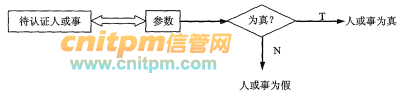
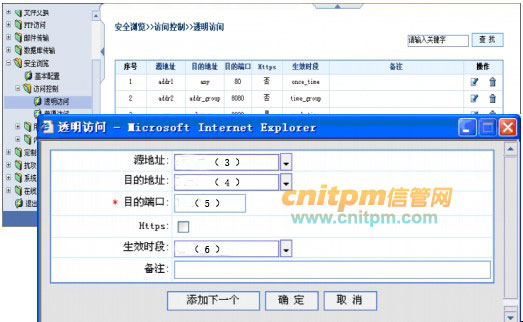
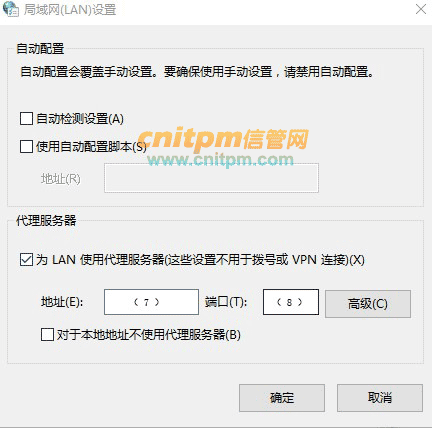
**信息安全工程师案例分析每日一练（2016/10/30）**

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】  
认证又称鉴别或确认，它是证实某事是否名副其实或是否有效的一个过程。认证和加密的区别在于:加密用以确保数据的保密'性，阻止对手的被动攻击，如截取，窃听等；而认证用以确保报文发送者和接收者的真实性以及报文的完整性，阻止对手的主动攻击，如冒充、篡改、重播等。认证往往是许多应用系统中安全保护的第一道设防，因而极为重要。  
认证的基本思想是通过验证称谓者（人或事）的一个或多个参数的真实性和有效性，来达到验证称谓者是否名副其实的目的。这样，就要求验证的参数和被认证的对象之间存在严格的对应关系，理想情况下这种对应关系应是唯一的。其基本原理如下图所示。  
                                         
认证原理  
  
认证系统常用的参数有口令、标识符、密钥、信物、智能卡、指纹、视网纹等。对于那些能在长时间内保持不变的参数(非时变参数)可采用在保密条件下预先产生并存储的位模式进行认证，而对于经常变化的参数则应适时地产生位模式，再对此进行认证。  
【问题1】（3分）  
认证和数字签名技术都是确保数据真实性的措施，请分析这两者之间的区别。  
【问题2】（5分）  
口令是接收双方预先约定的秘密数据，它用来验证用户知道什么。口令验证简单易行，因此口令验证是目前应用最为广泛的身份认证方法之一。在计算机系统中，操作系统、网络、数据库都采用了口令验证。在一些简单的系统中，用户的口令以口令表的形式存储。当用户要访问系统时，系统要求用户提供其口令，系统将用户提供的口令与口令表中存储的相应用户的口令进行比较，若相等则确认用户身份有效，否则确认用户身份无效，担绝访问。请分析在上述口令验证机制中会存在哪些问题？（3分）列举4种改进的口令验证机制。（2分）  
【问题3】（7分）  
在网络环境中，攻击者可进行以下攻击:  
（1）冒充发送方发送一条报文；  
（2）冒充接收方发送收到或未收到报文的应答；  
（3）插入、删除或修改报文内容；  
（4）修改报文顺序(插入报文、删除报文或重排序)议及延时或重播报文。  
因此，报文认证必须使通信方能够验证每份报文的发送方、接收方、内容和时间性的真实性和完整性。也就是说，通信方能够确定：  
（1）报文是由意定的发送方发出的；  
（2） 报文传送给意定的接收方；  
（3）报文内容有无篡改或发生错误；  
（4） 报文按确定的次序接收。  
报文认证的方式有报文源的认证、报文宿的认证及报文内容的认证，消息认证码MAC是属于哪种报文认证方式？（2分）其认证过程是怎样的？（5分）

