No: Date:

1、阐述哈希函数的概念和构造方法

哈希函数，是一种能把任意长度的输入通过特定算法变换成固定长度输出的函数。其输出称为对于输入的哈希值、散列值、消息摘要或数字指纹。

构造方法：①抗弱碰撞性：给定x，找到 y≠x 使 H(x)=H(y) 在计算上不可行。②抗强碰撞性：找到任意的两个数据对 (x,y) y≠x，使 H(x)=H(y) 在计算上不可行。

2、完善 MD5算法的详细步骤。

①首先对消息M进行填充，使其位长对512求余的结果等于448，即 Len(M) mod 512 = 448

②初始化哈希值：在MD5算法中有4个32位链接变量，分别为A、B、C、D，它们的初始值被称为幻数或魔术数。

③计算哈希值，对将填充后的消息以512位为单位进行划分块，每块再以32位为单位划分分组。

(2)每块可分16个分组，即 M_{i0}、M_{i1}、…、M_{i15}，取决于消息长度

(3)每块进行4轮计算，每轮有16次非线性变换。

(4)完成4轮循环运算后，将A、B、C、D分别加上a、b、c、d，即 A=A+a，B=B+b、C=C+C、D=D+d

(5)加载下一个512位数据块继续运行算法，最后输出的A、B、C和D的级联就是哈希值。

3、阐述消息认证的主要方法和特点。

①消息加密：以消息整体为对象进行加密，并以加密后的密文作为认证标识。

②消息认证码：一个公开函数，加上一个密钥产生一个固定长度的值，并以此作为认证标识。

③散列函数：一个公开函数，能够将任意长度的消息映射到一个固定长度的散列值，以此作为认证标识。

NOTEBOOK

4、阐述数字签名原理，并举例说明。

①唯一性：非对称密钥体制中私钥只有密钥发布者拥有，其他均不可能拥有；报文摘要也同样唯一，即一个报文只会得到唯一的摘要。

②敏感性：报文哪怕同个修改，其摘要均会出现变化。

③快速性：报文摘要的获得具有较快的速度，可以满足对实时性要求较高的场合。

5、阐述身份认证的概念，并总结不同认证方法的特点。

身份认证是对用户宣称的身份标识的有效性进行校验和测试的过程。

①口令认证：使用帐号和密码。

②生物鉴别方法：面部、指纹、虹膜、声音等特征。

③可信计算基：鉴别到相关的认证机制。