**信息安全工程师每日一练试题（2018/4/1）**

试题**1**： 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而增加开支，᳔ 合适的加密方式是  （1）  ，使用的会话密钥算法应该是  （2）  。

（1）A、 链路加密        B、 节点加密        C、 端－端加密        D、 混合加密
（2）A、 RSA B、 RC-5 C、 MD5 D、 ECC

试题**2**： 以下有关防火墙的说法中，错误的是（ ）。
A、防火墙可以提供对系统的访问控制 B、防火墙可以实现对企业内部网的集中安全管理
C、防火墙可以隐藏企业网的内部IP地址 D、防火墙可以防止病毒感染程序（或文件）的传播

试题**3**： 实现VPN的关键技术主要有隧道技术、加解密技术、 （1） 和身份认证技术。如果需要在传输层实现VPN，可选的协议是 （2） 。
（1）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
（2）A、L2TP B、PPTP C、TLS D、IPsec

试题**4**： 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**5**： 系统间进行异步串行通信时，数据的串/并和并/串转换一般是通过（）实现的。
A.I/O指令B.专用的数据传送指令C.CPU中有移位功能的数据寄存器D.接口中的移位寄存器

试题**6**： 某软件公司欲开发一个Windows平台上的公告板系统。在明确用户需求后，该公司的架构师决定采用Command模式实现该系统的界面显示部分，并设计UML类图如下图所示。图中与Command模式中的“Invoker”角色相对应的类是（1），与“ConcreteCommand”角色相对应的类是（2）。

（1）A. Command B. MenuItem C. Open D. ButktinBoardScreen
（2）A. Command B. MenuItem C. Open D. BulktinBoardScreen

试题**7**： 对于违反里氏替换原则的两个类A和B，可以采用的候选解决方案中，正确的是（）。
A. 尽量将一些需要扩展的类或者存在变化的类设计为抽象类或者接口，并将其作为基类，在程序中尽量使用基类对象进行编程
B. 创建一个新的抽象类C，作为两个具体类的超类，将A和B共同的行为移动到C中，从而解决A和B行为不完全一致的问题
C. 将B到A的继承关系改成组合关系
D. 区分是“Is-a”还是“Has-a”。如果是Is-a，可以使用继承关系，如果是Has-a，应该改成组合或聚合关系

试题**8**： 在结构化分析方法中，用（1）表示功能模型，用（2）表示行为模型。
(1)A．ER图 B．用例图 C．DFD D．对象图
(2)A．通信图 B．顺序图 C．活动图 D．状态转换图

试题**9**： 漏洞扫描技术包括ping扫描、端口扫描、Os探测、脆弱点探测、防火墙扫描等，每种技术实现的目标和运用的原理各不相同。其中端口扫描、防火墙扫描工作在  ( )  。
A．传输层B．网络层C．应用层D．会话层

试题**10**： 设计模式基于面向对象技术，是人们在长期的开发实践中良好经验的结晶，提供了一个简单、统一的描述方法，使得人们可以复用这些软件设计办法、过程管理经验。按照设计模式的目的进行划分，现有的设计模式可以分为创建型、（  ）和行为型三种类型。其中（  ）属于创建型模式，（  ）属于行为型模式。（  ）模式可以将一个复杂的组件分成功能性抽象和内部实现两个独立的但又相关的继承层次结构，从而可以实现接口与实现分离。
1.A．合成型 B．组合型 C．结构型 D．聚合型
2.A．Adaptor B．Façade C．Command D．Singleton
3.A．Decorator B．Composite C．Memento D．Builder
4.A．Prototype B．Flyweight C．Adapter D．Bridge

**信息安全工程师每日一练试题（2018/4/2）**

试题**1**： 应用系统运行中涉及的安全和保密层次包括系统级安全、资源访问安全、功能性安全和数据域安全。以下关于这四个层次安全的，错误的是（ ）。
A．按粒度从粗到细排序为系统级安全、资源访问安全、功能性安全、数据域安全
B．系统级安全是应用系统的第一道防线
C．所有的应用系统都会涉及资源访问安全问题
D．数据域安全可以细分为记录级数据域安全和字段级数据域安全

试题**2**： 《计算机信息系统安全保护等级划分准则》规定了计算机系统安全保护能力的5个等级。其中，按照（）的顺序从左到右安全能力逐渐增强
A、系统审计保护级、结构化保护级、安全标记保护级

