一、 简答题

1. 信息安全保障系统 PDRR 包括哪四个部分内容?
2. 为了更好地利用 DES 等对称密钥密码算法，人们已为它们设计了多种工作模式。请给出一种模式，具有如下两个特点：(1) 相同明文块对应不同的密文；(2) 一个密文块损坏仅有与其对应的明文块无法正常解密。要求给出该模式的加密，解密示意图并解释其主要思想。
3. 用 MD5 之类的散列函数来存储用户密码时，哈希碰撞是指攻击者可以从哈希码反推出用户密码。请问这个一说法是否正确？如果不正确，请解释错误之处。
4. 物理隔离和逻辑隔离区别?
5. 什么是认证中心？电子商务的交易过程中为什么必须设定 CA?
6. DNS 欺骗主要有两种形式，即监听式主机欺骗和 DNS 服务器污染。假设攻击者企图欺骗来自某个特定 IP 地址的用户在一段时间内的域名查询，该攻击者应该采用哪种形式？请简述该形式的 DNS 欺骗攻击的原理。
7. 防火墙的工作机制是依据安全规则检查每一个通过防火墙的数据包，只有符合安全规则的数据包才能通过。请简述防火墙的局限性。
8. （1）在 SET 协议中，电子信封指的是什么？（2）简述电子信封在 SET 协议中起什么作用？（3）简述电子信封的主要作用过程?

9. DRM（数字版权保护管理）系统一般分为服务器和客户端两部分。结合服务器，和客户端的主要功能，简述 DRM 工作原理。
10. 我国信息安全标准体系包括哪 6 个部分？在我国众多的信息安全标准中，哪个标准被认为是我国信息安全标准的奠基石。

二、 计算题和分析题

1. 已知仿射加密变换为 E（X）=5X+12（mod26），请问：（1）明文 HIT 对应密文（2）若已知 HGD 是上述仿射加密后的密文，其明文是什么？要求给出主要计算过程
2. RSA 签名算法每次只能对一个固定长度（比如 N 比特）的消息进行签名。为了对任意长度的消息进行签名，有人建议了这样一种处理方法：首先将长消息切割成固定长度 N 比特的数据块，然后用 RSA 签名算法对每个数据块进行签名，最后将这些签名块拼接起来就得到了长消息的签名。请问采用这种切割处理方法的签名算法安全吗？请举例说明为什么？

三、 设计题

1. 基本的 Diffie-Hellman 密钥交换算法容易受到中间人攻击。假设 A 和 B 要通信，攻击者可以冒充 B 获得一个与 A 共享的密钥，冒充 A 获得一个与 B 共享的密钥，进而实现中间人攻击。请在 Diffie-Hellman 密钥交换算法的基础上，利用数字证书，设计一个可以避免中间人攻击的 Diffie-Hellman 密钥交换协议。要求给出协议步

骤

2. 利用公钥密码算法实现认证时，一般采用如下步骤：（1）$C=E_{kra}$（M），发送方 A 用私钥加密 M 后把密文 C 发送给 B；（2）$M=D_{kva}$（C）接收方 B 用 A 方的公钥进行解密。请问，在这个过程中，能否同时保证消息的保密性？如不能，请在此基础上给出一个解决方案，既实现认证，有保证消息的保密性
3. 目前大多数的主机和服务器都使用访问控制列表作为文件访问控制的实现机制。若已知某文件系统的访问控制能力表 cap 如下，请给出对应的访问控制表 cal。
   1) cap(Bob)={(object1,{ 拥 有 }),(object2,{ 读 ，写}),(object4,{执行})}
   2) cap(Alice)={(object,{写}),(object2,{拥有}),(object3,{拥有}),(object3,{执行})}
   3) cap(John)={(obecjt1,{读,写}),(object3,{写}),(obejct4,{拥有})}