密码主要功能：

1. 机密性：指保证信息不泄露给非授权的用户或实体，确保存储的信息和传输的信息仅能被授权的各方得到，而非授权用户即使得到信息也无法知晓信息内容，不能使用。
2. 完整性：是指信息未经授权不能进行改变的特征，维护信息的一致性，即信息在生成、传输、存储和使用过程中不应发生人为或非人为的非授权篡改(插入、替换、删除、重排序等)，如果发生，能够及时发现。
3. 认证性：是指确保一个信息的来源或源本身被正确地标识，同时确保该标识的真实性，分为实体认证和消息认证。
   消息认证：向接收方保证消息确实来自于它所宣称的源；
   实体认证：参与信息处理的实体是可信的，即每个实体的确是它所宣称的那个实体，使得任何其它实体不能假冒这个实体。
4. 不可否认性：是防止发送方或接收方抵赖所传输的信息，要求无论发送方还是接收方都不能抵赖所进行的行为。因此，当发送一个信息时，接收方能证实该信息的确是由所宣称的发送方发来的；当接收方收到一个信息时，发送方能够证实该信息的确送到了指定的接收方。

信息安全：指信息网络的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露、否认等，系统连续可靠正常地运行，信息服务不中断。
信息安全的理论基础是密码学，根本解决，密码学理论

对称密码技术——分组密码和序列密码——机密性；
消息认证码——完整性，认证性；
数字签名技术——完整性，认证性，不可否认性；

1949 年 Shannon 发表题为《保密系统的通信理论》
1976 年后，美国数据加密标准（DES）的公布使密码学的研究公开，密码学得到了迅速发展。
1976 年，Diffe 和 Hellman 发表了《密码学的新方向》，提出了一种新的密码设计思想，从而开创了公钥密码学的新纪元。

置换密码
置换密码的特点是保持明文的所有字符不变，只是利用置换打乱了明文字符的位置和次序。
列置换密码和周期置换密码

使用密码设备必备四要素：安全、性能、成本、方便。

一个密码体制通常由以下 5 个部分构成：
(1) 明文空间 M，即全体明文的集合；
(2) 密文空间 C，即全体密文的集合；
(3) 密钥空间 K，全体密钥的集合；
(4) 加密器或加密算法 E，由加密密钥控制的加密变换的集合，即 Ek（m）=c；
(5) 解密器或解密算法 D，由解密密钥控制的解密变换的集合，即 Dk（c）=m。

密码体制的基本要求：

1. 密码体制既易于实现又便于使用，主要是指加密函数和解密函数都可以高效地计算。

2. 密码体制的安全性是依赖密钥的安全性，密码算法是公开的。
3. 密码算法安全强度高，也就是说，密码分析者除了穷举搜索攻击外再找不到更好的攻击方法。
4. 密钥空间应足够大，使得试图通过穷举密钥空间进行搜索的方式在计算上不可行。

密码算法公开的意义：
有利于增强密码算法的安全性；
有利于密码技术的推广应用；
有利于增加用户使用的信心；
有利于密码技术的发展。

熵的性质：H(X,Y)=H(Y)+H(X|Y)=H(X)+H(Y|X)
H(K|C)=H(K)+H(P)-H(C)

密码攻击类型
惟密文攻击(Ciphertext Only Attack)（仅仅搭线窃听）
密码分析者除了拥有截获的密文外（密码算法是公开的，以下同），没有其它可以利用的信息。
已知明文攻击(Known Plaintext Attack)（有内奸）
密码分析者不仅掌握了相当数量的密文，还有一些已知的明-密文对可供利用。
选择明文攻击(Chosen Plaintext Attack)（暂时控制加密机）
密码分析者不仅能够获得一定数量的明-密文对，还可以选择任何明文并在使用同一未知密钥的情况下能得到相应的密文。
选择密文攻击(Chosen Ciphertext Attack)（暂时控制解密机）
密码分析者能选择不同被加密的密文，并还可得到对应的明文，密码分析者的任务是推出密钥及其它密文对应的明文。
选择文本攻击(Chosen Text Attack)（暂时控制加密机和解密机）
它是选择明文攻击和选择密文攻击的组合，即密码分析者在掌握密码算法的前提下，不仅能够选择明文并得到对应的密文，而且还能选择密文得到对应的明文。

