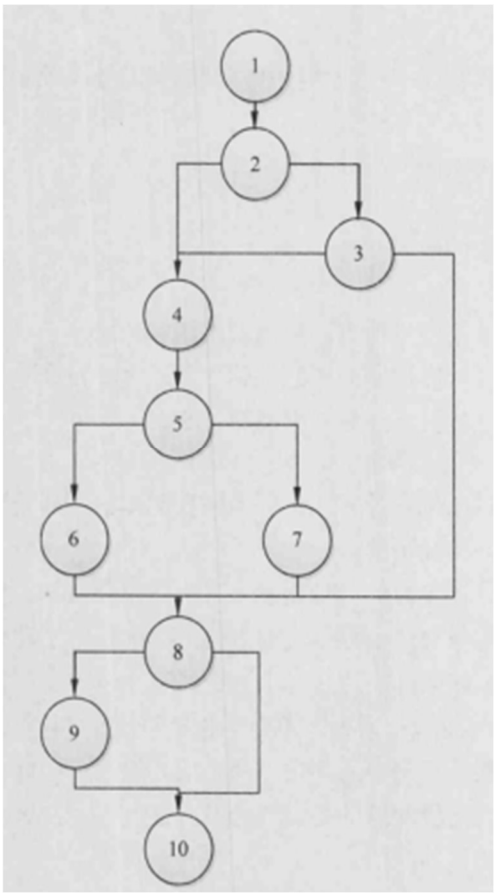
基本路径测试法是在程序控制流图的基础上，通过分析控制构造的环路复杂性，导出基本可

执行路径集合，从而设计测试用例的方法。

【问题 2】

请画出上述程序的控制流图，并计算其控制流图的环图复杂度 V(G)。

控制流图



环路复杂度 V(G)=5

本问题考查白盒测试用例设计方法：基本路径测试法。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的判断。本题程序中，if(tw!=size.x||th!=size.y)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。需要注意的是，复合条件之间是“&&”的关系还是“||”的关系反应在控制流图的画法是不同的。

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 4，所以 V(G)=5。

【问题 3】

请给出问题 2 中的控制流图的线性无关路径。

线性无关路径：

1. 1-2-4-5-6-8-9-10
2. 1-2-4-5-7-8-9-10(1-2-4-5-7-8-10)
3. 1-2-4-5-6-8-10(1-2-4-5-7-8-10)
4. 1-2-3-4-5-6-8-9-10(1-2-3-4-5-7-8-9-10，1-2-3-4-5-6-8-10，1-2-3-4-5-7-8-10)
5. 1-2-3-8-9-10(1-2-3-8-10)

本问题考查白盒测试用例设计方法：基本路径法。涉及到的知识点包括：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 5 条线性无关路径。

试题二

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】

某商店的货品价格（P）都不大于 20 元（且为整数），假设顾客每次付款为 20 元且每次限购一件商品，现有一个软件能在每位顾客购物后给出找零钱的最佳组合（找给顾客货币张数最少）。

假定此商店的找零货币面值只包括：10 元（N10）、5 元（N5）、1 元（N1）3 种。

【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 P 为非整数的情况）并填入到下表中。（<<N1,2>>表示 2 张 1 元，若无输出或输出非法，则填入 N/A）

序号	输入（商品价格 P）	输出（找零钱的组合）
1	20 (P = 20)	N/A
2	18（任意 15 < P < 20）	<<N1,2>>
3		
4		
5		
6		
7		
8		
9		
10		

序号	输入（商品价格 P）	输出（找零钱的组合）
1	20 (P = 20)	N/A
2	18（任意 15 < P < 20）	<<N1,2>>
3	15（P = 15）	<<N5,1>>
4	13（任意 10 < P < 15）	<<N5,1>, <N1,2>>
5	10（P = 10）	<<N10,1>>
6	8（任意 5 < P < 10）	<<N10,1>, <N1,2>>
7	5（P = 5）	<<N10,1>,<N5,1>>
8	3（任意 0<P<5）	<<N10,1>, <N5,1>, <N1,2>>
9	-10（任意 P < 1）	N/A
10	30（任意 P > 20）	N/A