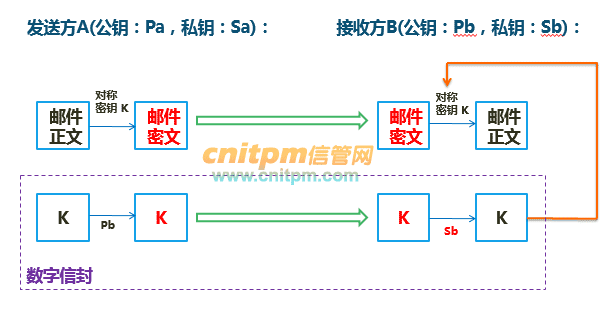
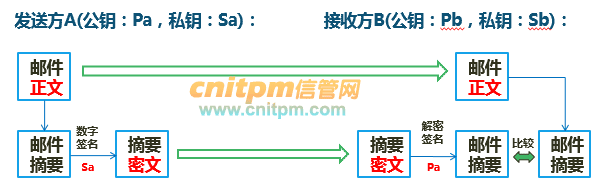
**信息安全工程师案例分析每日一练试题（2016/10/31）**

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】  
网御SIS-3000安全隔离网闸配置安全浏览，要求实现内网 IE 浏览器用户通过安全隔离网隔安全地访问外网 Web服务器（在 IE 浏览器地址栏输入： http: 192.168 .1 .2后，返回正确的页面，说明访问成功）。  
根据网络拓扑，其具体需求要点如下：  
1、网闸内、外网络口各直连一台装有 WindowsXP Professional 系统的主机，与网闸外侧相连的是 Web 服务器（端口 80），与网闸内侧相连的是 IE 浏览器用户；  
2、要求以透明和普通两种方式访问；  
3、 IP 地址设置如下图所示。  
  
安全浏览网络拓扑图  
  
（1）添加网闸内侧访问控制中的访问规则，并启动服务。  
添加普通访问规则，如下图所示。  
  
添加普通访问规则  
添加透明访问规则，如下图所示。  
  
添加透明访问规则  
（2）启动网闸外侧服务。  
无论是透明访问还是普通访问，仅进入"安全浏览→基本配置"启动服务。如下图。  
  
启动服务  
  
（3）配置IE浏览器用户主机  
针对普通访问，需要设置代理，如下图。  
  
代理设置  
  
针对透明访问，需要设置默认网关或静态路由，如下图。  
  
默认网关设置  
【问题1】（6分）  
根据下面选项将网闸配置中访问控制规则的空缺部分（1）—（6）补充完整。  
A、addr1 B、8080 C、work\_time D、addrgroup1 E、any  
F、time\_group1 G、lenovo H、addr2 I、21  
（1）                   （2）                       （3）   
（4）                   （5）                       （6）  
【问题2】（5分）  
根据安全浏览的配置需求，将配置IE浏览器用户主机中空缺（7）—（11）补充完整。  
（7）            （8）              （9）  
（10）          （11）  
【问题3】（2分）  
在Windows XP系统中，如何进入代理设置页面设置代理？（1分）如何进入默认网关设置页面设置默认网关？（1分）  
【问题4】（2分）  
如何判断安全浏览设置成功？