攻击密码体制的常用方法
穷举攻击
统计分析攻击
数学分析攻击

密码体制安全性：无条件安全性，计算安全性，可证明安全性

分组密码的要求：
分组长度要足够大
密钥量要足够大
密码变换足够复杂
加密和解密运算简单
无数据扩展或压缩

分组密码的设计思想（扩散和混乱）

扩散：是指要将算法设计成明文每一比特的变化尽可能多地影响到输出密文序列的变化，以便隐蔽明文的统计特性。形象地称为**雪崩效应**。扩散的另一层意思是密钥每一位的影响尽可能迅速地扩展到较多的密文比特中去。

混乱：指在加解密变换过程中明文、密钥以及密文之间的关系尽可能地复杂化，以防密码破译者采用解析法(即通过建立并求解一些方程)进行破译攻击。分组密码算法应有复杂的非线性因素。

轮函数基本准则：非线性，可逆性，雪崩效应

DES

分组加密算法：明文和密文为 64 位分组长度。密钥长度：56 位

采用混乱和扩散的组合，每个组合先代换后置换，共 16 轮。

互补性会使 DES 在选择明文攻击下所需的工作量减半。

如果给定初始密钥 k，经子密钥产生器产生的各个子密钥都相同，即有 k1=k2=…=k16，则称给定的初始密钥 k 为弱密钥。

若 k 为弱密钥，则对任意的 64bit 信息有：$E_k(E_k(m))=m$ 和 $D_k(D_k(m))=m$。

若给定初始密钥 k，产生的 16 个子密钥只有两种，且每种都出现 8 次，则称 k 为半弱密钥。

半弱密钥的特点是成对出现，且具有下述性质：若k_1和k_2为一对半弱密钥，m为明文组，则有：$E_{k2}(E_{k1}(m))=E_{k1}(E_{k2}(m))=m$。

差分分析：是分析一对给定明文的异或（对应位不同的个数称为差分）与对应密文对的异或之间的统计相关性。

3DES 特点：

优点：1. 密钥长度增加到 112 位或 168 位，克服了 DES 面临的穷举攻击。

2. 相对于 DES，增强了抗差分分析和线性分析等的能力。

3. 由于 DES 已经大规模使用，升级到 3DES 比更新新算法成本小得多。

4. DES 比其它任何加密算法受到的分析时间都长的多，相应地，3DES 抗分析能力更强。

不足：1. 3DES 处理速度较慢。

2. 虽然密钥长度增加了，但明文分组长度没变，与密钥长度的增长不匹配。

AES 分组长度、密钥长度、轮数的关系：

分组长度：128 位

密钥长度，轮数：128，10；192,12；256,14

每轮由四个阶段组成：字节代换、行位移、列混淆、轮密钥加。

DES 是面向比特的运算，AES 是面向字节的运算。

二重 DES 并不像人们相像那样可提高密钥长度到 112 比特，而相当 57 比特。

分组密码的操作模式

ECB：

模式操作简单，主要用于内容较短且随机的报文的加密传递；

相同明文（在相同密钥下）得出相同的密文，即明文中的

重复内容可能将在密文中表现出来，易实现统计分析攻击、分组重放攻击和代换攻击；

链接依赖性：各组的加密都独立于其它分组，可实现并行处理；

错误传播：单个密文分组中有一个或多个比特错误只会影响该分组的解密结果。

CBC(密文分组和明文分组异或得到下一个密文分组)