本题考查白盒测试法和黑盒测试法的应用。

本问题考查黑盒测试用例设计方法：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个具有代表性的数据作为测试用例。本题中规定了 P 的取值范围(1<=P<=20)，按规则可以划分为一个有效等价类{P|1<=?<=20}和两个无效等价类仄^<1}、{P|P>20}。根据题中描述，对 P 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 8 个等价类{P|P=20}、{P|15<P<20}、{P|P=15}、{P|10<P<15}>{P|P=10}、{P | 5<P<10}、{P|P=5}、{P|0<P<5}„这样一共得到 10 个等价类，包括 8 个有效等价类丨 P|P=20}、{P|15<P<20}、{P|P=15}、{P|10<P<15}、{P|P=10}>{P|5<P<10}、{P|P=5}、{P|0<P<5}和两个无效等价类{P|P<1}、{P|P>20}。设计用例时从这 10 个等价类中各任选一个代表元素即可。

【问题 2】

请采用边界值分析法为该软件设计测试用例。

序号	输入（商品价格 P）	输出（找零钱的组合）
1	20	N/A
2	19	<<N1,1>>
3	18	<<N1,2>>
4	16	<<N1,4>>
5	15	<<N5,1>>
6	14	<<N5,1>, <N1,1>>
7	13	<<N5,1>, <N1,2>>
8	11	<<N5,1>, <N1,4>>
9	10	<<N10,1>>
10	9	<<N10,1>,<N1,1>>
11	8	<<N10,1>,<N1,2>>
12	6	<<N10,1>,<N1,4>>
13	5	<<N10,1>,<N5,1>>
14	4	<<N10,1>,<N5,1>,<N1,1>>
15	3	<<N10,1>,<N5,1>,<N1,2>>
16	1	<<N10,1>,<N5,1>,<N1,4>>

本问题考查白盒测试用例设计方法：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。如果不考虑健壮性测试，也就是如果说不考虑无效等价类的边界取值，8 个有效等价类中有 20，19，16，15，14，11，10，9，6，5，4，1 这 12 个边界值，然后每个等价类中再取 1 个任意值，一共得到 16 个边界值的测试用例({P|P=20}、{P|P=15}、{P|P=10}、{P|P=5}这 4 个等价类的任意值是 20，15，10，5，与边界值有重复)。

【问题 3】

请给出采用决策表法进行测试用例设计的主要步骤。

(1) 确定规则的个数。

(2) 列出所有的条件桩和动作粧。

(3) 填入条件项和动作项。

(4) 合并相似规则，化简决策表。

本问题考查黑盒测试中决策表法。

采用决策表法设计测试用例分为四步：1)确定规则的个数；2)列出所有的条件桩和动作粧；3)填入条件项和动作项；4)合并相似规则，化简决策表。

试题三

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】

MOOC（慕课）教育平台欲开发一基于 Web 的在线作业批改系统，以实现高效的作业提交与批改并进行统计。系统页面中涉及内部的内容链接、外部参考链接以及邮件链接等。页面中采用表单实现作业题目的打分和评价，其中打分为 1~5 分制整数，评价为文本。

系统要支持：

（1）在特定时期内 300 个用户并发时，主要功能的处理能力至少要达到 16 个请求/秒，平均数据量 16KB/请求。

（2）系统前端采用 HTML 5 实现，以使用户可以通过不同的移动设备的浏览器进行访问。

【问题 1】

针对此在线系统进行链接测试时，需要测试哪些方面？

内部链接测试、外部链接测试、邮件链接测试、断链测试。

本题考查 Web 应用测试相关知识。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、表单和可用性等多个方面，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：系统页面中涉及内部内容的链接、外部参考链接以及邮件链接等。页面中采用表单实现作业题目的打分和评价，其中打分为 1～5 分制整数，评价为文本。

