第四章 报文摘要算法（第四小组）

一、单项选择

**1、以下哪一项是报文摘要算法特点**（C）？

A、碰撞性 B、低灵敏性 C、单向性 D、不易于实现

P85页最上

**2、报文摘要算法的（A）的特点是用报文摘要实现完整性检测的前提？**  
A、抗碰撞性 B、易于实现 C、单向性 D、高灵敏度

P85页上

判断题

1. PKI包括整数的生成、更新、撤销和交叉认证机制。（√）

P95页下

1. 利用报文摘要算法生成的报文摘要的目的是对传输数据进行加密，防止数据被窃听（×）

P84页下

解析：报文摘要是用来保证数据的完整性的。传输的数据一旦被修改，那么计算出来的摘要就不同，只要对比两次摘要就可以确定数据是否被修改过。因此其目的是为了防止发送的报文被篡改。

二、名词解释

**1、请简要解释什么是PKI技术？**

PKI提供了管理、控制证书全过程的方案，包括证书的生成、更新、撤销和交叉认证机制。是CA认证、数字证书、数字签名以及相关安全应用组件的模块的集合。

P95页下

**2.请简述在计算机网络中，数字签名是什么？**

数字签名（Digital Signature，DS）是某个报文的附加信息，该附加信息一是能证明签名者的真实性，二是能够证明签名者对该报文的确认。使用了公钥领域的技术实现，用于鉴别数字信息的方法。数字签名兼具可确认性和不可否认性。

P93页中

简述题

**1、请简述数字签名特征**

1. 接收者能够核实发送者对报文的数字签名；
2. 发送者事后无法否认对报文的数字签名；
3. 接收者无法伪造发送者对报文的数字签名。

P93页中

**2、简述报文摘要算法的特点**

1. 能够作用于任意长度的报文
2. 产生有限位数的标识信息
3. 易于实现
4. 具有单向性
5. 具有抗碰撞性
6. 具有高灵敏度

P84页下

**3.论述数字签名主要过程**

1. 数字签名主要经过以下几个过程。
2. 信息发送者使用一单向Hash函数对信息生成信息摘要。
3. 信息发送者使用自己的私钥签名信息摘要。
4. 信息发送者把信息本身和已签名的信息摘要一起发送出去。
5. 信息接收者通过使用与信息发送者使用的同一个单向Hash函数对接收的信息本身生成新的信息摘要,再使用信息发送者的公钥对信息摘要进行验证,以确认信息发送者的身份和信息是否被修改过。

P93页下图所示