

第3章 密钥管理

内容提要

密钥是加密运算和解密运算的关键，也是密码系统的关键。根据近代密码体制的观点，密码系统的安全取决于密钥的安全。密码体制可以公开，密码设备可以丢失，同一型号的加密设备可以继续使用，但密钥一旦丢失或出错，会导致信息遭非法用户窃取。将密钥泄露给他人意味着加密文档还不如使用明文，因此密钥管理在电子商务安全中极为重要。

本章的主要目的是让读者学习和掌握密钥管理的知识。密钥管理包括密钥的组织、产生、分配、保护等一系列技术问题。

3.1 密钥管理的目标和内容

密钥管理的目标在于提高系统的安全保密程度。一个好的密钥管理系统，其密钥的产生与分配应尽量减少人的直接干预，做到：

- (1) 密钥难以被非法窃取。
- (2) 在一定条件下，即使被窃取了也无用。
- (3) 密钥分配和更换的过程对用户是透明的，用户不一定亲自掌握密钥。

密钥管理的内容主要包括创建密钥、分发密钥、保护密钥、归档密钥、恢复密钥。

3.2 密钥的组织

在一种密码系统中，为了保证信息和系统安全，常需要多种密钥，且每种密钥担负相应的任务。下面介绍几种常用的密钥。

(1) 初级密钥。我们把保护数据（加密和解密）的密钥叫作初级密钥，记为 K 。初级密钥又称为数据加密（数据解密）密钥。当初级密钥直接用于提供通信安全时，叫作初级通信密钥，记为 K_C 。在通信会话期间，用于保护数据的初级通信密钥叫作会话密钥，但当初级密钥直接用于提供文件安全时，叫作初级文件密钥，记为 K_F 。

(2) 中级密钥。中级密钥（Secondary Key）用于保护初级密钥，记为 K_N ，这里 N 表示节点，源于它在网络中的地位。当中级密钥用于保护初级通信密钥时，称为中级通信密钥，记为 K_{NC} ；当中级密钥用于保护初级文件密钥时，称为中级文件密钥，记作 K_{NF} 。

(3) 高级密钥。高级密钥即主密钥（Master Key），是密钥管理方案中的最高级密钥，记为 K_M 。高级密钥主要用于对中级密钥与初级密钥进行保护。

(4) 其他密钥。在一个系统中，除上述密钥之外，还可能有通播密钥、共享密钥等，它

们也有各自的用途。

密钥长度一般以比特为单位，也有以字节为单位的。密钥长度的选取与加密时采用的加密算法直接相关。一般来说，密钥的长度越长，加密的效果越佳，但密钥长度的加大又会加大存储空间和密钥管理的难度，这就要在时间、空间和加密效果之间根据具体情况进行权衡，从而得到所需的密钥长度。

3.3 密钥的产生

3.3.1 密钥的随机性要求

密钥是数据保密的关键，应有足够的方法来产生密钥。密钥的一个基本要求是具有良好的随机性。

在一般的非密码应用场合，人们只要求产生的随机数呈平衡、等概分布，并不要求它的不可预测性。而在密码技术中，特别是在密钥产生技术中，不可预测性成了随机性的根本性质，因为那些虽然能经受随机统计检验但很容易预测的序列肯定是容易被攻破的。按这种理解，随机性包含了长周期性、非线性性、统计上的等概性，以及有关可预测性的一切有意义的密码学特性，其与计算复杂度和密码强度的概念等价，即在一个二进制序列中：

- (1) 0 与 1 的数量基本平衡。
- (2) 0 与 1 的游程数量基本平衡且随游程长度的增加以指数规律下降。
- (3) 在周期内（或在给定范围内），序列的异相自相关函数为常数。

然而，这 3 条标准只是达到随机性的必要条件，不满足这 3 条标准的序列肯定是不随机的，但对于满足了这 3 条标准的序列，也不能就此认为它是随机的。

目前，关于随机性最严格的定义：一个理想噪声源的二进制输出序列 $S_0, S_1, \dots, S_{n-1}, S_n, \dots$ 的随机性，表示为当前输出位 S_n 与在此之前的所有输出信号之间的完全独立性。也就是说，在已知 $S_0, S_1, \dots, S_{n-1}$ 的条件下， S_n 仍然是不可预测的。

3.3.2 噪声源产生密钥

噪声源的功能是产生二进制的随机序列或与之对应的随机数，它是密钥产生设备的核心部件。噪声源的随机性不好会给破译带来线索，而且某些破译方法特别依赖加密者使用简单的或容易破解的密钥。

在大型计算机密码系统中，常采用高级密钥、中级密钥和初级密钥等 3 种不同级别的密钥。针对不同的密钥，应采用不同的方法来产生。高级密钥是密码系统中的最高级密钥，可用它对其他密钥进行保护。高级密钥的生存周期长，因此它应是高质量的真随机序列。真随机序列的产生常采用物理噪声源的方法。目前，物理噪声源主要有基于力学的噪声源、基于电子学的噪声源和基于量子学的噪声源。一般而言，虽然物理噪声源可以产生真随机序列，但是其密码学统计特性并不好。因此，高质量的真随机序列产生器一般采用物理随机源加杂化处理的结构。物理随机源可确保产生序列的真随机性，杂化处理可确保产生序列的好的密

