《网络安全技术》作业

第三章 消息认证

3-1. 针对安全散列函数的三个安全性质：性质 4（抗原像攻击）、性质 5（抗弱碰撞性）和性质 6（抗强碰撞性）请分别给出一个安全应用场景说明该安全性的必要性。

3-2. 请比较并说明消息认证码 MAC 和数字签名 DS 的相同点和区别。现有如下前提条件：假如 Mary 可以看到 Alice 发送给 Bob 的所有消息以及 Bob 发回给 Alice 的所有消息。除了数字签名的公钥，Mary 不知道其他的密钥。请分别说明在如下场景(1)-(3)中，（i）数字签名（ii）消息认证码是否以及如何抵御攻击的。其中，H(x)分别由数字签名或消息认证码计算得到。

(1)（消息完整性）Alice 将消息 x=“transfer 10000 yuan to Tom”以明文的方式，加上 H(x)一起发给 Bob。Mary 截获上述内容，并将“Tom”替换为“Mary”，Bob 能否检测到？请说明理由

(2)（发送者认证，同时第三方存在欺骗行为）Mary 声称给 Bob 发送了消息 x，并附带有效的数字签名 H(x),但 Alice 声称她也发送了上述内容。Bob 能否区分究竟是哪种情况？请说明理由

(3)（认证中 Bob 存在欺骗行为）Bob 声称收到了 Alice 发来的消息 x(x=“transfer 10000 yuan to Tom”),并附带有效的数字签名 H(x)，但 Alice 声称她没有发送上述内容。Alice 能否证实是哪种情况？请说明理由

3-3. 已知 DSS 是美国 NIST 制定的公钥数字签名标准，其签名过程如图 1 所示。

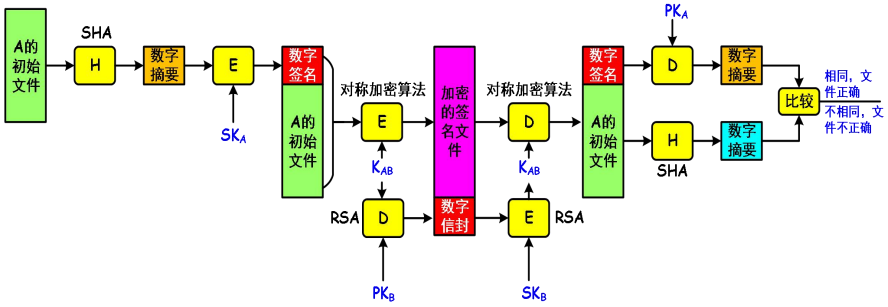

图 1：DSS 数字签名过程

其中： K_{AB}=AB 之间的共享密钥

PK_A/PK_B=用户 A/B 的公钥

SK_A/SK_B=用户 A/B 的私钥

E=加密算法

D=解密算法

H=散列函数

问题：(1)数字签名的作用是什么？图中 SK_A 和 PK_A 是否可以对调？请说明理由。

(2)数字信封的作用是什么？图 1 中 SK_B 和 PK_B 是否可以对调？请说明理由。

(3)请分析说明该标准提供的安全服务有哪些（提示：考虑机密性、完整性、源认证、不可否认等）？请说明理由。

(4)该方案是否存在安全风险？如果有，请进行说明。