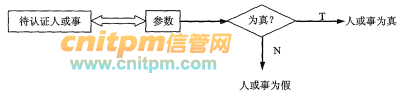
**信息安全工程师案例分析每日一练试题（2016/11/1）**

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】  
在Internet 技术飞速演变、电子商务蓬勃发展的今天，开发的银多应用程序都是 Web应用程序，随着微信、微博、网上银行等一系列的新型的 Web 应用程序的诞生， Web应用越来越广泛。然而 Web 应用程序及 Web 站点往往很容易遭受各种各样的入侵， Web数据在网络传输过程中也银容易被窃取或盗用。如何能够使 Web 及数据传输更加安全，就显得尤为重要。  
如今， Web 业务平台己经在电子商务、企业信息化中得到广泛应用，很多企业部将应用架设在 Web 平台上， Web 业务的迅速发展也引起了黑客们的强烈关注，他们将注意力从以往对传统网络服务器的攻击逐步转移到了对 Web 业务的攻击上。黑客利用网站操作系统的漏洞和 Web 服务程序的 SQL 注入漏洞等得到 Web 服务器的控制权限，轻则篡改网页内容，重则窃取重要内部数据，更为严重的则是在网页中植入恶意代码，使得网站访问者受到侵害。  
国际权威机构 Forrester 的统计数据表明， 67% 的攻击是通过应用层的攻击。即是，最简单的网页浏览也有可能造成威胁，比如，单击含有病毒的网址、隐秘的图片，或者，单击下载某些免费的软件、文件等，由于下载的软件或者文件中含有未知的恶意代码，当用户在运行程序或者打开这些文件时，恶意代码被启动就有可能造成用户个人信息丢失，甚至后台服务器系统出现漏洞给恶意攻击者窃取信息提供方便的大门。  
【问题1】（5分）  
开源 Web 应用安全项目 （OWASP） 是一个开放的社区组织。专注于讨论应用程序，代码开发的威胁讨论。 TOP 10项目的目标是通过找出企业组织所面临的最严重的十大风险来提高人们对应用程序安全的关注度。以下是其中罗列的十大最有可能发生的应用漏洞，将选项A-J正确对应到其括号内。  
1、注入（  ）  
2、失效的身份认证和会话管理（  ）  
3、跨站脚本（XSS）（  ）  
4、不安全的直接对象引用（  ）  
5、安全配置错误（  ）  
6、敏感信息泄露（  ）  
7、功能级访问控制缺失（  ）  
8、跨站请求伪造（CSRF）（  ）  
9、使用更含有已知漏洞的组件（  ）  
10、未验证的重定向和转发（  ）  
  
A、如果一个带有漏洞的组件被利用，这种攻击可以造成更为严重的数据丢失或服务器接管，在应用程序中使用会破坏应用程序防御系统。  
B、攻击者可能会窃取或篡改这些弱保护的数据以进行信用卡诈骗、身份窃取，或其他犯罪。  
C、Web 应用程序经常将用户重定向和转发到其他网页和网站，并且利用不可信的数据去判定目的页面。  
D、迫使登录用户的浏览器将伪造的 HTTP 请求，包括该用户的会话 cookie 和其他认证信息，发送到一个存在漏洞的 Web 应用程序。  
E、应用程序需要在每个功能被访问时在服务器端执行相同的访问控制检查。如果请求没有被验证，攻击者能够伪造请求以在未经适当授权时访问功能。  
F、好的安全需要对应用程序、框架、应用程序服务器、 Web 服务器、数据库服务器和平台定义和执行安全配置。  
G、攻击者通过在应用程序预先定义好的查询语句结尾加上额外的查询语句元素，欺骗数据库服务器执行非授权的任意查询。  
H、攻击者通过在这种链接中插入恶意代码，当用户不小心单击这样带有恶意代码的链接时，其用户信息就有可能被攻击者盗取。  
I、用户使用公共计算机浏览网站，登录验证身份之后，离开时没有退出账户而是选择直接关闭浏览器，使得下一个用户使用相同计算机浏览相同浏览器，可以看到上一个用户的对话。  
J、作为授权的系统用户，攻击者只需要修改指向一个系统对象的直接引用参数值，让其指向另一个无权的对象。  
【问题2】（2分）  
SQL注入攻击有4个基本的特点：A、局限性，B、隐蔽性，C、攻击时间短，D、危害大。其中哪个错误的？（1分）应该是什么？（1分）  
【问题3】（3分）  
SQL注入攻击的危害性很大，应该从哪些方面来避免这种漏洞攻击？  
【问题4】（5分）  
如何防范跨站脚本（XSS）？（3分）如何防范跨站请求伪造（CSRF）？（2分）

