1．是非判断题

(1)密码系统的安全性不应取决于不易改变的算法，而应取决于可随时改变的密钥。(V)

(2)密钥管理是一门综合性的系统工程，要求管理与技术并重，除了技术性的因素外，还与人的因素密切相关，包括密钥管理相关的行政管理制度和密钥管理人员的素质。(V)

(3)历史表明,从密钥管理途径窃取秘密要比单纯从破译密码算法窃取秘密所花费的代价要小得多。(V)

(4)密钥的分级系统主要简化了密钥管理，与密钥的安全性无关。(X)

(5)密钥管理的目标就是追求密钥的更高安全性。(X) 注：提供安全的密钥服务

(6)密钥使用次数越多，被破译的危险性就越大，所以，密钥需要定期更新。(V)

(7)有中心的密钥管理系统(包括基于 PKI)能够获取或分析出整个系统所有应用的密钥。(X) 注：譬如用户自己生成的密钥？

(8)密钥管理遵循“木桶”原理，即密钥的安全性是由密钥整个阶段中安全性最低的阶段决定的。(V)

(9)密钥的安全长度至少能够抵御穷举攻击。(V)

(10)数字证书是公开的、可复制的，那么数字证书的内容是容易被人修改和伪造。(X)

(11)证书撤销列表(CRL)包含被撤销的证书,随着时间的推移,CRL 会变得越来越长。(X)

(12) 在基于身份的公钥密码体制中，用户公钥的真实性是通过使用用户标识作为公钥来实现的，不需要公钥证书。(V)

(13) 在公钥密码体制中，公钥是公开的，任何人都可以知道的，但公钥的真实性需要有保障的，往往利用公钥证书方法来实现。(V)

(14)只用于数字签名的用户私钥不需要备份，因为即使用户私钥损坏或丢失，用户生成的签名也是能够验证的。(V)

(15)密钥过了有效期，密钥就没有保存的价值了，应该被销毁。(X)

(16)如果使用密钥托管技术，那么任何人都能够得到通信各方之间的通信内容。(X) 注：只有托管中心

(17)Diffie-Hellman 密钥交换协议之所以受到中间人攻击，是因为这个协议没有提供对消息源的认证。(V)

2．选择题

(1)密码系统的安全性取决于密钥的安全性,在密钥管理中下面那个阶段密钥最易受到攻击(C)。

A. 密钥的产生　B. 密钥的使用　C. 密钥的分发　D. 密钥的备份

(2)在通信或数据交换中，直接用于数据加解密的密钥被称为 (A)。

A. 会话密钥　B. 密钥加密密钥　C. 主密钥　D. 私钥

(3)在整个密钥生命周期中，如果用于有效文件保密的密钥使用期结束，那么这个密钥***最有可能***进入下面哪个阶段密钥。(C)

A. 密钥存储　B. 密钥备份　C. 密钥存档　D. 密钥销毁

(4)密钥在其生命周期中处于以下四种不同的状态，每种状态包含若干时期，那么密钥存档时期是密钥处于 (C)。

A. 使用前状态　B. 使用状态　C. 使用后状态　D. 过期状态

(5)密钥在其生命周期中处于以下四种不同的状态，每种状态包含若干时期，那么密钥备份

时期是密钥处于（ B ）。

A. 使用前状态 B. 使用状态 C. 使用后状态 D. 过期状态

(6)下面哪种公开密钥分发方式是一种在线服务器式公钥分发方法。(D)

A.广播式公开密钥分发 B.目录式公开密钥分发

C.带认证的公开密钥 D.公开密钥证书分发

(7) 在本章中，介绍了 Shamir 提出的密钥分发协议，该协议是属于（ C ）。

A. 密钥协商协议 B. 公开密钥分发 C. 无中心密钥分发 D. 有中心密钥分发

(8)下面描述最不正确的是（ C ）。

A. 通信双方可以各自生成自己的密钥。

B. 公钥是公开的，任何人都可以知道的。

C. 安全通信时，使用自己私钥直接加密明文发送给对方。

D. 使用公钥验证数字签名。

(9)下列那一项是 X.509v3 证书的扩展项（ B ）。

A. 证书序列号 B. 密钥用途 C. 证书版本号 D. CA 对证书的签名

(10)在 PKI 应用环境中，使用证书前要验证其有效性，那么验证证书第一步骤是（ A ）。

A. 使用 CA 证书验证证书签名的有效性。

B. 检查证书的有效期，确保该证书没有过期。

C. 检查将使用证书的用途是否符合 CA 在该证书中指定的所有策略限制。

D. 在证书撤销列表中查询证书是否被 CA 撤销。

(11)下列简称中，表示证书撤销列表的是（ C ）。

A. CA B. RA C. CRL D. OCSP

(12)在 PKI 中，关于 RA 的功能，下列说法正确的是（ B ）。

A. 提供目录服务，可以查询用户证书的相关信息。

B. 验证申请者身份。 C. 证书更新 D. 证书发放

(13)当用户收到一个证书时，应当从（ C ）中检查证书是否已经被撤销。

A. CA B. RA C. CRL D. OCSP

(14)数字证书一般要含有很多信息，下列哪个信息在数字证书中不存在。(D)

