1. **阐述哈希函数的概念和构造方法**

答：概念：哈希（Hash，也称为散列、杂凑）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。

构造哈希函数的方法：

\*直接寻址法

\*平方取中法

\*折叠法

\*随机数法

\*除留余数法

常用的构造算法：

1. MD4（Message Digest，消息摘要） 是 MIT 的 Ronald L. Rivest 在1990年提出的一个单向哈希函数，对于不同的输入可产生一个128位的哈希值。基于32位操作数的位操作，适应32位字长。
2. MD5是Rivest 于1991年提出的对MD4的改进版本。MD5比MD4来得复杂，速度也较慢，但更安全，在抗分析和抗差分方面表现更好。
3. SHA（Secure Hash Algorithm）由NSA最早于1993年提出，是以MD4为基础的哈希算法。包括SHA、SHA-1、SHA-2和SHA-3等多个版本。其中，对于SHA版本，输出为128位；SHA-1则为160位；SHA-2则有多种输出长度，包括224位、256位、384位和512位等。
4. **完善MD5算法的详细过程**

答：

1. 数据填充

将输入信息M按顺序进行分组，每512位为一组，同时，最后一组的长度应填充为448位。填充方法如下：

/\*\*

\*当的长度小于448时，在信息后加一个“1”，然后再填充若干个“0”。

\*当的长度大于448时，在信息后加一个“1”，然后再填充若干个“0”。

\*最终使得的长度为512，的长度为448。

\*/

if (.length != 488){

.append(1);

While(.length < 448){

.append(0);

}

if(.length > 448){

for (i=.length; i < 512; i++){

.append(0);

}

for (i=0; i < 448; i++){

.append(0);

}

}

}

最后，将填充前的信息消息长度转换为64位二进制数，若转超过64位，则只保留最后的64位，并将其与M的最后一个分组Mn连接在一起，使所有的分组都为512位。

1. 初始化哈希值

MD5算法的中间结果和最终结果保存在128位的缓冲区中，缓冲区用4个32位的变量表示，这些变量被称为链接变量，初始化：

\*A = 0x01234567

\*B = 0x89abcdef

\*C = 0xfedcba98

\*D = 0x76543210

当设置好这4个变量后，就开始进入算法的4轮循环运算。循环的总次数时信息中512位信息分组的数目。

1. 计算哈希值

分组：将填充后的消息以512位为单位进行划分块，每快再以32位为单位划分分组。

每块可分16个分组，即 Mi0，Mi2，…，Mi15，i取决于消息长度。

每块进行4轮计算（主循环），每轮有16次非线性变换。每轮的非线性变换各不相同，分别为F函数、G函数、H函数和I函数。

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（这里的加法是模232加法）

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。

1. 非线性计算

在每轮进行16次操作，每次操作都会调用一个包含非线性函数的方法。MD5总共定义了四个方法，分别是：

FF（a,b,c,d, Mj,s,ti）表示 a = b+（（a+F（b,c,d）+ Mj+ ti）<<<s）

GG（a,b,c,d, Mj,s,ti）表示 a = b+（（a+G（b,c,d）+ Mj+ ti）<<<s）

HH（a,b,c,d, Mj,s,ti）表示 a = b+（（a+H（b,c,d）+ Mj+ ti）<<<s）

II（a,b,c,d, Mj,s,ti）表示 a = b+（（a+I（b,c,d）+ Mj+ ti）<<<s）

i的取值为1~64，取决于当前循环次数。ti 取值为232×abs（sin（i））的整数部分，i为弧度。

j的取值为当前正在处理的分组号，0~15

MD5按照如下规则进行操作数循环左移：

s表示循环左移s位，s是常量，命名规则(s+方法名+第N个数)

SFF1=7; SFF2=12； SFF3=17; SFF4=22;

SGG1=5; SGG2=9； SGG3=14; SGG4=20;

SHH1=4; SHH2=11, SHH3=16; SHH4=23;

SⅡ1=6; SⅡ2=10, SⅡ3=15; SⅡ4=21;

1. **阐述消息认证的主要方法和特点**

答：主要方法及特点：

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。

\*接收方必须能够识别出所接收消息及信息源的真实性、合法性和正确性。

\*防范收发双方否认发送或接收消息的能力弱。

1. 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。

1. 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。

1. **阐述数字签名原理，并举例说明**

答：数字签名的原理：

1. 数字签名的基础是非对称加密技术和报文摘要技术（哈希）单独以非对称密钥技术也可以形成数字签名的效果，只不过计算能力要求高，不实用。
2. 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。
3. 敏感性：报文的任何修改，其摘要均会出现变化。
4. 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。

举例：RSA数字签名体制：

1. 初始化：

设用户A：取p=13，q=11，e=13

n=p\*q=143，ф（n）=12x10=120，

求解：ed=13d≡1 (mod 120),得：d=37

用户A的公钥：PKA=(143，13)， 私钥：SKA=(143，37)

1. 签名：

设消息m的哈希值h(m)=16,则，计算m的签名：

s=h(m)d(mod n)=1637 mod 143=3

1. 验证：

用户B：se mod n=313 mod 143=16

h(m)(mod n)=16 mod 143=16签名有效。

**5、阐述身份认证的概念，并总结不同认证方法的特点**

答：身份认证的概念：

（1）标识

\*用户向系统表明身份

\*系统可以识别的用户的内部名称：用户名、智能卡、登录ID

\*具有唯一性、不能被伪造

（2）认证（鉴别）

\*对用户宣称的身份标识的有效性进行校验和测试的过程。

（3）方法

\*口令——帐号、密码

\*密码验证——公钥基础设施（Public Key Infrastructure，PKI）

\*生物鉴别方法——面部、指纹、虹膜、声音等特征

\*可信计算基——与鉴别相关的认证机制

不同认证方法的特点：

1. 口令——帐号、密码

优点：简单易用

缺点：安全性较低

1. 密码验证——公钥基础设施

优点：相对传统的口令验证技术，有效保证了用户身份的安全性

缺点：如果客户端与服务器端的时间或次数不能保持良好的同步，存在合法用户无法登录的现象

1. 生物鉴别方法——面部、指纹、虹膜、声音等特征

优点：生物特征很难被模仿，安全性高

缺点：生物特征认证系统的成本相对更高

1. 可信计算基——与鉴别相关的认证机制

优点：方式灵活高效，可互相验证

缺点：局限于客户端与服务器，密钥管理相关的问题