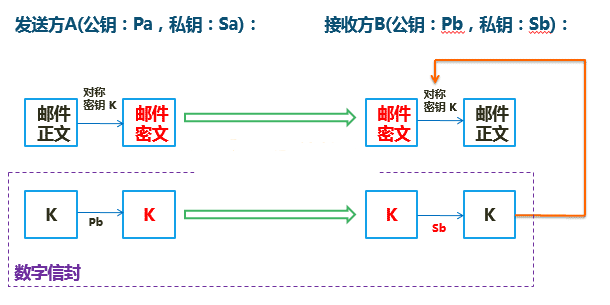
**2017年信息安全工程师考试下午试题加答案（三）**

新开的**信息安全工程师考试**分属该考试“信息系统”专业，位处中级资格。大家在找试题做练习的时候是否苦恼没有资源？希赛软考学院为大家整理了一些下午试题的练习，供大家参考，希望能有所帮助。

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。

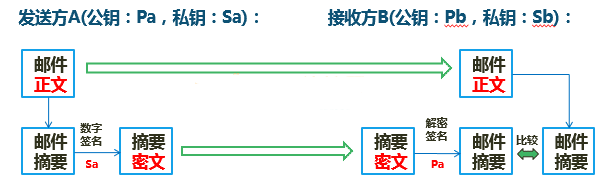
【说明】

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）

**参考答案**

【问题1】

对称加密：des,3des,aes.

非对称加密：rsa,idea,ec。

【问题2】

pa加密。sb解密。

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。

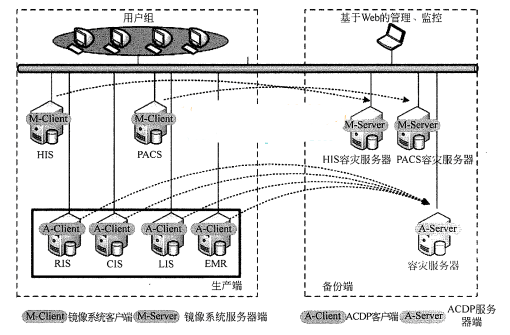
  【说明】

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）

**参考答案**

   1、远程镜像技术，快照技术，基于ip的san互连技术

   2、数据容灾，指建立一个异地的数据系统，改系统是本地关键应用数据的一个可用复制应用容灾，指在一定建立一套完整的与本地产生系统相当的备份应用系统

   3、在局域网内部署三台备用服务器，分别是his,pacs以及其他业务系统的容灾服务器。针对不同的业务对rto.rpo的要求，his和pacs数据库服务器部署镜像软件，ris,lis,cis等其他四台数据库服务器上分别部署连续数据保护cdp软件。