**信息加密技术简介**

随着互联网的快速发展，计算机信息的保密问题显得越来越重要。数据保密变换，或密码技术，是对计算机信息进行保护的最实用和最可靠的方法，本文拟对**信息加密技术**作一简要介绍。

**一、信息加密概述**

密码学是一门古老而深奥的学科，它对一般人来说是莫生的，因为长期以来，它只在很少的范围内，如军事、外交、情报等部门使用。计算机密码学是研究计算机信息加密、解密及其变换的科学，是数学和计算机的交义学科，也是一门新兴的学科。随着计算机网络和计算机通讯技术的发展，计算机密码学得到前所未有的重视并迅速普及和发展起来。在国外，它已成为计算机安全主要的研究方向，也是计算机安全课程教学中的主要内容。

密码是实现秘密通讯的主要手段，是隐蔽语言、文字、图象的特种符号。凡是用特种符号按照通讯双方约定的方法把电文的原形隐蔽起来，不为第三者所识别的通讯方式称为密码通讯。在计算机通讯中，采用密码技术将信息隐蔽起来，再将隐蔽后的信息传输出去，使信息在传输过程中即使被窃取或载获，窃取者也不能了解信息的内容，从而保证信息传输的安全。

任何一个加密系统至少包括下面四个组成部分：

（1）、未加密的报文，也称明文。

（2）、加密后的报文，也称密文。

（3）、加密解密设备或算法。

（4）、加密解密的密钥。

发送方用加密密钥，通过加密设备或算法，将信息加密后发送出去。接收方在收到密文后，用解密密钥将密文解密，恢复为明文。如果传输中有人窃取，他只能得到无法理解的密文，从而对信息起到保密作用。

**二、密码的分类**

从不同的角度根据不同的标准，可以把密码分成若干类。

**（一）按应用技术或历史发展阶段划分：**

1. 手工密码。以手工完成加密作业，或者以简单器具辅助操作的密码，叫作手工密码。第一次世界大战前主要是这种作业形式。
2. 机械密码。以机械密码机或电动密码机来完成加解密作业的密码，叫作机械密码。这种密码从第一次世界大战出现到第二次世界大战中得到普遍应用。
3. 电子机内乱密码。通过电子电路，以严格的程序进行逻辑运算，以少量制乱元素生产大量的加密乱数，因为其制乱是在加解密过程中完成的而不需预先制作，所以称为电子机内乱密码。从五十年代末期出现到七十年代广泛应用。
4. 计算机密码，是以计算机软件编程进行算法加密为特点，适用于计算机数据保护和网络通讯等广泛用途的密码。

**（二）按保密程度划分：**

1. 理论上保密的密码。不管获取多少密文和有多大的计算能力，对明文始终不能得到唯一解的密码，叫作理论上保密的密码。也叫理论不可破的密码。如客观随机一次一密的密码就属于这种。
2. 实际上保密的密码。在理论上可破，但在现有客观条件下，无法通过计算来确定唯一解的密码，叫作实际上保密的密码。
3. 不保密的密码。在获取一定数量的密文后可以得到唯一解的密码，叫作不保密密码。如早期单表代替密码，后来的多表代替密码，以及明文加少量密钥等密码，现在都成为不保密的密码。

**（三）、按密钥方式划分：**

1. 对称式密码。收发双方使用相同密钥的密码，叫作对称式密码。传统的密码都属此类。
2. 非对称式密码。收发双方使用不同密钥的密码，叫作非对称式密码。如现代密码中的公共密钥密码就属此类。

**（四）按明文形态：**

1. 模拟型密码。用以加密模拟信息。如对动态范围之内，连续变化的语音信号加密的密码，叫作模拟式密码。
2. 数字型密码。用于加密数字信息。对两个离散电平构成0、1二进制关系的电报信息加密的密码叫作数字型密码。

**（五）按编制原理划分：**

可分为移位、代替和置换三种以及它们的组合形式。古今中外的密码，不论其形态多么繁杂，变化多么巧妙，都是按照这三种基本原理编制出来的。移位、代替和置换这三种原理在密码编制和使用中相互结合，灵活应用。

