1. 对称与非对称密码的区别与联系有哪些？

对称密码是指双方共享一个密钥，并使用相同的加密方法和解密方法。

非对称密码是指双方使用不同的密钥：一个公钥和一个私钥。---4分

对称加密算法的优点：加密安全快速，密钥短。

存在一些缺点：无法解决密钥分配问题，密钥个数多，对对方的欺骗没有防御机制。

非对称密码的优点：可以解决密钥分配问题，能够提供消息验证，完整性和不可否认等安全性

---4分

非对称密码的缺点：加密速度慢，密钥长。

联系：在安全系统中，常常同时需要对称密码和非对称密码算法，两者相结合使用，可以有效的解决安全问题。---2分

简述哈希函数的属性以及作用

哈希函数的属性：机密性、完整性、认证性

应用：

文件、软件的完整性检验

消息认证码（检测并防止消息在传输中的错误、篡改以及伪装）

数字签名

伪随机生成器（保证随机数不可预测性）

基于口令的加密（原理是将口令和盐混合后计算散列值，作为加密的密钥，可预防口令猜测攻击）

公钥密码提供的安全服务：

机密性，认证性，完整性，不可否认性