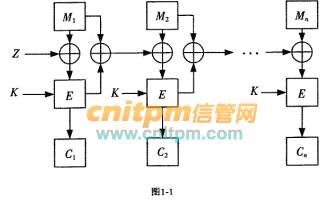
**信息安全工程师案例分析每日一练试题（2016/11/25）**

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】  
数据加密技术分为对称加密技术和非对称加密技术。对称加密技术要求需要强大的加密算法，发送方和接收方必须保证密钥的安全，其优点是加密速度快，缺点是加密强度不高、密钥分发困难，它能应用大量数据的加密。非对称加密技术的优点是加密强度高，密钥分发简单，其缺点是加密速度慢，算法复杂，它只能应用于少量数据的加密。为了使其能加密大量数据的同时，能保障加密数据的安全性及加密的效率，通常会对两者进行结合，对原文信息采用对称密钥进行加密，再利用非对称密钥加密传递对称密钥，这个过程称之为数字信封，具体如下图所示：  
  
数字信封  
  
数字签名是证明通信双方身份和数据真实性的一种信息。它满足以下的条件：签名者事后不能抵赖自己的签名；任何其他人不能伪造签名；如果当事的双方关于签名的真伪发生争执，能够在公正的仲裁者面前通过验证签名来确认其真伪。以邮件签名过程为例，具体如下图所示：  
  
数字签名  
  
【问题1】（3分）  
请分别列举3种以上的对称加密算法和非对称加密算法。  
【问题2】（4分）  
非对称加密技术的加解密和签名的过程中发送方用哪个密钥进行加密和签名，接收方用哪个密钥进行解密和验证签名？（2分）为什么？（2分）  
【问题3】（8分）  
根据上述的加密技术以及数字签名技术，请设计一个安全邮件传输系统，要求：该邮件以加密方式传输，邮件能支持最大附件的传送，发送者不可抵赖，若邮件被第三方截获，第三方无法篡改。

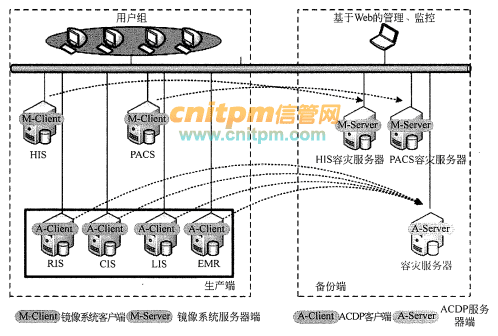
**信息安全工程师案例分析每日一练试题（2016/12/2）**

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】  
认证又称鉴别或确认，它是证实某事是否名副其实或是否有效的一个过程。认证和加密的区别在于:加密用以确保数据的保密'性，阻止对手的被动攻击，如截取，窃听等；而认证用以确保报文发送者和接收者的真实性以及报文的完整性，阻止对手的主动攻击，如冒充、篡改、重播等。认证往往是许多应用系统中安全保护的第一道设防，因而极为重要。  
认证的基本思想是通过验证称谓者（人或事）的一个或多个参数的真实性和有效性，来达到验证称谓者是否名副其实的目的。这样，就要求验证的参数和被认证的对象之间存在严格的对应关系，理想情况下这种对应关系应是唯一的。其基本原理如下图所示。  
                                         
认证原理  
  
认证系统常用的参数有口令、标识符、密钥、信物、智能卡、指纹、视网纹等。对于那些能在长时间内保持不变的参数(非时变参数)可采用在保密条件下预先产生并存储的位模式进行认证，而对于经常变化的参数则应适时地产生位模式，再对此进行认证。  
【问题1】（3分）  
认证和数字签名技术都是确保数据真实性的措施，请分析这两者之间的区别。  
【问题2】（5分）  
口令是接收双方预先约定的秘密数据，它用来验证用户知道什么。口令验证简单易行，因此口令验证是目前应用最为广泛的身份认证方法之一。在计算机系统中，操作系统、网络、数据库都采用了口令验证。在一些简单的系统中，用户的口令以口令表的形式存储。当用户要访问系统时，系统要求用户提供其口令，系统将用户提供的口令与口令表中存储的相应用户的口令进行比较，若相等则确认用户身份有效，否则确认用户身份无效，担绝访问。请分析在上述口令验证机制中会存在哪些问题？（3分）列举4种改进的口令验证机制。（2分）  
【问题3】（7分）  
在网络环境中，攻击者可进行以下攻击:  
（1）冒充发送方发送一条报文；  
（2）冒充接收方发送收到或未收到报文的应答；  
（3）插入、删除或修改报文内容；  
（4）修改报文顺序(插入报文、删除报文或重排序)议及延时或重播报文。  
因此，报文认证必须使通信方能够验证每份报文的发送方、接收方、内容和时间性的真实性和完整性。也就是说，通信方能够确定：  
（1）报文是由意定的发送方发出的；  
（2） 报文传送给意定的接收方；  
（3）报文内容有无篡改或发生错误；  
（4） 报文按确定的次序接收。  
报文认证的方式有报文源的认证、报文宿的认证及报文内容的认证，消息认证码MAC是属于哪种报文认证方式？（2分）其认证过程是怎样的？（5分）