**三、近代加密技术**

**（一）、数据加密标准**

数据加密标准（DES）是美国经长时间征集和筛选后，于1977年由美国国家标准局颁布的一种加密算法。它主要用于民用敏感信息的加密，后来被国际标准化组织接受作为国际标准。DES主要采用替换和移位的方法加密。它用56位密钥对64位二进制数据块进行加密，每次加密可对64位的输入数据进行16轮编码，经一系列替换和移位后，输入的64位原始数据转换成完全不同的64位输出数据。DES算法仅使用最大为64位的标准算术和逻辑运算，运算速度快，密钥生产容易，适合于在当前大多数计算机上用软件方法实现，同时也适合于在专用芯片上实现。

DES主要的应用范围有：

1. 计算机网络通信：对计算机网络通信中的数据提供保护是DES的一项重要应用。但这些被保护的数据一般只限于民用敏感信息，即不在政府确定的保密范围之内的信息。
2. 电子资金传送系统：采用DES的方法加密电子资金传送系统中的信息，可准确、快速地传送数据，并可较好地解决信息安全的问题。
3. 保护用户文件：用户可自选密钥对重要文件加密，防止未授权用户窃密。
4. 用户识别：DES还可用于计算机用户识别系统中。

DES是一种世界公认的较好的加密算法。自它问世20多年来，成为密码界研究的重点，经受住了许多科学家的研究和破译，在民用密码领域得到了广泛的应用。它曾为全球贸易、金融等非官方部门提供了可靠的通信安全保障。但是任何加密算法都不可能是十全十美的。它的缺点是密钥太短（56位），影响了它的保密强度。此外，由于DES算法完全公开，其安全性完全依赖于对密钥的保护，必须有可靠的信道来分发密钥。如采用信使递送密钥等。因此，它不适合在网络环境下单独使用。

针对它密钥短的问题，科学家又研制了 80位的密钥，以及在DES的基础上采用三重DES和双密钥加密的方法。即用两个56位的密钥K1、K2，发送方用K1加密，K2解密，再使用K1加密。接收方则使用K1解密，K2加密，再使用K1解密，其效果相当于将密钥长度加倍。

**（二）国际数据加密算法**

国际数据加密算法 IDEA是瑞士的著名学者提出的。它在1990年正式公布并在以后得到增强。这种算法是在DES算法的基础上发展出来的，类似于三重DES。发展IDEA也是因为感到DES具有密钥太短等缺点，已经过时。IDEA的密钥为128位，这么长的密钥在今后若干年内应该是安全的。

类似于 DES，IDEA算法也是一种数据块加密算法，它设计了一系列加密轮次，每轮加密都使用从完整的加密密钥中生成的一个子密钥。与DES的不同处在于，它采用软件实现和采用硬件实现同样快速。

由于 IDEA是在美国之外提出并发展起来的，避开了美国法律上对加密技术的诸多限制，因此，有关IDEA算法和实现技术的书籍都可以自由出版和交流，可极大地促进IDEA的发展和完善。但由于该算法出现的时间不长，针对它的攻击也还不多，还未经过较长时间的考验。因此，尚不能判断出它的优势和缺陷。

**（三） clipper加密芯片**

密码虽然可为私人提供信息保密服务，但是它首先是维护国家利益的工具。正是基于这个出发点，考虑到 DES算法公开后带来的种种问题，美国国家保密局（NSA）从1985年起开始着手制定新的商用数据加密标准，以取代DES。1990年开始试用，1993年正式使用，主要用于通信交换系统中电话、传真和计算机通信信息的安全保护。

新的数据加密标准完全改变了过去的政策，密码算法不再公开，对用户提供加密芯片（ clipper）和硬件设备。新算法的安全性远高于DES，其密钥量比DES多1000多万倍。据估算，穷举破译至少需要10亿年。为确保安全，clipper芯片由一个公司制造裸片，再由另一公司编程后方可使用。

由于完全是官方的封闭控制，该算法除可提供高强度的密码报密外，还可对保密通信进行监听，以防止不法分子利用保密通信进行非法活动，但这种监听是在法律允许的范围内进行的。官方控制也成为美国民间反对该方案的一个重要原因。

Clipper芯片主要用于商业活动的计算机通信网。NSA同时在着手进行政府和军事通信网中数据加密芯片的研究，并作为clipper的换代产品。它除了具有clipper的全部功能外，还将实现美国数字签名标准（DSS）和保密的哈稀函数标准以及用纯噪声源产生随机数据的算法等。