B、用户自主保护级、访问验证保护级、安全标记保护级
C、访问验证保护级、系统审计保护级、安全标记保护级
D、用户自主保护级、系统审计保护级、安全标记保护级

试题**3**： 某软件公司正在设计一个通用的嵌入式数据处理平台，需要支持各种数据处理芯片之间的数据传递与交换。该平台的核心功能之一要求能够屏蔽芯片之间的数据交互，使其耦合松散，并且可以独立改变芯片之间的交互过程。针对上述需求，采用（）最为合适。
A.抽象工厂模式 B.策略模式 C.中介者模式 D.状态模式

试题**4**： 以下关于软件架构设计重要性的描述，（）是错误的。
A．软件架构设计能够满足系统的性能、安全性、可维护性等品质
B．软件架构设计能够帮助项目干系入(Stakeholder)更好地理解软件结构
C．软件架构设计能够帮助架构师更好地捕获和细化系统需求
D．软件架构设计能够有效地管理系统的复杂性，并降低系统维护费用

试题**5**： 信息安全的级别划分为不同的维度，在下列划分中，正确的是（）
A、系统运行安全和保密有5个层次，包括设备级安全、系统级安全、资源访问安全、功能性安全和数据安全。
B、机房分为4个级别：A级、B级、C级、D级
C、根据系统处理数据的重要性，系统可靠性分A级和B级
D、根据系统处理数据划分系统保密登记为绝密、机密和秘密

试题**6**： 访问控制是信息安全管理的重要内容之一，以下关于访问控制规则的叙述中，（ ）是不正确的
A、应确保授权用户对信息系统的正常访问
B、防止对操作系统的未授权访问
C、防止对外部网络未经授权进行访问，对内部网络的访问则没有限制
D、访问对应用系统中的信息未经授权进行访问

试题**7**： 关于防火墙的功能，下列叙述中错误的是( )．。
A．防火墙可以检查进出内部网络的通信量B．防火墙可以使用过滤技术在网络层对数据包进行选择
C．防火墙可以阻止来自网络内部的攻击D．防火墙可以工作在网络层，也可以工作在应用层

试题**8**： 随着互联网的发展，网络安全越来越受到人们的重视，其中能够鉴别什么样的数据包可以进出组织内部网络的安全技术成为（）
A、入侵检测 B、防病毒软件 C、安全审计系统 D、防火墙

试题**9**： 某公司有4百万元资金用于甲、乙、丙三厂追加投资。各厂获得不同投资款后的效益见下表。适当分配投资（以百万元为单位）可以获得的最大的总效益为（  ）百万元。

A．15.1 B．15.6 C．16.4 D．16.9

试题**10**： 在嵌入式操作系统中，板级支持包BSP作为对硬件的抽象，实现了（）。
A．硬件无关性，操作系统无关性      B．硬件有关性，操作系统有关性
C．硬件无关性，操作系统有关性      D．硬件有关性，操作系统无关性

**信息安全工程师每日一练试题（2018/4/3）**

试题**1**： 数字证书采用公钥体制进行加密和解密。每个用户有一个私钥，用它进行 （1） ；同时每个用户还有一个公钥，用于 （2） 。X.509标准规定，数字证书由 （3） 发放，将其放入公共目录中，以供用户访问。X.509数字证书中的签名字段是指 （4） 。如果用户UA从A地的发证机构取得了证书，用户UB从B地的发证机构取得了证书，那么 （5） 。
（1）A、解密和验证  B、解密和签名  C、加密和签名  D、加密和验证
（2）A、解密和验证  B、解密和签名  C、加密和签名  D、加密和验证
（3）A、密钥分发中心  B、证书授权中心  C、国际电信联盟  D、当地政府
（4）A、用户对自己证书的签名  B、用户对发送报文的签名

C、发证机构对用户证书的签名  D、发证机构对发送报文的签名
（5）A、UA可使用自己的证书直接与UB进行安全通信  B、UA通过一个证书链可以与UB进行安全通信
C、UA和UB还须向对方的发证机构申请证书，才能进行安全通信

 D、UA和UB都要向国家发证机构申请证书，才能进行安全通信

试题**2**： 在X.509标准中，不包含在数字证书中的数据域是  （ ）  。
A、序列号 B、签名算法 C、认证机构的签名 D、私钥

试题**3**： 以下关于系统性能的叙述中，不正确的是（）。
A.常见的Web服务器性能评估方法有基准测试、压力测试和可靠性测试
B.评价Web服务器的主要性能指标有最大并发连接数、响应延迟和吞吐量
C.对运行系统进行性能评估的主要目的是以更好的性能/价格比更新系统
D.当系统性能降到基本水平时，需要查找影响性能的瓶颈并消除该瓶颈