**信息安全工程师案例分析每日一练试题（2016/12/5）**

阅读下列说明和图，回答问题1至问题3，将解答填入答题纸的对应栏内。  
【说明】  
研究密码编码的科学称为密码编码学，研究密码破译的科学称为密码分析学，密码编码学和密码分析学共同组成密码学。密码学作为信息安全的关键技术，在信息安全领域有着广泛的应用。  
【问题1】（9分）  
密码学的安全目标至少包括哪三个方面？具体内涵是什么？  
【问题2】（3分）  
对下列违规安全事件，指出各个事件分别违反了安全目标中的哪些项？  
（1）小明抄袭了小丽的家庭作业。  
（2）小明私自修改了自己的成绩。  
（3）小李窃取了小刘的学位证号码、登录口令信息、并通过学位信息系统更改了小刘的学位信息记录和登陆口令，将系统中小刘的学位信息用一份伪造的信息替代，造成小刘无法访问学位信息系统。  
【问题3】（3分）  
现代密码体制的安全性通常取决于密钥的安全，文了保证密钥的安全，密钥管理包括哪些技术问题？  
【问题4】（5分）  
在图1-1给出的加密过程中，Mi，i=1，2，…，n表示明文分组，Ci，i=1,2，…，n表示密文分组，Z表示初始序列，K表示密钥，E表示分组加密过程。该分组加密过程属于哪种工作模式？这种分组密码的工作模式有什么缺点？  


