数据加密及其在身份认证等方面的运用

李 铭 陈学广 (华中科技大学 430074)
甘 邯 (中国三峡总公司)

摘要：介绍一般数据加密算法，探讨综合利用多种加密算法以提高网络数据安全，以及其在身份验证、邮件文摘等电子商务中的运用。

关键词：数据安全 认证 密钥 加密算法 电子商务

对网上支付安全问题的担忧使许多人对电子商务望而却步[2]。这是因为，如果此时采用目前大多数 web 浏览器使用的http协议，其明文传输机制就会给网络数据安全造成了巨大的隐患——任何传输过程中的路由的网关和网上的监听软件都可以监听用户与另一个站点接受订单或进行信用卡支付的 Internet 会话[3]，甚至窃取用户的支付帐号和密码。所以，有人说，“安全问题仍旧是电子支付中最关键、最重要的问题。”[2] 还有，假如甲公司收到乙公司发来的订单，甲公司如何确认发来的订单一定是乙公司的呢?假如乙公司抵赖，那么甲公司如何能在对簿公堂时提供确凿的证据呢?乙公司又如何确保订单在路由时不被恶意篡改呢?所有这些都属于网络数据传输的安全与身份认证问题。

本文介绍一般数据加密算法，探讨综合利用多种加密算法以提高网络数据安全，以及其在身份验证、邮件文摘等电子商务中的运用。

1 数据加密算法

数据加密和解密历来是人们关注的话题。数据加密的目的是使其内涵受到保护而免于被他方获取，解密的目的则不言而喻。加密必须遵循一定的规则或算法，否则就无法还原经过加密的数据。

现代加密算法与古典算法的最大区别在于：将古老的数论应用进来，原文的保密性不再依赖于算法本身，而直接依赖于密钥的保密性，算法本身应是公开的。并且，密钥越长，相应的加密等级越高。按密钥的性质来分，可以分为对称性加密和非对称性加密两类[5]。

1.1 对称性加密算法

对称性算法的对称性体现在用相同的密钥加密和解密。代表算法有 DES，Tripl-Des,Rc2,Rc4,CAST 等。DES(Digital Encryption Standard)算法原是 IBM 公司为保护产品的机密于 1971 年至 1972 年研制成功的，后被美国国家标准局和国家安全局选为数据加密标准，并于 1977 年颁布使用。ISO 也已将DES作为数据加密标准。其加密等级随着密钥的长度呈几何级数增长，超过128位的密钥在当时很长一段时间内要单独破译几乎是不可能。其加密算法如图 1 所示。

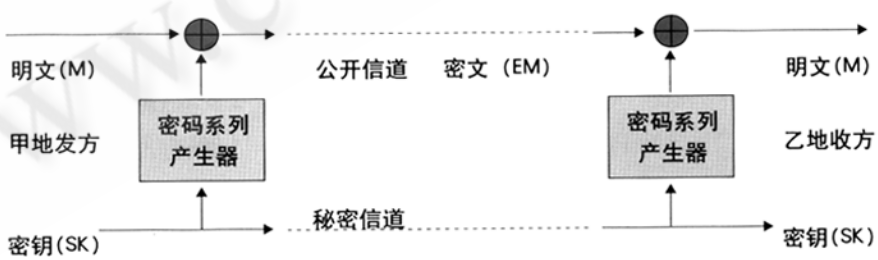

图 1 DES 加密算法

由图上可以看出，密钥的传递渠道和保密性是一个薄弱的环节，处理得不好，将直接关系到整个体系的安全。

1.2 非对称性加密算法

非对称性加密算法也称之为公开密钥体制(Public Key

Infrastructure ,PKI)，即将加密的密钥公开，而解密的密钥只有自己知道，两者一一对应。其中，公开的密钥通常称为公钥(PK)，而自己手中的密钥称为私钥(SK)。这样，用公钥加密的数据就无法用公钥解开，而只能由私钥解密。加密和解密过程通常是可逆的。

非对称性加密的代表算法有RSA、DSA、Diffie-Hellman、背包体制、POHLIG-Hellman算法和Rabin算法，还可以在有限域上的椭圆曲线上建立RSA、EIGamal等算法。其中最有影响力的是RSA(Rivest-Shamir-Adleman)算法。它出现于1976年，如今已被ISO/TC97的数据加密技术分委员会SC20推荐为公开密钥数据加密标准[5]。它基于大数不可质数因式分解假设性公理，即当选取两个很大的质数(通常都在100位以上)，求他们的乘积很容易，但是要从他们的乘积来逆向求这两个质数却是难上加难，这种函数称为“单向函数”。本质上讲，所有的“单向函数”都可以作公钥加密算法之用。这里通过运算得到两个数，其中一个用来公开给世人，即为公钥(RK)，而另一个则为密钥(SK)，由自己安全保存，它们之间的关系如图2所示。