本题考查 Web 应用链接测试的内容。题目中涉及到内部内容的链接、外部参考链接以及邮件链接，所以均需要测试。还要进行断链测试，测试每个链接是否有断链。

【问题 2】

为了达到系统要支持的（2），设计一个兼容性测试矩阵。

浏览器 / 平台	IE(7,8,9,10)	Firefox 12	Google Chrome	Android browser	Safari	……
Windows XP						
Windows(7,8,10)						
Linux						
iOS						
Android						
……						

本题考查 Web 应用兼容性测试的内容。Web 应用的兼容性是测试的重要方面，包括:浏览器兼容性、操作系统平台兼容性、移动浏览、打印选项等。本系统前端采用 HTML5 实现，以使用户可以通过不同的移动设备、操作系统和浏览器进行访问，因此需要针对普通设备和移动设备，进行操作系统平台和浏览器的兼容性测试。包括 Windows 系列、Linux 系列、移动操作系统 iOS、Android，与其上可以使用的浏览器进行结合，构建兼容性二维矩阵，行列分别表示操作系统平台和浏览器。测试时分别在单元格记录操作系统和浏览器组合的测试情况。

【问题 3】

给出计算系统的通信吞吐量的方法，并计算在满足系统要支持的（1）时系统的通信吞吐量。

通信吞吐量：P=N(并发用户的数量=300)×T(每单位时间的在线事务数量=16)×D(事务服务器每次处理的数据负载=16kB/S)

本系统满足条件(1)时的通信吞吐量为：300×16×16=76800kB/S(75MB/S)。

本题考查 Web 应用系统的性能指标计算。通信吞吐量，设定如下指标参数：

N：并发用户的数量 T：每单位时间的在线事务数量 D：事务服务器每次处理的数据负载 P：系统的通信吞吐量有如下计算公式：P=N×T×D

本题中系统要求支持的(1)中给出 300 个用户并发，即 N=300;主要功能的处理能力至少要达到 16 个请求/秒，即 T=16;平均数据量 16kB/请求，即 D=16kB/S。

则可得：通信吞吐量 P=300×16×16=76800kB/S(75MB/S)。

【问题 4】

设计 4 个打分和评价的测试输入，考虑多个方面的测试，如：正确输入、错误输入、

XSS、SQL 注入等测试。

(1) 打分为任何在 1～5 范围内的数字，评价为任意文本；

(2) 打分为任何在 1～5 范围外的数字，评价为任意文本；

(3) 打分和评价其中任一字段包含 HTML 标签，如：<HTML>，<SCRIRT>等；

(4) 打分和评价其中任一字段包含 SQL 功能符号，如包含’OR、2015’ OR ‘1’ = ‘1’ 等。

本题考查 Web 应用测试的输入方面，包括输入的不同情况、安全性方面的 SQL 注入和 XSS 跨站攻击。

打分和评价的测试输入应该考虑分值的取值范围之内和之外以及文本中的内容：

(1) 打分为任何在 1～5 范围内的数字，评论为任意文本；

(2) 打分为任何在 1～5 范围外的数字，评论为任意文本；

输入的内容中输入符号可能会传到后台引起安全问题。

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、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 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，进行认真严格的测试，以保证如果存在 SQL 注入可以及早发现。

本系统测试时，设计测试如为：对打分和评价中任一字段设计包含 SQL 功能符号，如包含 ‘，OR、2015’ OR ‘1’ = ‘1’ 等，检查结果是否造成注入问题。

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，在本系统中进行打分和评论后，学生查看时显示分值和评价的内容。如果用户可以输入如下带有 HTML 标记的内容：