一种反馈机制在分组密码中的应用，每个密文分组不仅依赖于产生它的明文分组，还依赖于它前面的所有分组；

相同的明文，即使相同的密钥下也会得到不同的密文分组，隐藏了明文的统计特性；

链接依赖性：对于一个正确密文分组的正确解密要求它之前的那个密文分组也正确，不能实现并行处理；

错误传播：密文分组中的一个单比特错误会影响到本组和其后分组的解密，错误传播为两组；

初始化向量 IV 不需要保密，它可以明文形式与密文一起传送。

CTR:

效率高：能够并行处理多块明(密)文，可用来提供像流水线、每个时钟周期的多指令分派等并行特征；

预处理：基本加密算法的执行并不依靠明文或密文的输入，可预先处理，当给出明文或密文时，所需的计算仅是进行一系列的异或运算；

随机访问：密文的第 i 个明文组能够用一种随机访问的方式处理；

简单性：只要求实现加密算法而不要求实现解密算法，像 AES 这类加解密算法不同就更能体现 CTR 的简单性。

CFB:

消息被看作 bit 流，不需要整个数据分组在接受完后才能进
行加解密；

可用于自同步序列密码；

具有 CBC 模式的优点；

对信道错误较敏感且会造成错误传播；

数据加解密的速率降低，其数据率不会太高。

OFB:

OFB 模式是 CFB 模式的一种改进，克服由错误传播带来的问题，但对密文被篡改难于进行检测；

OFB 模式不具有自同步能力，要求系统保持严格的同步，否则难于解密；

初始向量 IV 无需保密，但各条消息必须选用不同的 IV。

总结：

ECB 是最快、最简单的分组密码模式，但它的安全性最弱，一般不推荐使用 ECB 加密消息，但如果是加密随机数据，如密钥，ECB 则是最好的选择。

CBC 适合文件加密，而且有少量错误时不会造成同步失败，是软件加密的最好选择。

CTR 结合 ECB 和 CBC 的优点，最近为人们所重视，在 ATM 网络和 IPSec 中起了重要作用。

CFB 通常是加密字符序列所选择的模式，它也能容忍少量错误扩展，且具有同步恢复功能。

OFB 是在极易出错的环境中选用的模式，但需有高速同步机制。

序列密码属于对称密码体制，又称为流密码。

特点：

1. 加解密运算只是简单的模二加(异或)运算。
2. 密码安全强度主要依赖密钥序列的安全性。

密钥序列产生器(KG)基本要求：

种子密钥 K 的长度足够长，一般应在 128 位以上(抵御穷举攻击)；

密钥序列产生器 KG 生成的密钥序列{ki}具极大周期；

密钥序列{ki}具有均匀的 n-元分布，即在一个周期内，某特定形式的 n-长 bit 串与其求反，两者出现的频数大抵相当；

由密钥序列{ki}提取关于种子密钥 K 的信息在计算上不可行；

雪崩效应。即种子密钥 K 任一位的改变要引起密钥序列{ki}在全貌上的变化；

密钥序列{ki}不可预测的。密文及相应的明文的部分信息，不能确定整个密钥序列{ki} 。

只要选择合适的反馈函数才可使序列的周期达到最大值 2^n-1，周期达到最大值的序列称为 **m 序列**。

m-序列特性：0,1 平衡性：在一个周期内，0、1 出现的次数分别为 $2^{n-1}-1$ 和 2^{n-1}。

游程特性：

在一个周期内，总游程数为 2^{n-1}；对 $1\leqslant i\leqslant n-2$，长为 i 的游程有 2^{n-i-1} 个，且 0、1 游程各半；长为 n-1 的 0 游程一个，长为 n 的 1 游程一个。

非线性序列：为了使密钥流生成器输出的二元序列尽可能随机，应保证其周期尽可能大、线性复杂度和不可预测性尽可能高。

RC4 是 RSA 数据安全公司开发的可变密钥长度的序列密码，是世界上使用最广泛的序列密码之一. 为了保证安全强度，目前的 RC4 至少使用 128 位种子密钥。