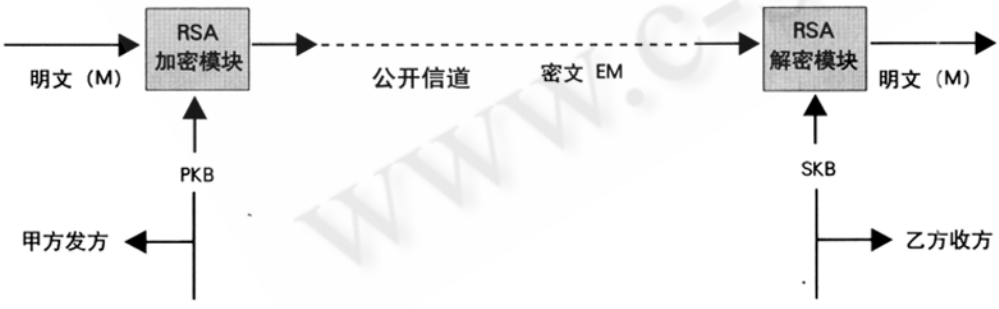

图 2 RSA 算法

DSK(EPK(x))=x; 同时有：EPK(DSK(x))=x

即使 DPK(EPK(x))≠ x

其中，D代表解密算法，E代表加密算法，x代表明文。在n足够大的情况下，对n进行因式分解事实上是不可行的，从而达到保密的目的。

2 综合加密算法

保密是加密算法的初衷。鉴于以上两种算法的特点，如何高效地实现加密和解密是各种算法关注的焦点。由前述讨论可知，对称加密算法密钥存在安全隐患；而公钥算法耗时、复杂则是它未能得到广泛应用的主要原因。如果能综合这两种算法的优点而构造一种新的算法，即：用DES来加密原明文，而用RSA算法来加密传送密钥，就会较好地解决这些矛盾，收到理想的效果。图3所示为这种综合加密算法的原理图。

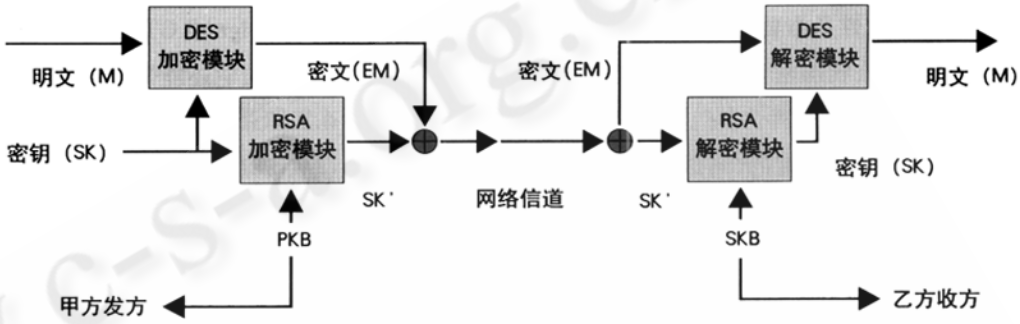

图 3 综合算法

事实上，著名的IDES就是基于这种想法实现的加密算法。

3 数据安全与身份认证的基本原则和实现

3.1 数据的保密性(Privacy)实现

由上面的分析可以看出，综合运用对称算法和非对称算法是当前加密领域的主流趋势。但是，近年来，随着处理器速度的高速提升及并行处理器的发展，使得密码分析员有可能破译加密信息。一些原本认为事实不可破解的算法现在可能利用最基本的穷举思想破解。特别是最近，高速运算力让破译DES及RSA的PKI加密信息的速度成倍增加[3]，数据的保密性能直接倚赖与密钥的长度，并随密钥长度几何倍增加。所以，根据数据的安全要求来选取适当的密钥长度是非常必要的。

3.2 数据的完整性(Integrity)实现

数据的完整性就是确认数据在传输途中没有被恶意篡改，即使被篡改，也能容易地辨别出来。为此，首先通过所谓的单向Hash函数提取出表征当前文件内容特征的“邮件精华”(Message Digest)，然后对其用接收者的公钥进行加密。这样，收方就可以通过利用发件方公钥解密这部分“精华”，再与由收到的文件产生的精华比照，达到校验内容的目的，从而保证数据的完整性，防止恶意篡改。

