第六章

一、填空：

1. 通信双方 A 和 B 通信，则可能发生哪两种形式的抵赖或欺骗？

2. 数字签名能够抵抗不可否认性攻击的原因是_____

3．基于公钥加密的数字签名方式中，加密的消息应该是_____

4. 直接方式的数字签名的公共弱点是_____

5. 在具有仲裁方式的数字签名中，以下方式可以提供消息的保密性、_____、_____

① X→A：$ID_X \| E_{SKX}[ID_X \| E_{PKY}[E_{SKX}[M]]]$

② A→Y：$E_{SKA}[ID_X \| E_{PKY}[E_{SKX}[M]] \| T]$

6. 在如下有仲裁签名过程中如下： 消息①中的两个 *IDx* 的作用_____

① X→A：$ID_X \| E_{SKX}[ID_X \| E_{PKY}[E_{SKX}[M]]]$

② A→Y：$E_{SKA}[ID_X \| E_{PKY}[E_{SKX}[M]] \| T]$

二、选择：每一项有 1 个或多个选项是正确的

1. 为防止通信双方之间互相抵赖，可采用以下哪种技术进行认证?（ ）

A. MAC B. HMAC C. 先 hash 再加密， D. 数字签名

2. 数字签名可以提供的安全属性有_____

A. 保密性 B. 认证性 C. 完整性 D.不可否认性

3. DSA 使用的散列算法是：_____ A．MD4 B．SHA-1 C．MD5 D．SHA-3

4. 假设发方 A 的密钥对为(*pka*, *ska*)，收方 B 的密钥对为(*pkb*, *skb*)，下面哪一种签名能够防止签名的收方假冒攻击_____

A. m||Sig_{ska}(H(m)) B. m||ID_B||Sig_{ska}(H(m)) C. E_{pkb}(m||Sig_{ska}(H(m))) D. m||Sig_{ska}(H(m||ID_B))

三、判断：(正确的划"√"，错误的划"×"，以下同)

1. 数字签名的验证可由第三方来完成 （ ）

2. 基于对称加密算法可以实现对消息的数字签名 ( )

3. GQ 签名体制是基于有限域上离散对数困难问题构建的的 ( )

四、简答与计算：

1. 试描述 RSA 签名算法的体制参数、签名算法和验证算法?

2. 试述 DSA 数字签名算法，包括密钥产生、签名算法和验证算法，并给出验证过程正确性证明

3. 已知一离散对数签名的密钥产生和签名算法，试给出验证方程，并证明其正确性。

4. 已知 schnorr 签名的密钥产生和签名算法，试给出验证方程，并证明其正确性。

5. 已知 Guillou-Quisquater 签名体制的密钥产生和签名算法，试给出验证方程，并证明其正确性。

五、证明题：

1.试证 DSA 签名中两次使用相同的会话密钥 k，是不安全的

2.试分析以下构造完成了 ElGamal 签名的一个伪造

伪造 1：随机选择 e，令 $r=g^e y \bmod p$, $s=-r$,则(r, s)是消息 $m=es$ 的签名，其中(x,y)是签名者的公私钥对；

伪造 2：随机选择 e,v，令 $r=g^e y^v \bmod p$, $s=-rv^{-1} \bmod p-1$，则(r, s)是消息 $m=es$ 的签名，其中(x,y)是签名者的公私钥对。

3 试证 ElGamal 签名中两次使用相同的会话密钥 k，则不安全的。