序列密码特点：

安全强度取决于密钥序列的随机性；

线性反馈移位寄存器理论上能够产生周期为 2n-1 的伪随机序列，有较理想的数学分析；

为了使密钥流尽可能复杂，其周期尽可能长，复杂度和不可预测尽可能高，常使用多个 LFSR 构造非线性组合系统；

在某些情况下，譬如缓冲不足或必须对收到字符进行逐一处理时，序列密码就显得更加必要和恰当。

在硬件实施上，不需要有很复杂的硬件电路，实时性好，加解密速度快，序列密码比分组密码更有优势。

公钥密码之前：都是基于代换和换位这两个基本方法，建立在字符或位方式的操作上。

公钥密码算法是建立在数学函数基础上的，而不是建立在字符或位方式的操作上的，是以非对称的形式使用加密密钥和解密密钥，这两个密钥的使用对密钥管理、认证等都有着深刻的实际意义。

对称密码缺陷：秘钥分配问题，秘钥管理问题，数字签名问题；

背包算法是第一个公开秘钥算法。

RSA：RSA 虽稍后于 MH 背包公钥系统，但它是到目前为止应用最广的一种公钥密码。RSA 的理论基础是数论的欧拉定理，它的安全性依赖于大整数的素因子分解的困难性。

欧拉定理：若整数 a 和 n 互素，则 $a\equiv 1 \pmod n$

RSA 秘钥长度 1024 位。

ElGamal 公钥密码基于有限域上离散对数问题的公钥密码体制。
基于有限域的离散对数公钥密码又称 ElGamal （厄格玛尔)算法。
ElGamal 算法的安全性依赖于计算有限域上的离散对数。
ElGamal 算法的离散对数问题等同 RSA 的大数分解问题。
ElGamal 算法既可用于数字签名又可用于加密，但更多地应
用在数字签名中。
目前密钥长度 1024 位是安全的。
ECC 安全性能更高（160 位等同 RSA 的 1024 位）
公钥密码学解决了秘钥分发和不可否认问题。
公钥证书较好地解决了公钥的真实性问题。

IBE(基于身份加密)

基于身份的密码系统中，用户的公钥是一些公开的可以唯一确定用户身份的信息，一般这些信息称为用户的身份(ID)。在实际应用中，用户的身份可以是姓名、电话号码、身份证号码、IP 地址、电子邮件地址等作为公钥。用户的私钥通过一个被称作私钥生成器 PKG(Private Key Generator)的可信任第三方进行计算得到。

在这个系统中，用户的公钥是一些公开的身份信息，其他用户不需要在数据库中查找用户的公钥，也不需要对公钥的真实性进行检验。

优点：

公钥的真实性容易实现，大大简化了公钥的管理。

不足：

身份确认本来就是一件复杂的事情，尤其用户数量很大时难以保证。也就是说，IBE 适合应用于用户群小的场合。

可信第三方如何安全地将用户的私钥送到用户的手中。

用户私钥由可信第三方生成和掌握，不具备唯一性，实现不可否认性时易引发争议。

公钥密码的优点(与对称密码相比)

1. 密钥分发简单；
2. 需秘密保存的密钥量减少；
3. 可以实现数字签名和认证的功能。

公钥密码的不足(与对称密码相比)

公钥密码算法比对称密码算法慢；

公钥密码算法提供更多的信息对算法进行攻击，如公钥密码算法对选择明文攻击是脆弱的，尤其明文集比较小时；

有数据扩展；

公钥密码算法一般是建立在对一个特定的数学难题求解上，往往这种困难性只是一种设想。

哈希函数：

单向性，输出长度固定,：数据指纹，实现数据完整性和数字签名。

性质：

输入：消息是任意有限长度。

输出：哈希值是固定长度。

容易计算：对于任意给定的消息，容易计算其哈希值。（正向容易）

单向性：对于给定的哈希值 h，要找到 M 使得 H(M)＝h 在计算上是不可行的。(逆向不可行)