**（四）公开密钥密码体制**

传统的加密方法是加密、解密使用同样的密钥，由发送者和接收者分别保存，在加密和解密时使用，采用这种方法的主要问题是密钥的生成、注入、存储、管理、分发等很复杂，特别是随着用户的增加，密钥的需求量成倍增加。在网络通信中，大量密钥的分配是一个难以解决的问题。

例如，若系统中有 n 个用户，其中每两个用户之间需要建立密码通信，则系统中每个用户须掌握 (n-1)/2 个密钥，而系统中所需的密钥总数为 n\*(n-1)/2 个。对 10 个用户的情况，每个用户必须有 9 个密钥，系统中密钥的总数为 45 个。对 100 个用户来说，每个用户必须有 99 个密钥，系统中密钥的总数为 4950 个。这还仅考虑用户之间的通信只使用一种会话密钥的情况。如此庞大数量的密钥生成、管理、分发确实是一个难处理的问题。

本世纪 70 年代，美国斯坦福大学的两名学者迪菲和赫尔曼提出了一种新的加密方法 -- 公开密钥加密队 PKE 方法。与传统的加密方法不同，该技术采用两个不同的密钥来对信息加密和解密，它也称为 “ 非对称式加密方法”。每个用户有一个对外公开的加密算法 E 和对外保密的解密算法 D ，

它们须满足条件：

1. D 是 E 的逆，即 D[E （ X ） ]=X ；
2. E 和 D 都容易计算；
3. 由 E 出发去求解 D 十分困难。

从上述条件可看出，公开密钥密码体制下，加密密钥不等于解密密钥。加密密钥可对外公开，使任何用户都可将传送给此用户的信息用公开密钥加密发送，而该用户唯一保存的私人密钥是保密的，也只有它能将密文复原、解密。虽然解密密钥理论上可由加密密钥推算出来，但这种算法设计在实际上是不可能的，或者虽然能够推算出，但要花费很长的时间而成为不可行的。所以将加密密钥公开也不会危害密钥的安全。

数学上的单向陷门函数的特点是一个方向求值很容易，但其逆向计算却很困难。许多形式为 Y=f （ x ）的函数，对于给定的自变量 x 值，很容易计算出函数 Y 的值；而由给定的 Y 值，在很多情况下依照函数关系 f(x) 计算 x 值十分困难。例如，两个大素数 p 和 q 相乘得到乘积 n 比较容易计算，但从它们的乘积 n 分解为两个大素数 p 和 q 则十分困难。如果 n 为足够大，当前的算法不可能在有效的时间内实现。

正是基于这种理论， 1978 年出现了著名的 RSA 算法。这种算法为公用网络上信息的加密和鉴别提供了一种基本的方法。它通常是先生成一对 RSA 密钥，其中之一是保密密钥，由用户保存；另一个为公开密钥，可对外公开，甚至可在网络服务器中注册。为提高保密强度， RSA 密钥至少为 500 位长，一般推荐使用 1024 位。这就使加密的计算量很大。为减少计算量，在传送信息时，常采用传统加密方法与公开密钥加密方法相结合的方式，即信息采用改进的 DES 或 IDEA 对话密钥加密，然后使用 RSA 密钥加密对话密钥和信息摘要。对方收到信息后，用不同的密钥解密并可核对信息摘要。

RSA 算法的加密密钥和加密算法分开，使得密钥分配更为方便。它特别符合计算机网络环境。对于网上的大量用户，可以将加密密钥用电话簿的方式印出。如果某用户想与另一用户进行保密通信，只需从公钥簿上查出对方的加密密钥，用它对所传送的信息加密发出即可。对方收到信息后，用仅为自己所知的解密密钥将信息脱密，了解报文的内容。由此可看出， RSA 算法解决了大量网络用户密钥管理的难题。

RSA 并不能替代 DES ，它们的优缺点正好互补。 RSA 的密钥很长，加密速度慢，而采用 DES ，正好弥补了 RSA 的缺点。即 DES 用于明文加密， RSA 用于 DES 密钥的加密。由于 DES 加密速度快，适合加密较长的报文；而 RSA 可解决 DES 密钥分配的问题。美国的保密增强邮件（ PEM ）就是采用了 RSA 和 DES 结合的方法，目前已成为 E-MAIL 保密通信标准。