A. 证书机构 B. 证书持有人 C. 持有人公钥 D. 持有人私钥

(16)下面那种公钥密码体制能根据公钥识别用户的身份。(D)

A. Rabin B. Goldwasser-Micali C. NTRU D. IBE

(17)从某种意义上讲，密钥托管也起到（ C ）的作用。

A.密钥存储 B.密钥使用 C.密钥备份 D.密钥存档

(18)对于一个重要的秘密信息，如主密钥、根私钥等，同样需要多人认可的情况下才可以使用。在密码学上，解决这类问题的技术称为(D)。

A.密钥分发技术 B.密钥协商技术 C.密钥托管技术 D.秘密共享技术

3．填空题

(1)一个三级密钥管理系统，可以将密钥分为三类：_主密钥_、_密钥加密密钥_和_会话密钥_。

(2)典型的密钥交换主要有两种形式：_有密钥交换中心_和_无密钥交换中心_。

(3)密钥在整个生命周期中可分为四个状态阶段：_使用前状态_、_使用状态_、_使用后状态_和_过期状态_。

(4)密钥的生命周期是由若干阶段组成，其中_密钥建立_阶段的安全是最难保障的。

(5)根据密钥传送的途径不同，可以将密钥分发分为_公开信道_和_秘密信道_。

(6)按照密钥分发内容的不同，密钥的分发可以分为_无密钥分发_和_有密钥分发_。

(7)秘密密钥主要用在对称密码体制中以实现通信方之间传送保密信息,按照是否需要可信

第三方来分，秘密密钥分发通常分为有密钥分配中心 和 无密钥分配中心 二种方式。

(8)基于身份的密码体制，利用用户公开信息作为公钥来解决用户公钥的真实性问题，但在实际应用中，这种体制存在以下两方面不足： 用户私钥安全传输问题 ， 大范围应用用户身份信息真实性保障问题 。

(9)典型的密钥协商协议是 Diffie-Hellman 密钥交换协议，但这个协议易受到 中间人攻击 。

(10)密钥托管加密体制的三个主要组成部分为 用户安全成分 、 密钥托管成分 和 数据恢复成分 。

(11)密钥托管分量主要是由 密钥托管代理 、 数据恢复密钥 、 数据恢复业务 和 托管密钥防护 四部分组成。

(12)1979 年 Shamir 提出了一个(t, n)门限方案,该方案是基于 多项式的拉格朗日 公式。

(13)1980 年 Asmuth 和 Bloom 提出了一个（n,t）门限方案，该方案是基于 中国剩余 定理。

4. 术语解释

(1)数字证书：p288

硬件、软件、人员、策略和规程的总和。颁发证书的实体是数字证书认证机构(Certificate Authority,CA),它通过在公钥(数字)证书上签名,可以使任何人确信证书上的公钥及与公钥相对应的私钥为证书所指定的主体所拥有。

(2)证书撤销列表 p289

证书上都会标明一个指定的过期时间,但是在一些特殊情况下,如由于私钥泄露等原因要求用户身份与公钥分离、用户和 CA 的雇佣关系结束、证书中信息修改等,CA 可通过证书撤销机制来缩短其生命周期。此时,CA 发布一个证书撤销列表 (Certificate Revocation List, CRL),列出被认为不能再使用的证书序列号。CA 也可以在 CRL 中加入证书被撤销的理由,还可以加入被认为这种状态改变所适用的起始日期。证书撤销流程通常包含:撤销请求、撤销

(3)密钥分配：P283

密钥分配协议或机制是一种动态密钥建立过程,它使得一个参与方可以建立或获得一个秘密值,并将它安全地传输给其他参与方。根据密钥分配协议中是否存在上层密钥(如密钥加

(4)密钥协商：P285

密钥协商协议或机制指其中两个(或更多的)参与方共同提供信息,推导出一个共享密钥,(理想状态下)任何一方不能预先确定会话密钥的值。它既包含动态密钥协商技术,也包含静

(5)中间人攻击：p286

Diffie-Hellman 密钥交换协议不包含通信双方的身份认证过程，所以，处于通信双方 A 和 B 中间的攻击者能够截获并替换他们之间交互的消息，最终可以监听到他们实际通信的数据，这种攻击被称为中间人攻击。

(6) 密钥托管：P292

密钥托管也称为托管加密，是指为公众和用户提供更好安全通信的同时，也允许授权者（包括政府保密部门、企业专门技术人员和特殊用户等）为了国家、集团的利益，监听某些通信内容并能解密相关密文。密钥托管也叫“密钥恢复”，或者理解为“受信任的第三方”、“数据恢复”和“特殊获取”等含义。

(7) 秘密共享：p294 重要信息，多人认可；n 和 t；小于 t，大于等于 t

发射、金库门打开等。对于一个重要的秘密信息，如主密钥、根私钥等，同样需要多人认可的情况下才可以使用。在密码学上，解决这类问题的技术称为秘密共享技术。它的基本思想是把重要的秘密分成若干份额，分别由若干人保管，必须有足够多的份才能重建这个重要的秘密。

秘密共享技术的基本要求是将秘密 s 分成 n 个份额 $s_1, s_2, \cdots, s_n$：

(1) 已知任意 t 个 s_i 值易于算出 s；

(2) 已知任意 $t-1$ 个或更少个数的 s_i，则不能确定出 s。