安全性：
抗弱碰撞性：对于给定的消息 M1，要发现另一个消息 M2，满足 H(M1)＝H(M2)在计算上是不可行的。
抗强碰撞性：找任意一对不同的消息 M1，M2 ，使 H(M1)＝H(M2)在计算上是不可行的。
随机性：当一个输入位发生变化时，输出位将发生很大变化。(雪崩效应)。

MD: MD2(1989)、MD4(1990)和 MD5(1991)都产生一个 128 位的信息摘要。
SHA-1 接受任何有限长度的输入消息，并产生长度为 160 比特的 Hash 值。

消息验证的目的：
验证信息的来源是真实的，而不是冒充的，此为消息源认证。
验证消息的完整性，即验证信息在传送或存储过程中是否被修改。
哈希函数分类：
改动检测码 MDC：不带密钥的哈希函数，主要用于消息完整性。
消息认证码 MAC：带密钥的哈希函数，主要用于消息源认证和消息完整性。

HMAC: 算法公式 ： HMAC（K，M）=H（K⊕opad｜H（K⊕ipad｜M））
K—代表认证密码
HMAC 主要应用在身份验证中，它的使用方法是这样的：
(1) 客户端发出登录请求（假设是浏览器的 GET 请求）
(2) 服务器返回一个随机值，并在会话中记录这个随机值
(3) 客户端将该随机值作为密钥，用户密码进行 HMAC 运算，然后提交给服务器
(4) 服务器读取用户数据库中的用户密码和步骤 2 中发送的随机值做与客户端一样的 HMAC 运算，然后与用户发送的结果比较，如果结果一致则验证用户合法
在这个过程中，可能遭到安全攻击的是服务器发送的随机值和用户发送的 HMAC 结果，而对于截获了这两个值的黑客而言这两个值是没有意义的，绝无获取用户密码的可能性，随机值的引入使 HMAC 只在当前会话中有效，大大增强了安全性和实用性。

数字签名与消息认证不同：
数字签名也是一种消息认证技术，它属于非对称密码体制，消息认证码属于对称密码体制，所以消息认证码的处理速度比数字签名快得多。但是，消息认证码无法实现不可否认性。
数字签名的安全要求
签名是可以被验证的接受者能够核实签名者对消息的签名。
签名是不可伪造的
除了签名者，任何人(包括接受者)不能伪造消息的签名。
签名是不可重用的
同一消息不同时刻其签名是有区别的。
签名是不可抵赖的
签名者事后不能抵赖对消息的签名，出现争议时，第三方可解决争端。

数字签名的组成：明文空间，密文空间，秘钥空间，签名算法，验证算法
数字签名常见的实现算法

基于 RSA 的签名算法
基于离散对数的签名算法
基于 ECC 的签名算法

RSA 数字签名算法(初始化)
1. 选取两个大(满足安全要求)素数 p 和 q，两个数长度接近且相差很大，强素数。
2. 计算 n=p*q, $\phi(n)=(p-1)(q-1)$
3. 随机选取整数 e($1<e<\phi(n)$)，满足 gcd(e, $\phi(n)$) = 1
4. 计算 d，满足 $d*e \equiv 1 \pmod{\phi(n)}$
注：n 公开， p 和 q 保密。
e 为公钥，d 为私钥。
签名算法
1.利用一个安全的 Hash 函数 h 来产生消息摘要 h(m)。
2.用签名算法计算签名 $s=Signk(m)\equiv h(m)^d \bmod n$。
验证算法
1.首先利用一个安全的 Hash 函数 h 计算消息摘要 h(m)。
2.用检验等式 $h(m) \bmod n \equiv s^e \bmod n$ 是否成立，若相等签名有效，否则，签名无效。
假如直接对消息进行私钥加密,攻击者获得两个签名后可以伪造 m1*m2 的有效签名 s1*s2(同态性)

