计算机网络的通信面临两大类威胁：被动攻击和主动攻击。

被动攻击：指攻击者从网络上窃听他人的通信内容。通常把这类攻击成为截取。

主动攻击：通常有篡改，恶意程序，拒绝服务方式。

篡改：攻击者故意篡改网络上传送的报文。这里也包括彻底中断传送的报文，甚至是把完全伪造的报文传送给接收方。这种攻击方式有时也称为更改报文流。

恶意程序：恶意程序种类繁多，对网络安全威胁较大的主要有：计算机病毒，计算机蠕虫，特洛伊木马，逻辑炸弹，后门入侵，流氓软件等。

拒绝服务：指攻击者向互联网上的某个服务器不停地发送大量分组，使该服务器无法提供正常服务，甚至完全瘫痪。

两类密码体制

对称密钥密码体制：加密密钥和解密密钥使用相同的密码体制。

对称密钥密码体制中的数据加密标准DES：DES是一种分组密码。在加密前，先对整个的明文进行分组。每一个组为64位长的二进制数据。然后对每一个64位二进制数据进行加密处理，产生一组64位密文数据，最后将各组密文串接起来，即得出整个的密文。使用的密钥占有64位（实际密钥长度为56位，外加8位用于奇偶校验）。

对称密钥密码体制中的高级加密标准AES：AES是在DES上发展而来的，因为DES的密钥长度较小（56位），不适合当今数据加密安全性的要求，而AES能支持的密钥长度可以为128,192,256位(也即16,24,32个字节)。

公钥密码体制：使用不同的加密密钥与解密密钥。

在公钥密码体制中，加密密钥（公钥）是向公众公开的，而解密密钥（私钥）则是需要保密的。加密算法和解密算法也都是公开的。

RSA体制：请参考公钥密码体制RSA算法原理。

公开密钥和对称密钥的区别：在使用对称密钥时，由于双方使用同样的密钥，因此在通信信道上可以进行一对一的双向保密通信，每一方既可用此密钥加密明文，并发送给对方，也可以接收密文，用同一密钥对密文解密。这种保密通信仅限于持有此密钥的双方（如再有第三方就不保密了）。在使用公钥时，在通信信道上可以是多对一的单向保密通信。多方持有公钥，一方持有私钥。

注意：任何加密方法的安全性取决于密钥的长度，以及攻破密文所需的计算量，而不是简单地取决于加密的体制（公钥密码体制或传统加密体制）。公钥密码体制并没有使传统密码体制被弃用，因为目前公钥加密算法的开销较大，在可见的将来还不会放弃传统加密方法。

数字签名

数字签名主要是能够