试题**4**： （）把整个软件开发流程分成多个阶段，每一个阶段都由目标设定、风险分析、开发和有效性验证以及评审构成。
A.原型模型 B.瀑布模型 C.螺旋模型 D. V模型

试题**5**： 软件质量保证是软件项目控制的重要手段，（）是软件质量保证的主要活动之一。
A.风险评估 B.软件评审 C.需求分析 D.架构设计

试题**6**： 以下关于白盒测试方法的叙述中，错误的是（）。
A．语句覆盖要求设计足够多的测试用例，使程序中每条语句至少被执行一次
B．与判定覆盖相比，条件覆盖增加对符合判定情况的测试，增加了测试路径
C．判定/条件覆盖准则的缺点是未考虑条件的组合情况
D．组合覆盖要求设计足够多的测试用例，使得每个判定中条件结果的所有可能组合最多出现一次

试题**7**： 通过收集和分析计算机系统或网络的关键节点信息，以发现网络或系统中是否有违反安全策略的行为和被攻击的迹象的技术被称为（）
A、系统检测B、系统分析C、系统审计D、入侵检测

试题**8**： 在软件系统工具中，版本控制工具属于（  ），软件评价工具属于（  ）。
1.A．软件开发工具B．软件维护工具C．编码与排错工具D．软件管理和软件支持工具
2.A．逆向工程工具B．开发信息库工具C．编码与排错工具D．软件管理和软件支持工具

试题**9**： 某公司拟开发一个扫地机器人。机器人的控制者首先定义清洁流程和流程中任务之间的关系，机器人接受任务后，需要响应外界环境中触发的一些突发事件，根据自身状态进行动态调整，最终自动完成任务。针对上述需求，该机器人应该采用（  ）架构风格最为合适。
A．面向对象B．主程序一子程序C．规则系统D．管道一过滤器

试题**10**： 某公司拟开发一个语音识别系统，其语音识别的主要过程包括分割原始语音信号、识别音素、产生候选词、判定语法片断、提供语义解释等，每个过程都需要进行基于先验知识的条件判断并进行相应的识别动作。针对该系统的特点，采用（）架构风格最为合适。
A．解释器B．面向对象    C．黑板    D．隐式调用

**信息安全工程师每日一练试题（2018/4/4）**

试题**1**： HTTPS是一种安全的HTTP协议，它使用 （1） 来保证信息安全，使用 （2）来发送和接收报文。
（1）A、IPSec  B、SSL  C、SET  D、SSH
（2）A、TCP的443端口  B、UDP的443端口  C、TCP的80端口  D、UDP的80端口

试题**2**： 建立PPP连接以后，发送方就发出一个提问消息（Challenge Message），接收方根据提问消息计算一个散列值。 （ ） 协议采用这种方式进行用户认证。
A、ARP B、CHAP C、PAP D、PPTP

试题**3**： 下面关于钓鱼网站的说法中错误的是（）。
A. 钓鱼网站仿冒真实网站的URL地址 B. 钓鱼网站通过向真实网站植入木马程序以达到网络攻击的目的
C. 钓鱼网站用于窃取访问者的机密信息D. 钓鱼网站可以通过E-mail传播网址

试题**4**： 以下关于软件中间件的叙述，错误的是（）。
A. 中间件通过标准接口实现与应用程序的关联，提供特定功能的服务
B. 使用中间件可以提高应用软件可移植性
C. 使用中间件将增加应用软件设计的复杂度
D. 使用中间件有助于提高开发效率

试题**5**： 以下关于第三方认证服务的叙述中，正确的是（）。
A．Kerberos认证服务中保存数字证书的服务器叫CA B．第三方认证服务的两种体制分别是Kerberos和PKI
C．PKI体制中保存数字证书的服务器叫KDC D．Kerberos的中文全称是“公钥基础设施”

试题**6**： 按照网络分层设计模型，通常把局域网设计为3层，即核心层、汇聚层和接入层，以下关于分层网络功能的描述中，不正确的是（）。
A．核心层设备负责数据包过滤、策略路由等功能
B．汇聚层完成路由汇总和协议转换功能
C．接入层应提供一部分管理功能，例如MAC地址认证、计费管理等
D．接入层负责收集用户信息，例如用户IP地址、MAC地址、访问日志等

