网络安全中的数据加密技术研究

重庆大学机械工程学院 CAD/CAM研究室 黄志清

数据加密技术是实现网络安全的关键技术之一。本文系统地讨论了对称式加密、公开密钥加密以及混合式加密三种数据加密技术以及链路加密和端对端加密两种网络数据加密方式。

引言

随着信息技术突飞猛进的发展和计算机技术的广泛应用，计算机网络得到了长足发展和应用，比如电子商务，基于网络的产品设计、经营管理等。同时，由于计算机网络缺乏足够的安全性，网络上传输的信息随时都受到非法存取、盗听、篡改和破坏等的威胁，网络安全性问题日益突出，网络安全对策研究显得尤为重要。

网络安全是计算机安全在网络环境下的扩展和延伸，主要包括用户身份验证、访问控制、数据完整性、数据加密、防抵赖和审计追踪等安全要求。

数据加密技术是对信息进行重新编码，从而达到隐藏信息内容，使非法用户无法获得信息真实内容的一种技术手段。网络中的数据加密则是通过对网络中传输的信息进行数据加密，满足网络安全中数据加密、数据完整性等要求，而基于数据加密技术的数字签名技术则可满足防抵赖等安全要求。可见，数据加密技术是实现网络安全的关键技术。

数据加密技术

1. 数据加密、解密基本过程

通常情况下，人们将可懂的文本称为明文(plaintext)；将明文变换成的不可懂的形式的文本称为密文(ciphertext)；把明文变换成密文的过程叫加密(encipher)；其逆过程，即把密文变换成明文的过程叫解密（decipher）。密钥（keyword）是用于加解密的一些特殊信息，它是控制明文与密文之间变换的关键，它可以是数字、词汇或语句。密钥分为加密密钥(Encryption Key)和解密密钥(Decryption Key)。完成加密和解密的算法称为密码体制（Cipher System）。传统的密码体制所用的加密密钥和解密密钥相同，形成了对称式密钥加密技术；在一些新体制中，加密密钥和解密密钥不同，形成非对称式密码加密技术，即公开密钥加密技术。数据加密或解密变换过程如图1所示：

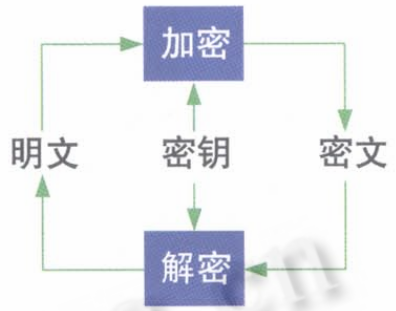

图 1 加密或解密变换

2. 对称式密钥加密技术

(1)基本概念。对称式密钥加密技术是指加密和解密均采用同一把秘密钥匙，而且通信双方必须都要获得这把钥匙，并保持钥匙的秘密。当给对方发信息时，用自己的加密密钥进行加密，而在接收方收到数据后，用对方所给的密钥进行解密。故它也称为秘密钥匙加密法。

(2)加密算法。实现对称式密钥加密技术的加密算法主要有以下两种：

① DES（Data Encryption Standard）算法。DES即数据加密标准，是1977年美国国家标准局宣布用于非国家保密机关的数据保护。这种加密算法是由IBM研究提出来，它综合运用了置换、代替、代数多种密码技术，把信息分成64位大小的块，使用56位密钥，迭代轮数为16轮的加密算法。

② IDEA（International Data Encryption Algorithm）算法。IDEA是一种国际信息加密算法。它是1991年在瑞士ETH Zurich由James Massey和Xueiia Lai 发明，于1992年正式公开，是一个分组大小为64位，密钥为128位，迭代轮数为八轮的迭代型密码体制。此算法使用长达128位的密钥，有效地消除了任何试图穷尽搜索密钥的可能性。

(3)对称式密钥加密技术的优缺点。对称式密钥加密技术具有加密速度快，保密度高等优点。但也有其缺点:

①密钥是保密通信安全的关键，发信方必须安全、妥善地把钥匙护送到收信方，不能泄露其内容，如何才能把密钥安全地送到收信方，是对称密钥加密技术的突出问题，可见，此方法的密钥分发过程十分复杂，所花代价高。

②多人通信时密钥的组合的数量，会出现爆炸性的膨胀，使密钥分发更加复杂化，n个人进行两两通信，总需要的密钥数为n(n−1)/2。

③通信双方必须统一密钥，才能发送保密的信息。如果发信者与收信人是素不相识的，这就无法向对方发送秘密信息了。

3. 公开密钥加密技术

(1)基本概念。公开密钥加密技术要求密钥成对使用，即加密和解密分别由两个密钥来实现。每个用户都有一对选定的密钥，一个可以公开，即公共密钥，用于加密；另一个由用户安全拥有，即秘密密钥，用于解密。公共密钥和秘密密钥之间有密切的关系。当给对方发信息时，用对方的公开密钥进行加密，而在接收方收到数据后，用自己的秘密密钥进行解密。故此技术也称为非对称密码加密技术。

(2)加密算法。公开密钥加密算法主要是RSA加密算法。此算法是美国MIT的Rivest、Shamir和Adleman于1978年提出的，它是第一个成熟的、迄今为止理论上最为成功的公开密钥密码体制，它的安全性基于数论中的Euler定理和计算复杂性理论中的下述论断：求两个大素数的乘积是容易的，但要分解两个大素数的乘积，求出它们的素因子则是非常困难的，它属于NP−完全类。RSA加密、解密过程由密钥生成、加密过程和解密过程组成。