**四、网络通信安全措施**

对于网络通信，可采用以下两种具体措施进行加密传输。这些措施的加、解密功能都可以采用上述算法实现：

**（ 1 ）链路加密**

链路加密是传输数据仅在物理层前的数据链路层进行加密。接收方是传送路径上的各台节点机，信息在每台节点机内都要被解密和再加密，依次进行，直至到达目的地。

使用链路加密装置能为某链路上的所有报文提供传输服务。即经过一台节点机的所有网络信息传输均需加、解密，每一个经过的节点都必须有密码装置，以便解密、加密报文。如果报文仅在一部分链路上加密而在另一部分链路上不加密，则相当于未加密，仍然是不安全的。与链路加密类似的节点加密方法，是在节点处采用一个与节点机相连的密码装置（被保护的外围设备）, 密文在该装置中被解密并被重新加密，明文不通过节点机，避免了链路加密关节点处易受攻击的缺点。

**（ 2 ）端 - 端加密**

端 - 端加密是为数据从一端传送到另一端提供的加密方式。数据在发送端被加密，在最终目的地（接收端）解密，中间节点处不以明文的形式出现。

采用端 - 端加密是在应用层完成，即传输前的高层中完成。除报头外的的报文均以密文的形式贯穿于全部传输过程。只是在发送端和最终端才有加、解密设备，而在中间任何节点报文均不解密，因此，不需要有密码设备。同链路加密相比，可减少密码设备的数量。另一方面，信息是由报头和报文组成的，报文为要传送的信息，报头为路由选择信息。由于网络传输中要涉及到路由选择，在链路加密时，报文和报头两者均须加密。而在端 -- 端加密时，由于通道上的每一个中间节点虽不对报文解密，但为将报文传送到目的地，必须检查路由选择信息，因此，只能加密报文，而不能对报头加密。这样就容易被某些通信分析发觉，而从中获取某些敏感信息。

**（ 3 ）加密传输方式的比较**

数据保密变换使数据通信更安全，但不能保证在传输过程中绝对不会泄密。因为在传输过程中，还有泄密的隐患。

采用链路加密方式，从起点到终点，要经过许多中间节点，在每个节点地均要暴露明文（节点加密方法除外），如果链路上的某一节点安全防护比较薄弱，那么按照木桶原理（木桶水量是由最低一块木板决定），虽然采取了加密措施，但整个链路的安全只相当于最薄弱的节点处的安全状况。

采用端 - 端加密方式，只是发送方加密报文，接收方解密报文，中间节点不必加、解密，也就不需要密码装置。此外，加密可采用软件实现，使用起来很方便。在端 -- 端加密方式下，每对用户之间都存在一条虚拟的保密信道，每对用户应共享密钥（传统密码保密体制，非公钥体制下），所需的密钥总数等于用户对的数目。对于几个用户，若两两通信，共需密钥 n\*(n-1)/2 种，每个用户需 (n-1) 种。这个数目将随网上通信用户的增加而增加。为安全起见，每隔一段时间还要更换密钥，有时甚至只能使用一次密钥，密钥的用量很大。

链路加密，每条物理链路上，不管用户多少，可使用一种密钥。在极限情况下，每个节点都与另外一个单独的节点相连，密钥的数目也只是 n\*(n-1)/2 种。这里 n 是节点数而非用户数，一个节点一般有多个用户。

从身份认证的角度看，链路加密只能认证节点，而不是用户。使用节点 A 密钥的报文仅保证它来自节点 A 。报文可能来自 A 的任何用户，也可能来自另一个路过节点 A 的用户。因此链路加密不能提供用户鉴别。端 -- 端加密对用户是可见的，可以看到加密后的结果，起点、终点很明确，可以进行用户认证。

总之，链路加密对用户来说比较容易，使用的密钥较少，而端 - 端加密比较灵活，用户可见。对链路加密中各节点安全状况不放心的用户也可使用端 - 端加密方式。

当然，对于互联网中应用最广泛的WWW服务器的信息加密，最简单又最安全的加密方式是为服务器部署 [SSL数字证书](http://www.wosign.com/)，充分利用现有的服务器和客户端软件广泛支持的PKI技术来轻松实现信息加密。