<Script>alert("HelloWorld!");</Script>

在提交之后，标记将提交到服务器上，并在有学生访问新的页面中显示，此时所看到的

网页中包含以上标记的部分元素可能是：

<Script>alert(''HelloWorld!"); 〈/Script〉

从学生的角度看，该网页中就出现了弹出窗口提示，显示 HelloWorld!，如下图所示：

JavaScriptAlert x

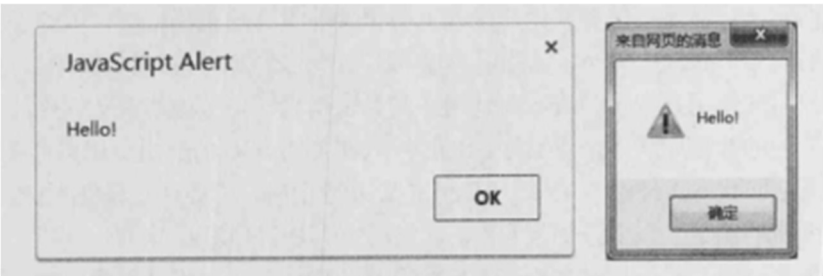
即：用户输入的内容已经被浏览器成功执行。再如输入如下内容:

<bonmouseover=alert('Hello!1)>clickme!

在提交之后，后续学生再访问时，所看到的网页中包含标记的部分元素可能是:

<bonmouseover=alert('Hello!1'>clickme!

即新用户所看到的网页中显示 Clickme!，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以作为功能符号在后续使用。所以测试时需要考虑设计包含 HTML 标记符、脚本等测试输入，如:<HTML>、<script>、等功能符号。

试题四

阅读下列说明，回答问题 1 至 3，将解答填入答题纸的对应栏内。

【说明】

某嵌入系统中，存在 16 路数据采集通道，为了提高数据采集的可靠性，对 16 路采集频道均采用双余度设计;为了监控采集通道是否发生故障,对各路双度通道采集值进行了比较。只有当通道两个度设备采集值不小于 45 时，才表示该路通道正常。设计人员设计函数 mun_of_passer 用于统计无故障通道数目，在改函数的设计中考虑了如下以因素：

（1）采用如下数据库结构存储通道号及采集值：

```
struct Value
    {  unsigned int    No;          //通道号，1到16
       unsigned short  Value1;      //余度1采集值
       unsigned short  Value2;      //余度2采集值
    }
```

（2）当输入参数异常时，函数返回-1；

（3）若正确统计了无故障通道数目，则返回该数目；

（4）该函数需要两个输入参数，第一个参数是用于存储通道号及余度采集值的数组，第二个参数为通道总数目；

（5）调用函数 sort()对存储通道号及余度采集值得的数组进行排序处理。

开发人员根据上述要求使用 ANSI C 对代码实现如下，（代码中每行第一个数字代表行号）：

```
1   unsigned int num_of_passer(struct Value array[], unsigned int num)
2   {
3       unsigned int n = 0;              //循环变量
4       unsigned int counter;            //无故障通道数目
5       if((array == NULL)||(num == 0)||(num > 16))
6           return -1;                   //当输入参数异常时，函数返回-1
7       sort(array);                     //对存储值的数组进行排序处理
8       for(n = 0;n <= num;n++)
9       {
10          if((array[n].Value1 > 45) && (array[n].Value2 > 45))
11              counter = counter + 1;
12      }
13      return counter;
14  }
```

【问题 1】

嵌入或软件中通常使用函数扇出数的注释来衡量程序的可维护性，请计算

num_of_passer 的扇出数和注释率，并判断此函数扇出数和注释率是否符合嵌入式软件的一般要求。

扇出数：1

注释率：28.6%(4/14)

