**第 4 章 身份认证课后作业**

一、填空题

1、公钥密码体制由明文、加密算法、公钥、私钥、密文、解密算法六部分组成。

2、对付重放攻击的方法有：\_\_\_序列号\_\_\_\_，\_\_时间戳\_\_\_\_，\_\_挑战/应答\_\_\_\_。

3、基于生理特征的身份认证技术中，生理特征必须具有如下特性：

\_普遍性\_\_\_\_，\_\_唯一性\_\_，

\_\_可测量性\_\_，\_\_稳定性\_\_，\_安全性\_\_\_。

二、选择题

1、下面关于公钥密码技术的说法正确的是： （A ）

A. 公钥密码技术包括公钥和私钥； B. 公钥密码比对称密码更安全；

C. 公钥密码完全可以替代对称密码； D. 与对称密码相比，公钥密码实现

密钥分配更加容易。

2、数字签名的特征不包括： ( D)

A. 依赖性；

B. 可保存； C. 抗伪造； D. 挑战/应答

3、下列关于数字签名的说法正确的是： （C ）

A. 数字签名用于保证消息的私密性；

B. 数字签名的有效性不依赖于签名者的私钥安全性；

C. 数字签名可以保证消息的完整性；

D. 数字签名的有效性不依赖于签名者的公钥安全性。

4、下面关于公钥密码技术的说法错误的是： （BCD ）

A. 公钥密码技术包括公钥和私钥； B. 公钥密码比对称密码更安全；

C. 公钥密码完全可以替代对称密码； D. 与对称密码相比，公钥密码实现

密钥分配更加容易。

5、对称密码学可以实现的功能包括： （ AB）

A. 私密性；

B. 完整性； C. 互易性；

D. 消息认证

三、简答题

1. 请简述使用序列号抵抗重放攻击的基本思路，并说明其存在的问题。

服务器端和客户端约定一个序列号生成算法（保证全局唯一性），客户端每次请求时都需要携带请求序列号。服务器端接到请求时，先验证序列号是否合法，不合法直接拒绝。否则查看缓存中是否已经存在过该序列号，若已经存在，表明该请求已经被处理，不允许再次调用。本次处理完毕，将请求序列号缓存。这样可以保证一个序列号对应的请求只会被处理一次，相对比较安全地杜绝了重放攻击。

问题：实现相对复杂，客户端序列号生成算法存在被破解的风险。

1. 请简述对称密码算法作为身份认证的问题。

问题：对称加密算法是通信双方所持有，接收方通过验证发送方是否持有该密钥来验证发送发的身份，因为对称密钥无法唯一标识用户的身份，无法作为验证用户身份的依据。

1. 什么是单向认证协议？什么是双向认证协议？

单向认证协议：接收方通过验证发送方或者仲裁者的签名结果，来验证发送者的身份；

双向认证协议：通信过程中需要相互认证通信参与方的身份的通信过程即为双向认证，双向认证协议可以使通信双方在确认对方身份的基础上交换会话密钥。

4.公钥密码技术满足的要求

从这三个方面说明：密钥的长度；破解密文的计算量；破解密文的复杂度