第八章 数字签名技术

1．是非判断题

(1) 在数字签名方案中，不仅可以实现消息的不可否认性，而且还能实现消息的完整性、机密性。（ X ）

(2) 在实际应用中，消息的签名过程其实就是签名者使用自己的私钥对消息**加密**的过程，譬如基于 RSA 的数字签名。（ X ） 注：先哈希，后对哈希值处理

(3) 在数字签名中，签名值的长度与被签名消息的长度有关。（ X ）

(4) 数字签名方案往往是非确定性的，即同一人利用同一签名算法对同一消息进行多次签名所得的签名值是不相同的。（ V ）

(5) 在商用数字签名方案中，签名算法和其验证算法都是公开的，消息的签名值包含签名者的私钥，所以，攻击者一旦获取消息的签名值就能获得签名者的私钥。（ X ）

(6) 根据不同的应用需求，提出多种代理签名，但无论那种代理签名的验证算法，其必须用到代理签名者的公钥。（ X ） 注：原始签名者的公钥

(7) 直观上讲，盲签名就像签名者闭着眼睛对消息签名一样，所以，在实际应用中很难涉及到这种签名。（ X ）注：有广泛的应用，譬如电子货币、电子投票等

(8) 在 Elgamal 广播多重数字签名方案中，其签名值的长度与签名者的人数无关。（ V ）

(9) 在不可否认签名方案中，签名的验证必须签名者参与，所以，这种签名方案是有利于签名者。（ V ）

(10) 群签名的不可关联性是指群成员代表多个群成员对不同消息所产生的的群签名，验证者不能判定这些群签名是否由同一个人签发的。（ V ）

(11) 环签名与群签名的主要不同是环签名提供完全的匿名性来保护其成员。（ V ）

(12) 一次数字签名是指签名者只能签署一条消息的签名方案，否则，签名可能被伪造。（ V ）

(13) 失败-停止数字签名其实也是一次性数字签名。（ X ）

(14) 前向安全数字签名能够实现私钥变换了而验证所使用的公钥不变。（ V ）

(15) 变色龙签名其实就是一种指定验证者的数字签名。（ X）

2．选择题

(1) 数字签名技术主要解决了信息安全中存在的（ D ）问题。

A．保密性 B．认证性 C．完整性 D．不可否认性

(2) 通信中如果仅仅使用数字签名技术，则下面哪些安全特性不能被满足。（ A ）

A. 保密性 B. 认证性 C. 完整性 D. 不可否认性

(3) Alice 收到 Bob 发给她一个文件的签名，并要验证这个签名的有效性，那么签名验证算法需要 Alice 选用的密钥是（ C ）。

A. Alice 的公钥 B. Alice 的私钥 C. Bob 的公钥 D. Bob 的私钥

(4) 在普通数字签名中，签名者使用（ B ）进行信息签名。

A. 签名者的公钥 B. 签名者的私钥 C. 签名者的公钥和私钥 D. 验证者的公钥

(5) 签名者无法知道所签消息的具体内容，即使后来签名者见到这个签名时，也不能确定当时签名的行为，这种签名称为（ D ）。

A. 代理签名 B. 群签名 C. 多重签名 D. 盲签名

(6) 签名者把他的签名权授给某个人，这个人代表原始签名者进行签名，这种签名称为（ A ）。

A. 代理签名 B. 群签名 C. 多重签名 D. 盲签名

(7) 针对电子文件或产品的版权保护，防止滥用或盗版，为此，最有可能使用的特殊数字签名是（ D ）。

A. 代理签名　　B. 群签名　　C. 多重签名　　D. 不可否认签名

(8) 下面的特殊数字签名中，那种签名最不可能具备匿名性。（ C ）

A. 门限签名　　B. 环签名　　C. 多重签名　　D. 群签名

(9) 下面的特殊数字签名中，那种签名具有完全匿名性。（ D ）

A. 代理签名　　B. 门限签名　　C. 群签名　　D. 环签名

(10) 下列哪种签名中，签名者的公钥对应多个不同私钥。（ A ）

A. 失败-停止签名　　B. 前向安全签名　　C. 变色龙签名　　D. 同时生效签名

(11) 针对重要文件的签署，需要多人的同意和参与后才能生成该文件的有效数字签名，为此，最有可能使用的特殊数字签名是（ B ）。

A. 代理签名　　B. 门限签名　　C. 环签名　　D. 群签名

(12) 下列哪种签名中，除了签名者以外还有人能够生成有效签名。（ C ）

A. 失败-停止签名　　B. 前向安全签名　　C. 变色龙签名　　D. 同时生效签名

(13) 下面的特殊数字签名中，那种签名最鲜明的特点是其不可转让性。（ C ）

A. 失败-停止签名　　B. 前向安全签名　　C. 变色龙签名　　D. 同时生效签名

(14) 在广域网上，两用户实现网上电子合同的签署，为此，最有可能使用的特殊数字签名是（ D ）。

A. 失败-停止签名　　B. 前向安全签名　　C. 变色龙签名　　D. 同时生效签名

(15) 下面的特殊数字签名中，这种签名能实现根据已有的相关签名能生成一个另外有效签名（ C ）。

A. 代理签名　　B. 前向安全签名　　C. 传递签名　　D. 同时生效签名

3．填空题

(1) 数字签名技术在许多领域中被广泛应用，尤其是在网络环境中用于 不可否认性的应用 。

(2) 在数字签名方案中，不仅可以实现消息的不可否认性，而且还能实现消息的 完整性 、 认证性 。

(3) 数字签名体制也是一种消息认证技术，与消息认证码相比，其主要区别是 采用的密码体制 、 不可否认性 和 效率 、**公开验证性**。

(4) 普通数字签名一般包括三个过程，分别是 密钥生成算法 、 签名算法 和 验证算法 。

(5) 1994 年 12 月美国 NIST 正式颁布了数字签名标准 DSS，它是在 ElGamal 和 Schnorr 数字签名方案 的基础上设计的。（注：p227）

(6) 针对数字签名方案，影响其性能主要因素是 计算量 和 签名值长度 ，而算法的计算量主要与 幂运算 、 哈希函数计算 和 乘积运算 的运算有关。（注：p288）

(7) 根据不同的签名过程，多重数字签名方案可分两类：即 广播多重数字签名 和 有序多重数字签名 。

(8) 群签名除具有一般数字签名的特点外，还有两个特征即 匿名性 、 可跟踪性 。

(9) 盲签名在电子货币、电子投票、电子拍卖等应用中发挥了重要作用，是因为盲签名具有两个重要特点即 匿名性 和 不可跟踪性 。

(10) 代理签名按照原始签名者给代理签名者的授权形式可分为三种： 完全委托的代理签名 、 部分授权的代理签名 、 带授权书的代理签名 。

(11) 不可否认的签名方案不仅包含一个签名算法、一个验证协议，还要包含 一个不可否认算法 。 （p239）

(12)门限数字签名是一种涉及一个组，需要由多个用户来共同进行数字签名的，其具有两个重要的特征：少于 t 个用户不可能共谋得到秘密 s 和 t 个有效分片即可恢复整个秘密 s

(13)一次性数字签名是指签名者只能签署一条消息的签名方案，如果签名者签署消息多于一个，那么签名者的私钥将泄露，攻击者可冒充签名者进行签名。

(14) 失败-停止的签名方案不仅包含一个签名算法、一个验证算法，还要包含“伪造”证明算法。

4．术语解释

(1) 数字签名

(2) 盲签名

(3) 代理签名

(4) 多重签名

(5) 群签名

(6) 不可否认签名