嵌入式软件一般要求扇出数不大于 7 和注释率不小于 20%，所以此函数扇出数和注释率均符合要求。

本题考查软件测试的一些基本概念和通过代码审查查找软件缺陷以及设计测试用例的能力。

此题目要求考生认真阅读题目所给的软件设计说明信息和软件代码，熟悉结构体数据类型和不同代码覆盖率的要求，结合软件测试的一些基本概念，在此嵌入式软件中进行实际应用。

扇出数指在结构图中，模块所属的直接下级模块个数，即本模块所调用的模块数目。模块 num_of_passer 中仅调用了排序模块 sort，所以模块 num_of_passer 的扇出数为 1。注释率指代码中注释的行数与代码总行数的比率，即注释行数/代码总行数×100%所得的结果。模块 num_of_passer 的注释率为 4/14×100%=28.6%。为了保证软件的可维护性，嵌入式软件的相关标准中一般要求模块的扇出应控制在 7 以下，注释的行数不得少于源程序总行数的 1/5。模块 num_of_passer 的扇出数为 1，注释率为 28.6%，均满足嵌入式软件的一般要求。

【问题 2】(8 分)

请使用代码审查的方法找出该程序中所包含的至少四处错误，批出错误的行号和问题描述。

序号	错误所在行号	错误描述
1		
2		
3		
4		

序号	错误所在行号	错误描述	
1	第 1 行	函数返回值类型错误，应为 int 型	
2	第 4 行	变量 counter 未初始化导致函数返回结果可能出错，应初始化为 0	
3	第 5 行	使用“>”导致数组越界，改为“>=”	只能修改第 5 行或第 8 行中一处
	第 8 行	使用“<=”导致数组越界，应改为“<”	
4	第 10 行	判断条件错误，应将两处“>”都更改为“>=”	

代码审查是不执行软件代码，而通过阅读软件代码发现代码可能存在的错误的过程。代码审查的测试内容包括检查代码和设计的一致性；检查代码执行标准的情况；检查代码逻辑表达的正确性；检查代码结构的合理性；检查代码的可读性。通过对说明的阅读，按照说明中描述的要求进行模块 num_of_passer 的代码审查。

阅读第 1 行代码，函数返回值定义为 unsignedint；而在说明的第(2)条描述了当输入参数异常时，函数返回-1;这样发现说明和代码不一致，显然代码定义的 unsignedim 不能返回-1，此为第 1 处错误。修改函数返回值的定义为 int 类型即可。

阅读第 4 行代码，定义了无故障通道数目 counter，在定义时未进行初始化，并且在 11 行使用前依然未初始化。这就导致 counter 的初值为非确定值，可能出错，此为第 2 处错误。在第 4 行定义 counter 时初始化为 0 或者在使用前进行初始化为 0 均可。

第 5 行代码对模块输入参数进行合法性检查，num 合法值为 1 至 16;然后查找使用 num 之处，在第 8 行对 num 进行了使用，但第 8 行使用时却从 0 开始，而且是小于等丁-num，这就意味着如果第 5 行 num 值为最大值 16，在第 8 行就需要循环判断 17 次(0 到 16)，而本题的说明中描述很清楚，最多就 16 路通道，此为第 3 处错误。但此问题的更改有两种方案，方案 1 可以更改第 5 行 num>16 为 num>=16，缩小此参数的合法范围；方案 2 可以更改第 8 行 n<=num 为 n<num 减少循环次数。

阅读第 10 行代码，对每个通道采集的双余度值进行有效性判断。按照说明，当余度设备采集值均不小于 45 时，才表示该路通道正常；但代码中使用当余度设备采集值均大于 45 时，表示该路通道正常，在对边界点 45 的处理上与说明不一致，此为第 4 处错误。将第 10 行代码中的两个“>”符号修改为“>=”即可与说明一致。

【问题 3】(6 分)

覆盖率是度量测试完整性的一个手段，也是度量测试有效性的一个手段。在嵌入式软件的白盒测试过程中，通常以语句覆盖率、分支覆盖率和 MC/DC 覆盖率作为度量指标，请分别指出对函数 num_of_passer 达到 100%语句覆盖、100%分支覆盖和 100%MC/DC 覆盖所需的最少测试用例数目。

