6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实现三点功能：

接受者能够核实发送者对报文的签名。也就是说，接受者能确信该报文的确是发送者发送的。其他人无法伪造对报文的签名。这叫做报文鉴别。

接受者确信所收到的数据和发送者发送的完全一样而没有被篡改过。这叫做报文的完整性。

发送者事后不能抵赖对报文的签名。这叫做不可否认。

鉴别

鉴别是要验证通信的对方的确是自己要所通信的对象，而不是其他的冒充者，并且所传送的报文是完整的，没有被他人篡改过。

鉴别分为报文鉴别和实体鉴别：

报文鉴别：鉴别所收到的报文的确是报文的发送者所发送的，而不是其他人伪造的或篡改的。

实体鉴别：仅仅鉴别发送报文的实体。

报文鉴别

密码散列函数

特点：

散列函数的输入长度可以很长，但其输出长度则是固定的，并且较短。散列函数的输出叫做散列值，或更简单些，称为散列。

不同的散列值肯定对应于不同的输入，但不同的输入却可能得出相同的散列值。这就是说，散列函数的输入和输出并非一一对应的，而是多对一的。

在密码学中使用的散列函数称为密码散列函数，其最重要的特点就是：要找到两个不同的报文，他们具有同样的密码散列函数输出，在计算上是不可行的。也就是说，密码散列函数实际上是一种单向函数。

实用的密码散列函数MD5 和 SHA-1

MD5：MD是Message Digest 的缩写，意思是报文摘要。MD5 是报文摘要的第5个版本。

在2004年，中国学者王小云证明可以用系统的方法找出一对报文，这对报文具有相同的 MD5 报文摘要，并且只需要15分钟或不到1小时。所以MD5 最终被另一种叫做安全散列算法 SHA（Secure Hash Alogorithm） 的标准所取代。

MD5 算法的大致过程：

先把任意长的报文按模2^64计算其余数（64位），追加在报文的后面。

在报文和余数之间填充1～512位，使得填充后的总长度是512 的整数倍。填充的首位是1，后面都是0。

把追加和填充后的报文分割为一个个512位的数据块，每个512位的报文数据再分成4个128位的数据块一次送到不同的散列函数进行4轮计算。每一轮又都按32位的小数据块进行复杂的运算。一直到最后计算出 MD5 报文摘要代码（128位）。

这样得出的 MD5 报文摘要代码中的每一位都与原来的报文中的每一位有关。由此可见，像MD5这样的密码散列函数实际上已是个相当负责的算法，而不是简单的函数了。

SHA 与 MD5 相似，但码长位 160位（比MD5的128位多了25%）。SHA 也是用512位长的数据块经过复杂的运算得出的。SHA 比 MD5 更安全，但计算起来却比 MD5 要慢些。

实体鉴别

实体鉴别是在系统介入的全部持续时间内对和自己通信的对方实体只需要验证一次。

由于实体鉴别容易被攻击者截取而不安全，所以这里不对实体鉴别做详细介绍。

密钥分配

对称密钥的分配

对称密钥分配方式是设立密钥分配中心 KDC （Key Distribution Center）。KDC 是大家都信任的机构，其任务就是给需要进行密钥通信的用户临时分配一个会话密钥（仅使用一次）。

公钥的分配

认证中心 CA（Certification Authority），一般由政府出资建立的。每个实体都有 CA 发来的证书（certificate），里面有公钥及其拥有者的标识信息（人名或IP地址）。此证书被CA 进行了数字签名。任何用户都可以从可信的地方（如代表政府的报纸）获得认证中心CA的公钥，此公钥用来验证某个公钥是否为某个实体所拥有（通过向CA查询）。有的大公司（如Netscape）也提供认证中心服务。

为了使CA的证书具有统一的格式，ITU-T制定了X.509协议标准，用来描述证书的结构。在X.509中规定要使用ASN.1。IETE 接受了X.509（仅有少量的改动），并在RFC 5280（现在是建议标准）中给出了互联网 X.509公钥基础结构PKI（Public Key Infrastructure）。

互联网使用的安全协议

运输层安全协议

现在广泛使用的两个协议：

安全套接字层 SSL（Secure Socket Layer）

运输层安全 TLS (Transport Layer Security)

SSL 作用在端系统应用层的HTTP和传输层之间，在TCP之上建立起一个安全通道，为通过TCP传输的应用层数据提供安全保障。

TLS 是IETF在 SSL 3.0 的基础上设计的，为所有基于 TCP的网络应用提供安全数据传输服务。

SSL 提供的安全服务可归纳下面三种：

SSL 服务器鉴别，允许用户证实服务器的身份。支持SSL的客户端通过验证来自服务器的证书，来鉴别服务器的真实身份并获得服务器的公钥。
SSL 客户鉴别， SSL 的可选安全服务，允许服务器证实客户的身份。

加密的 SSL 会话，对客户和服务器间发送的所有报文进行加密，并检测报文是否被篡改。