**# 1.什么是对称加密，有哪些常用算法，有哪些运行模式**

采用``单钥``密码系统的加密方法，同一个密钥可以同时用作信息的加密和解密，这种加密方法称为对称加密，也称为单密钥加密。

DES、3DES、AES。

ECB（电码本模式）、CFB（密码反馈模式）、OFB（输出反馈模式）、CBC（密码分组链接模式）、CTR（counter计算器模式）。

**# 2.什么是非对称加密，有哪些常用算法，给出任意一个非对称加密算法的密钥生成过程和加密过程**

使用两个密钥，加密公开密钥，解密用私有密钥。

RSA、Elgamal、D-H、ECC（椭圆曲线加密算法）。

RSA：

**# 3.什么是哈希函数，有哪些常用算法**

哈希函数（Hash Function），也称为散列函数，给定一个输入x，它会算出相应的输出H(x)。哈希函数的主要特征是：

*>输入x可以是``任意``长度的字符串*

出结果即H(x)的长度是``固定``的

常用算法:MD4,MD5,SHA-1,SHA-2.

**# 4.什么是hmac算法，有什么用处**

HMAC是密钥相关的哈希运算消息认证码，HMAC运算利用``哈希算法``，以一个``密钥``和一个``消息``为输入，生成一个``消息摘要``作为输出。

``用处``：

（1）验证TPM接受的授权``数据``和认证数据；

（2）确认TPM接受到的命令请求是已授权的``请求``，并且，命令在传送的过程中没有被改动过。

**# 5.什么是数字签名，有哪些常用算法，给出任意一个数字签名算法的密钥生成过程和签名过程**

也称签名方案，是以``电子形式存储``的消息签名的方法，包括``签名算法``和``验证算法``。发送发使用唯一的私钥进行签名，接收方通过公开的验证算法对签名进行确认。

RSA、Elgamal、Schnorr、DSA（数字签名算法）。

RSA：私钥签名，公钥认证。

**# 6.什么是DH协议，什么是中间人攻击？**

Diffie和Hellman开发的一种``密钥协商协议``，它可以让双方在完全没有任何对方预知信息的条件下，通过``不安全``的信道``交换密钥``。

中间人攻击：

攻击者与通讯的``两端分别``建立独立的联系，并交换其所收到的数据，使通讯的两端认为他们正在通过一个``私密``的连接与对方``直接对话``，但事实上整个会话都被攻击者``完全控制``。

**# 7.椭圆曲线密码常用的参数有哪些，有什么含义**

p、G、a、b、n、h。

有限域参数：p(或者其它)

方程参数：a, b

生成元参数：P(有时用G表示)

阶数参数：n（例如上例中28个点，xP中的x取值为{0,…,27}，点的个数称为阶数）

协因子参数h：椭圆曲线群总点数与n的比值