覆盖率类型	所需的最少用例数
100%语句覆盖	
100%分支覆盖	
100%MC/DC 覆盖	

覆盖率类型	所需的最少用例数
100%语句覆盖	2
100%分支（DC）覆盖	2
100%MC/DC 覆盖	4

覆盖率是度量测试完整性的一个手段，也是度量测试有效性的一个手段。在嵌入式软件白盒测试过程中，通常以语句覆盖率、分支覆盖率和 MC/DC 覆盖 f 作为度量指标。语句覆盖率指程序中每条可执行语句至少被执行一次。分支覆盖指程序中每个判定取所有可能值至少一次。MC/DC 覆盖率指在一个程序中每一种输入输出至少应出现一次，在程序中的每一个条件必须产生所有可能的输出结果至少一次，并且每个判定中的每个条件必须能够独立影响一个判定的输出，即在其他条件不变的前提下仅改变这个条件的值，而使判定结果改变。

对模块 num_of_passer 来说，为了使其中所有的语句至少执行一次，程序中的两种返回值必须各覆盖一次，所以为达到 100%语句覆盖率，至少需要两个测试用例，即参数异常的测试用例和参数正常的测试用例。

模块 num_of_paSSer 在第 5 行和第 10 行有两处条件判断，为了使程序中每个判定取所有可能值至少一次，第 5 行需要取 TRUE 和 FALSE，第 10 行需要取 TRUE 和 FALSE。由于第 5 行取 FALSE 时，就能覆盖到第 10 行判定，同时又由于第 10 行的判定在一个大于一次的循环中，一个测试用例就可以覆盖到第 10 行的 TRUE 和 FALSE，所以模块 num_of_passer100%的分支覆盖也最少两个测试用例就可以满足，即一个第 5 行取 TRUE 的测试用例和一个第 5 行取 FALSE、第 10 行取 TRUE 和 FALSE 的测试用例即可，由于第 10 行的条件判断在多次循环中，取 TRUE 和 FALSE 的测试用例也比较好构造。

模块 num_of_passer 的组合条件也出现在第 5 行和第 10 行。对第 5 行的组合条件需要 4 个测试用例来满足 MC/DC 覆盖，分别为①参数 array 为 NULL，②array 不为 NULL 且 num 为 0，③array 不为 NULL 且 num 为大于 16 的值，④array 不为 NULL 且 num 为 1 到 16 之间的值。对第 10 行的组合条件需要 3 个测试用例来满足 MC/DC 覆盖，分别为①Value1>45 且 Value12>45，②Value1>45 且 Value2<=45，③Value1<=45 且 Value2 为任意值。由于取第 5 行 array 不为 NULL 且 num 为 1 到 16 之间值的测试用例时，程序将执行到第 10 行，这时由于第 10 行在一个多次循环中，第 10 行需要的 3 个测试用例都可以在此用例中进行覆盖，所

以最少需要 4 个测试用例就可以使模块 num_of_passer 满足 100%的 MC/DC 覆盖。

试题五

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】

某互联网企业开发了一个大型电子商务平台，平台主要功能是支持注册卖家与买家的在线交易。在线交易的安全性是保证平台上正常运行的重要因素，安全中心是平台上提供安全保护措施的核心系统，该系统的主要功能包括：

（1）密钥管理功能，包括公钥加密体系中的公钥及私钥生成与管理，会话密的协商、生成、更新及分发等。

（2）基础加解密服务，包括基于 RSA、ECC 及 AES 等多密码算法的期本加解密服务。

（3）认证服务，提供基于 PKI 及用户名/口令的认证机制。

（4）授权服务，为应用提供资源及功能的授权管理和访问控制服务。

现企业测试部门拟对产台的密钥管理与加密服务系统进行安全性测试，以检验平台的安全性。

【问题 1】（4 分）

给出安全中心需应对的常见安全攻击手段并简要说明。

该平台需应对的常见安全攻击手段应包括：

(1) 网络侦听：指在数据通信或数据交互的过程中，攻击者对数据进行截取分析，从而实现对包括用户支付账号及口令数据的非授权获取和使用。

(2) 冒充攻击：攻击者采用口令猜测、消息重演与篡改等方式，伪装成另一个实体，欺骗安全中心的认证及授权服务，从而登录系统，获取对系统的非授权访问。

(3) 拒绝服务攻击：攻击者通过对网络协议的实现缺陷进行故意攻击，或通过野蛮手段耗尽被攻击对象的资源，使电子商务平台中包括安全中心在内的关键服务停止响应甚至崩溃，从而使系统无法提供正常的服务或资源访问。

