数据加密技术的应用研究

摘 要

信息安全是当今社会非常重要的问题之一。数据安全是信息安全的重要组成部分，如何确保数据安全可靠，是信息领域中非常重要的课题。对重要的数据进行加密处理，是保证数据安全的重要手段之一。研究数据加密技术与方法不仅有非常重要的学术意义，同时也具有非常重要的现实意义。

信息安全是当今社会非常重要的问题之一。数据安全是信息安全的重要组成部分，如何确保数据安全可靠，是信息领域中非常重要的课题。对重要的数据进行加密处理，是保证数据安全的重要手段之一。研究数据加密技术与方法不仅有非常重要的学术意义，同时也具有非常重要的现实意义。

信息安全是当今社会非常重要的问题之一。数据安全是信息安全的重要组成部分，如何确保数据安全可靠，是信息领域中非常重要的课题。对重要的数据进行加密处理，是保证数据安全的重要手段之一。研究数据加密技术与方法不仅有非常重要的学术意义，同时也具有非常重要的现实意义。

# 背景

随着计算机技术的革新，对网络的通信安全要求水平水 涨船高，与此同时，各种各样的网络信息窃取和破坏也使得社 会各领域在对计算机安全方面的需求日益强烈。总的来说， 计算机的信息安全包涵了两个层面的要求：一方面是对计算 机信息的存储安全要求；另外一方面就是对计算机网络的通 信安全要求。在对计算机安全存在的威胁中人为因素要比非 人为因素的影响大得多，人为的安全威胁又分为被动攻击和 主动攻击。其中被动攻击主要影响计算机的数据保密性，常 用的手段有六个：一是对通信线路上传递信息的窃取和监听； 二是对窃取和监听的数据分析；三是冒充用户身份；四是对网 络中传播的信息进行篡改；五是拒绝确认所发信息；六是其他手段。

# 发展过程

# 常用的加密方式

我们所研究的数据加密技术，并不是单单一种。一般说来，从数据加密的方法上分，数据加密技术可以分为两种：动态数据加密技术和静态数据加密技术。动态数据加密技术是指当数据经过网络时，数据在数据库服务器和客户端之间的相互传送，这种传输过程中数据的加密技术就是动态数据加密技术。这种方法可以有效的阻止会话攻击。现实生活中，这种动态数据加密技术已经被广泛的应用了。静态数据加密技术是指对存在于数据库中的数据进行加密处理。这种静态加密技术还没有广泛的应用。

# 加密的实现原理

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 ( plaintex t) ;将明文变换成的不可懂的形式的文本称为密文 ( ciphertex t) ;把 明文变换成密文的过程叫加密 ( enciphe r) ; 其逆过程 ,即把密 文变换成明文的过程叫解密 ( decipher)。 密钥 ( keywo rd)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 ( Encry ption Key)和解密密钥 ( Decr yptio n Key)。完成加密和解密 的算法称为密码体制 ( Ciphe r 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。

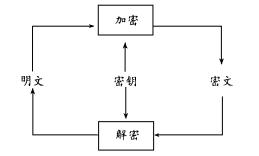


图1 加密或解密变换

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( Da ta Enc ryption Standa rd)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( Internatio nal Da ta Encry ption Alg o rithm )算法

IDEA是一种国际信息加密算法。 它是 1991年在瑞士

E TH 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 ,在

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

M IT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

N P—— 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

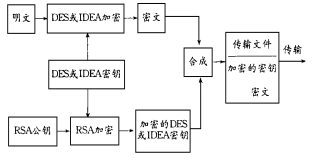
鉴于对称密钥和公开密钥加密技术的特点 ,在实际应用

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。



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 RS A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( Pr etty Go od 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 ( PRM )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( Secur e Sockets Lay er,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。

# 加密的常用方法

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。 每一个连接相当于 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:

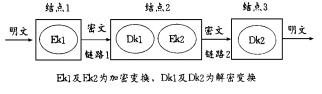


图3 链路加密方式

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:

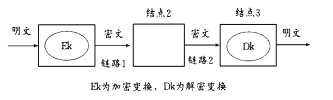


图4 端对端加密方式示意图

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

性; 而其源代码则表现出可移植性 ,可扩展性和代码可维护

性。

# 主要应用

## 数字签名

数字签名（Digital Signature）在ISO7498-2标准中定义为：“附加在数据单元上的一些数据，或是对数据单元所做的密码变换，这种数据和变换允许数据单元的接收者泳衣确认数据单元来源和数据单元的完整性，并保护数据，防止被人（例如接收者）进行伪造”。美国电子签名标准（DSS，FIPS186-2）对数字签名作了如下解释：“利用一套规则和一个参数对数据计算所得的结果，用此结果能够确认签名者的身份和数据的完整性”。按上述定义PKI提供可以提供数据单元的密码变换，并能使接收者判断数据来源及对数据进行验证。

数字签名是邮件、文件或其他数字编码信息的发件人将她们的身份与信息绑定在一起的方法。对信息进行数字签名的过程中，需要将信息与由发件人掌握的秘密信息一起转换为叫做签名的标记。数字签名用于公钥环境中，它通过验证发件人确实是她或他所生命的那个人，并确认收到的邮件与发送的邮件完全相同，来帮助确保电子商务交易的安全。

## 数字证书

数字证书（Digital Certificate，Digital ID）用以证实一个用户的身份和对网络资源的访问权限，是目前电子商务广泛采用的技术之一。在网上的点子交易中，如果双方都出示了各自的数字证书，并用它们进行交易操作，那么双方就不必为对方身份的真实性担心了。

数字证书与传输密钥和签名密钥对的产生相对应。对每一个公钥做一张数字证书，私钥用最安全的方式交给用户或用户自己生产密钥对。数字证书的内容包括用户的公钥，姓名、发证机构的数字签名及用户的其他信息。公钥的拥有者是身份的象征。对方可以据此验证身份。对于密钥的丢失情况、则采用恢复密钥、密钥托管等方法。另外对于证书的有效期在政策上加以规定，已过期的证书应重新签发对于私钥丢失或非法使用应废止。

# 加密性能优劣

# 未来发展趋势