一、填空题

1、公钥密码体制由**公钥**，**私钥**，**明文**，**密文**，**加密算法**，**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**，**应答/挑战**。

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**，**安全性**，**稳定性**。

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**）**ABD**

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。

**首先通信双方需要提前约定好一个一致的序列号生成算法。在每次通信时发送方需要附加上使用这一算法生成的序列号，同时更新自己缓存中的序列号；接收方收到后先使用相同算法对消息中的序列号进行验证，确认序列号是否合法，并且查找缓存确认不是先前已收到或发送过的。若不合法或已缓存中已存在，则拒绝通信请求；若合法且第一次收到，则建立起通信，并将该序列号存入缓存。在下一次通信时重复上述过程。**

**存在的问题是：依赖序列号生成算法的保密性，若序列号算法被破解且某次通信中的序列号被获取，则无法抵御攻击。**

2. 请简述对称密码算法作为身份认证的问题。

**密钥协商的过程中如何把密钥安全地传输给对方是难点；对称密钥不具有不可抵赖性：比如A、B持有一对对称密钥，A向B发送过消息m，但之后A可以否认自己发送过消息m而声称是B发送的，而这是无法验证的，即A、B的身份不能由对称密码来分辨。**

**所以对称密码体制不能唯一标识用户身份，故不能用于身份认证。**

3、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。**