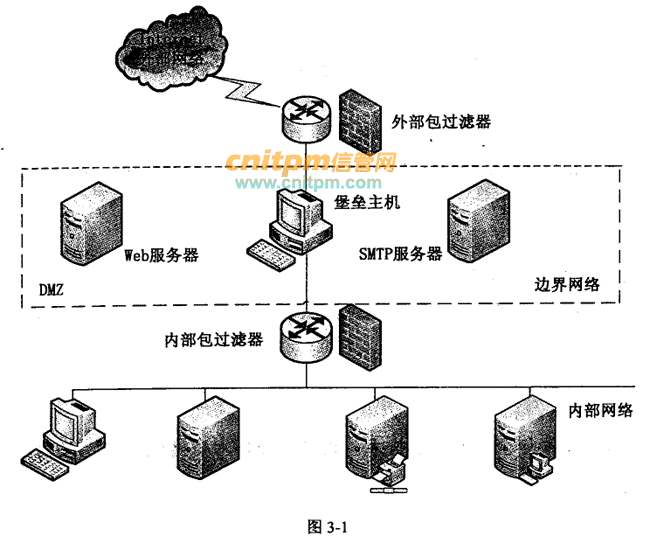
**信息安全工程师案例分析每日一练试题（2016/12/14）**

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】  
网络容灾备份系统是指在相隔较远的异地，建立两套或多套功能相同的 IT 系统，互相之间可以进行健康状态监视和功能切换，当一处系统因意外（如火灾、地震等）停止工作时，整个应用系统可以切换到另一处，使得该系统功能可以继续正常工作。网络容灾技术是系统的高可用性技术的一个组成部分，网络容灾系统更加强调处理外界环境对系统的影响，特别是灾难性事件对整个 IT 节点的影响，提供节点级别的系统恢复功能。  
从根本上说，灾难恢复计划应当包括 个重要部分:数据保护、灾难防备和事后恢复。数据系统的安全体系主要有数据备份系统、高可用系统两个方面，备份系统提供应用系统的数据后援，确保在任意情况下(包括人工操作失误)数据具有完整的恢复能力，高可用性系统提供故障检测和故障切换功能，确保系统在规定时间内恢复服务能力。  
一个完善的网络容灾备份应包括硬件级物理容错和软件级数据备份，并且能够自动地跨越整个系统网络平台，其主要包括构造双机容错系统、各类数据库的备份、网络故障和灾难恢复、备份任务管理等。  
大型医院因为其各方面因素，常常对数据容灾有很高的要求，根据国家等级规范，可达到最高层次的第6级要求，下图是某医皖的容灾架构图。  
  
容灾系统拓扑结构图  
【问题1】（3分）  
建立容灾备份系统时会涉及到哪些技术？  
【问题2】（6分）  
网络容灾备份系统的分类有哪些？（3分）其含义是什么？（3分）  
【问题3】（6分）  
在容灾系统拓扑结构图中，哪些是局域网内部署的备用服务器？（3分）为了实现数据的实时复制和操作系统、文件的定时备份要在哪些服务器上分别部署什么软件？（3分）

**信息安全工程师案例分析每日一练试题（2016/12/23）**

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】  
日志分析就是对有关操作系统、系统应用或用户活动所产生的一系列的计算机安全事件进行记录和分析的过程。在计算机系统中，安全管理员采用日志分析审计系统来监视系统的状态和活动，并对日志文件进行分析、及时发现系统中存在的安全问题。  
一个安全的网络系统中的日志分析审计系统，是对网络系统中任一或所有安全相关事件进行记录、分析和再现的处理系统。对于日志分析审计系统的一般要求主要包括：  
1、记录与再现：要求审计系统能够记录系统中所有的安全相关事件，同时，如果有必要，应该能够再现产生某一系统状态的主要行为；  
2、入侵检测：分析审计系统应能够检查出大多数常见的系统入侵的企图，同时，经过适当的设计，应该能够阻止这些入侵行为；  
3、记录入侵行为：分析审计系统应该记录所有的入侵企图，即使某次入侵己经成功，这时候调查取证和系统恢复必不可少的；  
4、威慑作用：应该对系统中具有的日志分析审计系统及其性能进行适当宣传，这样可以对企图入侵者起到威慑作用，又可以减少合法用户在无意中违反系统的安全策略；  
5、系统本身的安全性：必须保证日志分析审计系统本身的安全性，其中，一方面包括操作系统和软件的安全性，另一方面包括分析审计数据的安全性；一般来说，要保证日志分析审计系统本身的安全，必须与系统中其他安全措施，例如认证、授权、加密措施等相配合。  
一个日志分析审计系统的简单模型包括两个部分：日志数据采集器，它用于采集数据；日志数据分析器，它负责对分析审计数据采集器发送给它的日志数据进行分析。  
【问题1】（2分）  
根据说明，日志分析审计的功能包括（  ）（可多选）  
A、对潜在的攻击者起到震慑或警告  
B、对于已经发生的系统破坏行为，提供有效的追纠证据  
C、为系统管理员提供有价值的系统使用日志，从而帮助系统管理员及时发现系统入侵行为或潜在的系统漏洞  
D、能检测并查杀计算机病毒保证计算机系统的安全  
【问题2】（3分）  
日志分析方法通常有以下三种，请将该描述的选项对应到其中。  
1、基于正则表达式的模式匹配日志分析（  ）  
2、基于关联分析的日志分析（  ）  
3、基于聚类分析的日志分析（  ）  
A、用一定数量的样本（称为训练样本集） ，由这些样本及其己知类别，给出一套分类判别准则，使得按照这套分类判别准则，对待识别模式进行分类使错误识别率最小。训练完毕后，对任何一个样本，都可以利用分类器将其归到某类中。  
B、是数据挖掘中最活跃的研究方法之一。给定一个日志数据库，通过用户指定最小支持度和最小可信度来寻找合适关联规则的过程。  
C、可以用于模式匹配和替换的强有力的工具，可以让用户通过一系列的特殊字符构建匹配模式，然后捏匹配模式与数据文件、程序输入以及 Web 页面的表单输入等目标对象进行比较，根据比较对象中是否包含匹配模式，执行相应的程序。它通常在对日志文件的初步分析中使用。  
【问题3】（2分）  
一般关联规则挖掘问题可以划分成两个子问题，一是通过用户给定的最小支持度（ minsupport） ，寻找所有频繁项目集 （Frequent Item set） ，即满足 support不小于 minsupport 的项目集。事实上，这些频繁项目集可能具有包含关系。一般地，我们只关心那些不被其他频繁项目集所包含的所谓频繁大项集 （Frequent Large Item set）的集合。这些频繁大项集是形成关联规则基础。二是通过用户给定的最小可信度（ minconfidence） ，在每个最大频繁项目集中，寻找 confidence 不小于minconfidence 的关联规则。根据描述写出这两个子问题名称。  
【问题4】（8分）  
通过典型的基于关联分析的 Apriori 算法进行日志分析得出的是特征模式，例如通过对用户历史数据的分析，发现如下关联规则：  
模式 ： username = A, timestamp = am， hostip = 192.168.1.119, userip = 192.168. 1.201 [0.98 ,0.60]  
则该模式表示用户A通常在每天的上午登录，登录的主机是192.168.1.119，登录时的IP地址是192.168.1.201，该模式的置信度为98% ，支持度为60%。  
（1）根据上述方法，请分析模式：username = A, command = vi, param=.c[0.45, 0.05]。其中，command表示用户经常执行的命令，param表示执行命令时所使用的参数（3分）  
如果在 Apriori 算法的基础上加上一个时间约束则是时间序列分析算法，它用于分析不同审计记录之间的相关性。它的形式为：X，Y→Z[C ,S,w]， X,Y,Z为项集，W为时间约束。含义：若X,Y发生，则在w秒内，Z也发生。  
S=Support(XYZ) 是规则的支持度：满足规则的样本百分比。  
C=Support(XYZ)/Support( XY)是置信度：当X，Y发生时Z发生的条件概率。  
系统调用序列与时间序列分析不同的是它只有一个支持度，没有时间窗口的限制，也没有置信度。  
如：通过对用户A所执行的命令序列进行分析，发现如下序列模式：  
command=vi,param=.c→command=gcc,param=-g-o→command=gdb(0.4)  
（2）请分析该模式的含义。（3分）  
（3）假设以上的三个模式是挖掘出的关联规则和序列模式，试对其进行分析。（2分）