Elgamal 签名算法(举例)
初始化：
假设 A 选取素数 $p=19$ ，Zp* 的生成元 $g=2$。选取私钥 $x=15$，计算 $y \equiv g^x \bmod p \equiv 215 \bmod 19 = 12$，则 A 的公钥是(p = 19, g = 2, y = 12)。
签名过程：
设消息 m 的 Hash 值 h(m) = 16，则 A 选取随机数 k = 11，计算 $r \equiv g^k \bmod p \equiv 211 \bmod 19 \equiv 15$，$k^{-1} \bmod (p-1) = 5$。最后计算签名 $s \equiv [h(m)-xr]k^{-1} \bmod (p-1) \equiv 5(16-15\times 15) \bmod 18 = 17$。得到 A 对 m 的签名为(15, 17)。
验证过程：
接受者 B 得到签名(15 , 17)后计算 $y^r r^s \bmod p \equiv \bmod 19 = 5$ ，$g^{h(m)} \bmod p \equiv 216 \bmod 19 = 5$ 。验证等式 $y^r r^s \equiv g^{h(m)} \pmod p$相等，因此 B 接受签名。
Elgamal 签名算法(安全性)
不能泄露随机数 k。
不能使用相同的 k 对两个不同消息进行签名。
签名者多次签名时所选取多个 k 之间无关联。

整个密码系统的安全性并不取决对密码算法的保密，而是由密钥的保密性决定的。解决的核心问题是密钥管理问题,而不是密码算法问题。密钥的管理水平直接决定了密码的应用水平。密钥管理就是在授权各方之间实现密钥关系的建立和维护的一整套技术和程序。密钥管理括密钥的生成、存储、建立(分配和协商)、使用、备份/恢复、更新、撤销/存档/销毁等。

典型的密钥层次结构
主密钥：对应于层次化密钥结构中的最高层次，它是对密钥加密密钥进行加密的密钥，主密

钥应受到严格的保护。
密钥加密密钥：一般是用来对传输的会话密钥进行加密时采用的密钥。密钥加密密钥所保护的对象是实际用来保护通信或文件数据的会话密钥。
会话密钥：在一次通信或数据交换的任务中，用户之间所使用的密钥，是由通信用户之间进行协商得到的。它一般是动态地、仅在需要进行数据加密时产生，并在任务完成后立即进行销毁，也称为数据加密密钥。
密钥的生成一般首先通过密钥生成器借助于某种随机源产生具有较好统计分析特性的序列，以保障生成密钥的随机性和不可预测性.
密钥存储目的是确保密钥的秘密性、真实性以及完整性。
密钥更新情况：密钥有效期结束；密钥的安全受到威胁；通信成员中提出更新密钥。

对称密码其实就一个密钥(即已知一个密钥可推出另一个密钥)，因此，密钥的秘密性、真实性、完整性都必须保护。
公钥的秘密性不用确保，但其真实性、完整性都必须严格保护。
公钥密码体制的私钥的秘密性、真实性、完整性都必须保护。

中间人攻击：
将公共目录中 B 的公钥替换成自己的公钥。
将他认为的 B 的公钥提取出来，而实际上那是 C 的公钥。
现在可以读取 A 送给 B 的加密信息。
将 A 的信息解密并阅读，然后他又用真实的 B 的公钥加密该信息并将加密结果发送给 B。
数字证书实现公钥的真实性。

数字证书也称为公钥证书，是将证书持有者的身份信息和其所拥有的公钥进行绑定的文件。
证书用途：
签名证书：签名证书主要用于对用户信息进行签名，以保证信息的不可否认性。（私钥不需备份）
加密证书：加密证书主要用于对用户传送信息的密钥进行加密，以保证信息的保密性。（私钥需要备份）
CRL：证书撤销列表
在线证书状态协议 OCSP：其目的为了克服基于 CRL 的撤销方案的局限性，为证书状态查询提供即时的最新响应。OCSP 使用证书序列号、CA 名称和公开密钥的散列值作为关键字查询目标的证书。
为防止攻击者得到密钥，必须时常更新密钥，密码系统的强度依赖于密钥分配技术。