3.3 数据的确认性(Authentication)实现

数据确认性是指要提供能表征发信人真实身份的一种证据。利用公钥加密算法，很容易实现这种认证。比如，甲方要给乙方发送信件，为了让乙方确认该信的确是甲方所发，而不是别人假冒的，可以用甲方自己的私钥对其进行加密，如果乙方能用甲方的公钥解开，则表明此信确由甲方发来。否则，不能确信。这在如今的电子商务中有较为普遍的运用，常称为“数字签名”(Digital Signatures)，并且常常和“邮件文摘”结合使用。

3.4 网上密钥分配及认证机制的实现

使用公钥加密算法的一个重要问题就是公钥本身的传递，或者说是如何通过安全渠道获得可以确信的公钥。如果公钥被篡改，其后果便不堪设想，黑客不仅可以解密信件，在一定程度上还可以伪造信件。目前普遍的认证机制是利用“中介人”，或者被称为“密匙侍者”或者“权威认证机构”(Certificate Authority)。这个角色由大家普遍信任和认可的机构担任，由他签发的公钥被认为是有效的。由于他的广泛流通性，想伪造几乎是不可能的。国内的认证机构主要是相关的政府机构，而在国外，已有许多相关的商业发证网上机构，比如Verisign,BankGate CA,BelSign NV SA等。

当然，还有其他认证公钥的方法。譬如，直接与对方联系，获得对方公钥，或者电话认证等等。

其实，在电子商务日益发展的今天，利用密码学可以实现的商业行为远远不止这些，例如，可以利用加密算法实现零知识验证，盲签名，同时签名，秘密同时交换等等，甚至可以达到比传统的业务运作更高的安全性和效率。这里由于篇幅的限制，就不一一详述了。

4 几种常用加密及安全认证机制的比较

4.1 PGP

PGP(Pretty Good Privacy)是一种基于RSA公钥加密体系的邮件加密软件，它是由美国的Phil Zimmermann于1991年开发的[1]。PGP将RSA体系的方便性和对称加密算法IDEA结合起来，并在数字签名和密钥认证管理上有巧妙的设计，因此成为目前最流行的公钥加密软件包。

4.2 S/MIME

S/MIME(Secure/MIME)于1996年开发成功，目前也广泛运用到电子邮件软件之中。它的特点在于利用数字签名维护邮件完整性和真实性，而用数字信封确保邮件隐私性。同时，为了防止假冒他人名义发布公钥，它使用X.509数字证书来认证公钥主人身份的真实性。即在获得第三方如Verisign或GTE认证，就可以自己发布自己的数字证书，同时它还能管理密钥的生存周期以及证书撤消列表。

4.3 SSL

SSL(Secure Socket Layer)是基于HTTP协议的安全加密层，起初是由Netscape公司为自己的浏览器在应用层和传输层添加的一个安全层，由于它以较小的成本实现了数据加密和安全保障，因此后来被广泛地应用于Web领域。但是，它只能实现双方的安全认证，不支持多方身份认证，因而在在线交易中的应用受到了一些限制。

4.4 SET

SET(Secure Electronic Transaction)是由VISA和Master两大信用卡组织提出的以信用卡为基础的电子系统付款系统规范。涉及SET交易的有持卡人、商家和支付网关三个实体。认证机构需要分别向持卡人、商家和支付网关发出证书，这样，保证商家无法获得持卡人的信用卡信息，银行无法获得持卡人购物信息，同时还保证商家收到货款的SET支付的目标。

但是，SET本身是个庞大而复杂、涉及面很广的系统，已非IT行业本身所能完成，并且实施费用较高，通常需要硬件加密，所以很难迅速普及。针对这种状况，又出现了许多折中解决方案。■

参考文献

1 《计算机密码学》，卢开澄，清华大学出版社(第一版) 1998年

2 《银行业发展电子商务面临的难题》，张艾，计算机世界网络与通信版 2000年24期

3 《银行在线交易的风险与防范》，宋伟昊，微电脑世界，2000年28期

4 《建立安全的认证中心》，徐快，王峰，微电脑世界，2000年28期

5 《Cryptography and Data Security》 Dorothy Elizabeth Rolbling Denning Addison—Wesley Publishing Company 1982