**信息安全工程师案例分析每日一练试题（2016/12/24）**

阅读下列说明和图，回答问题1至问题3，将解答填入答题纸的对应栏内。  
【说明】  
防火墙是一种广泛应用的网络安全防御技术，它阻挡对网络的非法访问和不安全的数据传递，保护本地系统和网络免于受到安全威胁。  
图3-1改出了一种防火墙的体系结构。   
  
【问题1】（6分）  
防火墙的体系结构主要有：  
（1）双重宿主主机体系结构；  
（2）（被）屏蔽主机体系结构；  
（3）（被）屏蔽子网体系结构；  
请简要说明这三种体系结构的特点。  
【问题2】（5分）  
（1）图3-1描述的是哪一种防火墙的体系结构？  
（2）其中内部包过滤器和外部包过滤器的作用分别是什么？  
【问题3】（8分）  
设图3-1中外部包过滤器的外部IP地址为10.20.100.1，内部IP地址为10.20.100.2，内部包过滤器的外部IP地址为10.20.100.3，内部IP地址为192.168.0.1，DMZ中Web服务器IP为10.20.100.6，SMTP服务器IP为10.20.100.8.  
关于包过滤器，要求实现以下功能，不允许内部网络用户访问外网和DMZ，外部网络用户只允许访问DMZ中的Web服务器和SMTP服务器。内部包过滤器规则如表3-1所示。请完成外部包过滤器规则表3-2，将对应空缺表项的答案填入答题纸对应栏内。   