(4) Web 安全攻击：攻击者通过跨站脚本或 SQL 注入等攻击手段，在电子商务平台系统网页中植入恶意代码或在表单中提交恶意 SQL 命令，从而旁路系统正常访问控制或恶意盗取用户信息。

软件系统的安全性是信息安全的一个重要组成部分，对于在线交易业务来说，安全性更是保证系统正常运行的重要因素，针对安全中心安全保护措施的测试是检验安全中心可用性的主要手段，本题考查对安全保护措施进行安全性测试的相关知识。

本问题考查考生对常见安全攻击手段的了解。在解答本问题时，应结合电子商务平台的业务特征及题目中给出的安全中心主要功能，给出需应对的常见安全攻击手段。该平台需应对的常见安全攻击手段应包括：

(1) 网络侦听：指在数据通信或数据交互的过程中，攻击者对数据进行截取分析，从而实现对包括用户支付账号及口令数据的非授权获取和使用。

(2) 冒充攻击：攻击者采用口令猜测、消息重演与篡改等方式，伪装成另一个实体，欺骗安全中心的认证及授权服务，从而登录系统，获取对系统的非授权访问。

(3) 拒绝服务攻击：攻击者通过对网络协议的实现缺陷进行故意攻击，或通过野蛮手段耗尽被攻击对象的资源，使电子商务平台中包括安全中心在内的关键服务停止响应甚至崩溃，从而使系统无法提供正常的服务或资源访问。

(4) Web 安全攻击：攻击者通过跨站脚本或 SQL 注入等攻击手段，在电子商务平台系统网页中植入恶意代码或在表单中提交恶意 SQL 命令，从而旁路系统正常访问控制或恶意盗取用户信息。

【问题 2】

针对安全中心的安全性测试，可采用哪些基本的安全性测试方法？

可采用的基本安全性测试方法包括：

(1) 功能验证：采用软件测试中的黑盒测试方法，对安全中心提供的密钥管理、加解密服务、认证服务以及授权服务进行功能测试，验证所提供的相应功能是否有效。

(2) 漏洞扫描：借助于特定的漏洞扫描工具，对安全中心本地主机、网络及相应功能模块进行扫描，发现系统中存在的安全性弱点及安全漏洞，从而在安全漏洞造成严重危害之前，发现并加以防范。

(3) 模拟攻击试验：模拟攻击试验是一组特殊的黑盒测试案例，通过模拟典型的安全攻击来验证安全中心的安全防护能力。

(4) 侦听测试：通过典型的网络数据包获取技术，在系统数据通信或数据交互的过程中，对数据进行截取分析，从而发现系统在防止敏感数据被窃取方面的安全防护能力。

本问题考查考生对安全测试基本方法的理解。在解答本问题时，应针对电子商务平台的业务特征及题目中给出的安全中心主要功能，给出相应的安全性测试方法。针对安全中心的安全性测试，可采用的基本安全性测试方法包括：

(1) 功能验证：采用软件测试中的黑盒测试方法，对安全中心提供的密钥管理、加解密

服务、认证服务以及授权服务进行功能测试，验证所提供的相应功能是否有效。

(2) 漏洞扫描：借助于特定的漏洞扫描工具，对安全中心本地主机、网络及相应功能模块进行扫描，发现系统中存在的安全性弱点及安全漏洞，从而在安全漏洞造成严重危害之前，发现并加以防范。