试题**7**： 某公司欲开发一个用于分布式登录的服务端程序，使用面向连接的TCP协议并发地处理多客户端登录请求。用户要求该服务端程序运行在Linux、Solaris和WindowsNT等多种操作系统平台之上，而不同的操作系统的相关API函数和数据都有所不同。针对这种情况，公司的架构师决定采用“包装器外观(Wrapper Facade)”架构模式解决操作系统的差异问题。具体来说，服务端程序应该在包装器外观的实例上调用需要的方法，然后将请求和请求的参数发送给（1），调用成功后将结果返回。使用该模式（2）。
(1)A．客户端程序 B．操作系统API函数C．TCP协议API函数 D．登录连接程序
(2)A．提高了底层代码访问的一致性，但降低了服务端程序的调用性能
B．降低了服务端程序功能调用的灵活性，但提高了服务端程序的调用性能
C．降低了服务端程序的可移植性，但提高了服务端程序的可维护性
D．提高了系统的可复用性，但降低了系统的可配置性

试题**8**： 在对一个软件系统的架构进行设计与确认之后，需要进行架构复审。架构复审的目的是为了标识潜在的风险，及早发现架构设计中的缺陷和错误。在架构复审过程电，主要由（）决定架构是否满足需求、质量需求是否在设计中得到体现。
A．系统分析师与架构师 B．用户代表与领域专家C．系统拥有者与项目经理 D．系统开发与测试人员

试题**9**： 某公司的人员流动比较频繁，网络信息系统管理员为了减少频繁的授权变动，其访问控制模型应该采用()  。
A．自主型访问控制B．强制型访问控制C．基于角色的访问控制D．基于任务的访问控制

试题**10**： 某公司拟为某种新型可编程机器人开发相应的编译器。该编译过程包括词法分析、语法分析、语义分析和代码生成四个阶段，每个阶段产生的结果作为下一个阶段的输入，且需独立存储。针对上述描述，该集成开发环境应采用（  ）架构风格最为合适。
A．管道—过滤器B．数据仓储C．主程序—子程序D．解释器

**信息安全工程师每日一练试题（2018/4/5）**

试题**1**： （ ）指对主体访问和使用客体的情况进行记录和审查，以保证安全规则被正确执行，并帮助分析安全事故产生的原因。
A.安全授权 B.安全管理 C.安全服务 D.安全审计

试题**2**： 关于网络安全服务的叙述中，（ ）是错误的。
A、应提供访问控制服务以防止用户否认已接收的信息 B、应提供认证服务以保证用户身份的真实性
C、应提供数据完整性服务以防止信息在传输过程中被删除

D、应提供保密性服务以防止传输的数据被截获或篡改

试题**3**： 若对关系R（A，B，C，D）和S（C，D，E）进行关系代数运算，则表达式 与（）等价。

试题**4**： 系统输入设计中应尽可能考虑人的因素，以下关于输入设计的一般原理中，错误的是（）。
A.只让用户输入变化的数据B.使用创新的模式吸引用户的眼球
C.表格中各个数据项应有提示信息D.尽可能使用选择而不是键盘输入的方式获取数据

试题**5**： 公司总部与分部之间需要传输大量数据，在保障数据安全的同时又要兼顾密钥算法效率，最合适的加密算法是（）。
A. RC-5  B. RSA  C. ECC  D. MD5

试题**6**： 在采用公开密钥密码体制的数字签名方案中，每个用户有一个私钥，可用它进行(1)；同时每个用户还有一个公钥，可用于(2)．。
(1)A．解密和验证 B．解密和签名 C．加密和签名 D．加密和验证
(2)A．解密和验证 B．解密和签名 C．加密和签名 D．加密和验证

试题**7**： 特洛伊木马程序分为客户端（也称为控制端）和服务器端（也称为被控制端）两部分。当用户访问了带有木马的网页后，木马的( )部分就下载到用户所在的计算机上，并自动运行。
A．客户端 B．服务器端 C．客户端和服务器端 D．客户端或服务器端

试题**8**： 计算机网络的安全主要是指（）。
A．网络设施环境的安全B．网络中信息的安全C．网络中使用者的安全D．网络中财产的安全

试题**9**： 螺旋模型在（  ）的基础上扩展而成。
A．瀑布模型B．原型模型C．快速模型D．面向对象模型

试题**10**： 软件著作权保护的对象不包括（  ）
A．源程序B．目标程序C．用户手册D．处理过程

**2018/4/1 1~5 CB D DC C D 6~10 BC A CD A 无**

**2018/4/2 1~5 C D C C D 6~10 C C D C B**

**2018/4/3 1~5 BDBCB D C C B 6~10 D D BD C C**

**2018/4/4 1~5 BA B B C B 6~10 A BA B C A**

**2018/4/5 1~5 D A B B A 6~10 BD B B B D**