密钥分配中心模式（KDC 生成回话密钥）：
前提条件：密钥分配中心与每个用户之间有共享密钥。

1. A 向密钥分配中心 KDC(Key Distribute Center)发出会话密钥请求。请求内容包括 A 与 B 的身份以及一次性随机数 N1。
2. KDC 为 A 的请求发出应答。应答内容包括：一次性会话密钥 Ks、A 的请求、用 B 与 KDC 的共享密钥加密一次性会话密钥 Ks 和 A 的身份，其中应答信息是用 A 与 KDC 的共享密钥加密。
3. A 存储会话密钥 Ks，并向 B 转发用 B 与 KDC 的共享密钥加密的一次性会话密钥 Ks 和 A 的身份。

4. B 使用会话密钥 Ks 加密另一个一次性随机数 N2 ，并将加密结果发送给 A.
5. A 使用会话密钥 Ks 加密 f(N2),并将加密结果发送给 B.

基于公钥密钥分配（会话密钥）：
前提条件：通信双方在 CA 中拥有自己的证书。
1. A 向 B 发出会话密钥请求，请求内容包括 A 的身份、一次性随机数 N1 以及利用 B 的公钥加密一次性会话密钥 Ks。
2. B 使用会话密钥 Ks 加密一次性随机数 N1 ，并将加密结果发送给 A。
3. A 使用会话密钥 Ks 加密 f(N1),并将加密结果发送给 B。

密钥协商是保密通信双方（或更多方）通过公开信道的通信来共同形成秘密密钥的过程。密钥协商的结果是：参与协商的双方（或更多方）都将得到相同的密钥，同时，所得到的密钥对于其他任何方都是不可知的。

密码算法是密码协议的最基本单元，主要包含四个方面：
公钥密码算法，在分布式环境中实现高效密钥分发和认证；
对称密码算法，使用高效手段实现信息的保密性；
散列函数，实现协议中消息的完整性；
随机数生成器，为每个参加者提供随机数,实现唯一性和不可预测性。

零知识证明实际上一种密码协议,该协议的一方称为证明者(Prover) ， 通常用 P 表示， 协议的另一方是验证者(Verifier)，一般用 V 表示。零知识证明是指 P 试图使 V 相信某个论断是正确的，但却不向 V 提供任何有用的信息，或者说在 P 论证的过程中 V 得不到任何有用的信息。也就是说，零知识证明除了证明证明者论断的正确性外不泄露任何其它信息或知识，或者说零知识证明是那种除了论证论题的有效性外不产生任何知识的证明。

盲签名：签名要求签名者能够在不知道被签名文件内容的情况下对消息进行签名。另外，即使签名者在以后看到了被签名的消息及其签名,签名者也不能判断出这个签名是他何时为谁生成的。（隐私性，不可追踪性）

SSL: SSL（Secure Socket Layer，即安全套接层）协议是网景（Netscape）公司于1994年最先提出来的。SSL被设计成使用TCP来提供一种可靠的端到端的安全服务，是一种基于会话的加密和认证的Internet协议，它在两实体---客户和服务器之间提供了一个安全的管道。为了防止客户/服务器应用中的监听、篡改、消息伪造等，SSL提供了服务器认证和可选的客户端认证。通过在两个实体间建立一个共享的秘密，SSL提供保密性。
提供的主要服务：
加密处理，加密数据以防止数据中途被窃取；
维护数据的完整性，确保数据在传输过程中不被改变。
实体认证服务，认证客户端（可选）和服务器，确保数据发送到正确的客户端（可选）和服务器。

PGP是一个基于RSA公匙加密体系的邮件加密软件，可以用它对邮件保密以防止非授权者阅读，还能对邮件加上数字签名从而使收信人可以确信邮件的发送者。它可以提供一种安全的通讯方式，事先并不需要任何保密的渠道用来传递密匙，并采用了一种RSA和传统加密的混

合算法，用于数字签名的邮件利用加密前压缩、哈希算法等技术，功能强大有很快的速度。