(3)公开密钥加密技术的优缺点。公开密钥加密技术的优点是:

①密钥少便于管理，网络中的每一用户只需保存自己的解密密钥，则N个用户仅需产生N对密钥。

②密钥分配简单，加密密钥分发给用户，而解密密钥则由用户自己保管。

③不需要秘密的通道和复杂的协议来传送密钥。

④可以实现数字签名和数字鉴别。

公开密钥加密技术的缺点是加、解密速度慢。

4. 对称密钥和公开密钥相结合的加密技术

鉴于对称密钥和公开密钥加密技术的特点，在实际应用中将两种加密技术相结合，即结合使用DES/IDEA和RSA，对于网络中传输的数据用DES或IDEA加密，而加密用的密钥则用RSA加密传送，此方法既保证了数据安全又提高了加密和解密的速度。DES/IDEA 和RSA结合使用如图2所示:

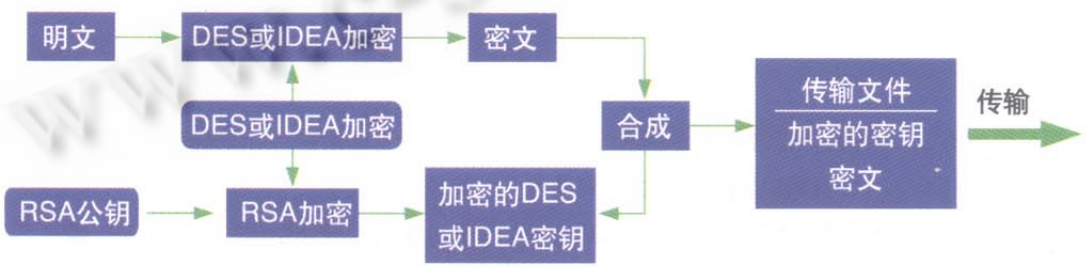

图 2　DES/IDEA 和RSA 结合的加密技术示意图

首先发信者使用DES/IDEA算法用对称钥将明文原信息加密获得密文，然后使用接收者的RSA公开钥将对称钥加密获得加密的DES或 IDEA密钥，将密文和加密的密钥一起通过网络传送给接收者。接收方接收到密文信息后，首先用自己的密钥解密而获得DES或 IDEA密钥，再用这个密钥将密文解密而最后获得明文原信息。由此，起到了对明文信息保密的作用。

著名的PGP(Pretty Good Privacy)软件就是使用RSA和IDEA相结合进行数据加密。另外，保密增强邮件（PEM）将RSA和DES结合起来，成为一种保密的

E_mail 通信标准。常用到的SSL(Secure Sockets Layer,安全套层)安全措施也是利用两种加密技术对客户机和服务器之间所传输的信息进行加密的。

网络中的数据加密方式

数据加密可以在网络 OSI 七层协议的多层上实现，从加密技术应用的逻辑位置看，主要有链路加密和端对端加密两种方式。

1. 链路加密方式

面向链路的加密方式将网络看作由链路连接的结点集合，每一个链路被独立的加密。它用于保护通信结点间传输的数据。每一个链接相当于OSI参考模型建立在物理层之上的链路层。链路加密方式如图 3 所示:

Ek1及Ek2为加密变换，Dk1及Dk2为解密变换

图 3 链路加密方式示意图

链路加密方式的优缺点如下:

(1) 加密对用户是透明的，通过链路发送的任何信息在发送前都先被加密。

(2) 每个链路只需要一对密钥。

(3) 提供了信号流安全机制。

(4) 缺点是数据在中间结点以明文形式出现，维护结点安全性的代价较高。

2. 端对端加密方式

端对端加密方式建立在OSI 参考模型的网络层和传输层。这种方法要求传送的数据从源端到目的端一直保持密文状态，任何通信链路的错误不会影响整体数据的安全性。端对端加密方式如图 4 所示:

Ek为加密变换，Dk为解密变换

图 4 端对端加密方式示意图

在端对端加密方式中，只加密数据本身信息，不加密路径控制信息。在发送主机内信息是加密的，在中间结点信息是加密的。用户必须找到加密算法，决定施加某种加密手段。加密可以用软件编程实现。但此方式密钥管理机制复杂，主要适合大型网络系统中信息在多个发方和收方之间传输的情况。

结束语

随着网络的应用与发展，网络安全问题日益突出。本文讨论的数据加密技术是实现计算机网络环境下数据安全的重要手段之一，它是一种主动安全防御策略，为信息传输提供安全保护。并和其他网络安全技术（如防火墙、访问控制系统等）一起构筑安全、可靠的网络环境，使得计算机网络的应用更加广泛和深入。■

参考文献

1 张超 Internet/Intranet 实用安全技术 西安电子科技大学出版社 1999

2 樊宸丰，林东 网络信息安全 &PGP 加密 清华大学出版社 1998

3 贾晶 等 信息系统的安全与保密 清华大学出版社 1999

4 胡英伟 等 网络安全技术--数据加密 计算机与通信 1998 (10)

5 李海泉，李健 计算机网络的安全与加密 计算机与通信 1999 (7)