(3) 模拟攻击试验：模拟攻击试验是一组特殊的黑盒测试案例，通过模拟典型的安全攻击来验证安全中心的安全防护能力。

(4) 侦听测试：通过典型的网络数据包获取技术，在系统数据通信或数据交互的过程中，对数据进行截取分析，从而发现系统在防止敏感数据被窃取方面的安全防护能力。

【问题 3】(5 分)

请分别说明针对密钥管理功能进行功能测试和性能测试各自应包含的基本测试点。

密钥管理功能的基本测试点：

(1) 功能测试

①系统是否具备密钥生成、密钥发送、密钥存储、密钥查询、密钥撤销、密钥恢复等基本功能；

②密钥库管理功能是否完善；

③密钥管理中心的系统、设备、数据、人员等安全管理是否严密；

④密钥管理中心的审计、认证、恢复、统计等系统管理是否具备；

⑤密钥管理系统与证书认证系统之间是否采用基于身份认证的安全通信协议。

(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利用并发压力测试工具测试受理点连接数、签发在用证书数目、密钥发放并发请求数是否满足业务需求；

②测试是否具备系统所需最大量的密钥生成、存储、传送、发布、归档等密钥管理功能；

③是否支持密钥用户要求年限的保存期；

④是否具备异地容灾备份；

⑤是否具备可伸缩配置及扩展能力；

⑥关键部分是否采用双机热备和磁盘镜像。

本问题考查密钥管理功能安全测试内容的相关知识。

按题目描述，密钥管理功能包括公钥加密体系中的公钥及私钥生成与管理，会话密钥的协商、生成、更新及分发等，因此密钥管理功能的安全测试应涵盖相应主要功能的测试，此

外，对于本系统还应进行相应的性能测试。

功能测试的基本测试点包括系统是否制定了密钥管理策略；系统是否具备密钥生成、密钥发送、密钥存储、密钥查询、密钥撤销、密钥恢复等基本功能；密钥库管理功能是否完善；密钥管理中心的系统、设备、数据、人员等安全管理是否严密；密钥管理中心的审计、认证、恢复、统计等系统管理是否具备；密钥管理系统与证书认证系统之间是否采用基于身份认证的安全通信协议等。性能测试的基本测试点包括利用并发压力测试工具测试受理点连接数、签发在用证书数目、密钥发放并发请求数是否满足业务需求；测试是否具备系统所需最大量的密钥生成、存储、传送、发布、归档等密钥管理功能；是否支持密钥用户要求年限的保存期；是否具备异地容灾备份；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。

【问题 4】（5 分）

请分别说明针对加解密服务功能进行功能测试和性能测试各自应包含的基本测试点。

加解密服务功能的基本测试点：

(1)功能测试

①系统是否具备基础加解密功能；

②能否为应用提供相对稳定的统一安全服务接口；

③能否提供对多密码算法的支持；

④随着业务量的逐渐增加，是否可以灵活增加密码服务模块，实现性能平滑扩展。

(2)性能测试

①各加密算法使用的密钥长度是否达到业内安全的密钥长度；

②RSA、ECC 等公钥算法的签名和验证速度以及 AES 等对称密钥算法的加解密速度是否满足业务要求；

③处理性能如公钥密码算法签名等是否具备可扩展能力。

本问题考查加解密服务功能安全测试内容的相关知识。

按题目描述，加解密服务功能包括基于 RSA、ECC 及 AES 等多密码算法的基本加解密服务，因此加解密服务功能的安全测试应涵盖基本加解密算法相应的功能测试与性能测试。功能测试的基本测试点包括系统是否具备基础加解密功能；能否为应用提供相对稳定的统一安全服务接口；能否提供对多密码算法的支持；随着业务量的逐渐增加，是否可以灵活增加密码服务模块，实现性能平滑扩展等。性能测试的基本测试点包括各加密算法使用的密钥长

度是否达到业内安全的密钥长度；RSA、ECC 等公钥算法的签名和验证速度以及 AES 等对称密钥算法的加解密速度是否满足业务要求；处理性能如公钥密码算法签名等是否具备可扩展能力等。