码学统计特性。所以,通常采用这种方法产生高质量的真随机序列并作为高级密钥。中级密钥可以像高级密钥那样产生,但是如果不能方便地利用真随机数产生器产生中级密钥,那么在高级密钥产生后,可以借助高级密钥和一个强的密码算法来产生中级密钥。类似地,初级密钥也可以借助中级密钥和一个强的密码算法来产生。

3.4 密钥分配

密钥管理解决的一个基本问题是密钥的定期更换问题。任何密钥成分都应该有规定的使用期限,制定使用期限的依据不是在这段时间内密码能否被破译,而是从概率的意义上看,密钥机密是否有可能被泄露出去。从密码技术的现状来看,现在完全可以做到使加密设备里的密钥几年不更换,甚至在整个加密设备的有效寿命期间,密钥保持不变,而且其仍然是安全的。但是,加密设备里的密钥在使用多长时间后就有可能被窃取或泄露,这个问题超出了数学的能力。例如,一个花了 100 万美元也难以破译的密码系统,可能只需 1 万美元就能买通密钥管理人员。显然,密钥应经常更换,而且更换密钥时应尽量减少人的参与,实现密钥的自动分配,必要时,一些核心的密钥成分对操作人员也是保密的,使其无法通过实验求解出存放在密封的核心部件里的密钥机密。这就涉及密钥分配问题了。

目前,密钥管理的分配模式分为以下 3 类。

(1) 点对点模式,即通信双方直接管理共享通信密钥。

(2) 密钥分配中心 (Key Distribution Center, KDC) 模式,即通信双方的会话密钥由 KDC 管理生成。

(3) 密钥传递中心 (Key Translation Center, KTC) 模式,即通信双方的会话密钥由发起方产生/获取,并由 KTC 管理传递。

KTC 的功能是为需要通信而又尚未建立共享密钥的双方建立一个用于双方安全通信的共享密钥。KTC 作为可信赖的第三方,其与需要进行通信的双方分别具有共享密钥的加密密钥。与 KDC 建立环境不同的是, KTC 环境中的通信发起方具有产生或获取(数据)密钥的能力。当 KTC 收到来自通信发起方的密钥建立请求后, KTC 依次处理密钥的加密密钥和数据密钥,然后分别用公证密钥和接收方密钥的加密密钥加密发起方产生/获取的数据密钥,再返回给发起方,最后由发起方将经过公证的数据密钥传递给接收方,通信双方依据此数据密钥进行安全会话。

密钥分配中最成熟的方案是采用 KDC 模式,这是当今密钥管理的一个主流,其基本思想如下。

每个节点或用户只要保管与 KDC 之间使用的密钥加密密钥,这样的密钥配置实现了以 KDC 为中心的星形通信网。当两个用户需要相互通信时,只要向 KDC 申请,其就把用密钥加密密钥加密过的工作密钥分别发送给主叫用户和被叫用户,这样对每个用户来说,就不需要保存大量的密钥了,而且真正用于加密明文的工作密钥是一报一换的,可以做到随用随申请随清洗。但这种方法的缺点是通信量大。为了保证 KDC 正常,还应考虑非法的第三方不能插入伪造的服务而取代 KDC。这种验证身份的工作也是 KDC 的工作。

KDC 方式还可以变形为电话号码本方式，适用于公钥密码体制，其可以通过建立用户的公开密码表，在密钥的连通范围内进行散发；也可以采用目录方式进行动态查询，用户在进行保密通信前，首先产生一个工作密钥并使用对方的公钥进行加密传输，对方在获悉这个工作密钥后，使用对称密码体制与其进行保密通信。

此外，还可以采用离散对数方法和智能卡方式，其基本思想是利用数学的方法使别人无法获得密钥。

3.5 密钥保护

密钥保护涉及密钥在传送、注入、存储、更换、销毁等多个方面，以下简要讨论密钥保护中的几个基本问题。

1) 密钥的注入

加密设备里的最高级密钥（高级密钥）通常需要以人工的方式注入。经常采用的把密钥注入到加密设备里的方式有键盘输入、软盘输入、专用的密钥注入设备（密钥枪）输入。除正在进行加密操作的情况以外，密钥一律以加密保护的形式存放。密钥的注入过程应在一个封闭的工作环境，所有接触密钥注入工作的人员应是绝对安全的，不存在可被窃听装置接收的电磁或其他辐射。

在采用密钥枪或密钥软盘进行密钥注入时，应与键盘输入的口令相结合，只有在输入了合法的加密操作口令后，才能激活密钥枪或密钥软盘里的密钥信息，同时建立一定的接口规约。在密钥注入完成后，不允许存在任何可能导出密钥的残留信息，应将内存中使用过的存储区清零。当使用密钥注入设备用于远距离传递密钥时，注入设备本身应设计成像加密设备那样的封闭式的物理、逻辑单元。

在可能的条件下，重要的密钥可采取由多人、多批次分开完成注入的方式，这种方式的代价较大，但提供了多密钥的加密环境。

密钥注入的内容不能被显示出来。为了掌握密钥注入的过程，所有的密钥应按编号进行管理，而这些编号是公开的、可显示的。

2) 密钥的存储

当密钥注入完成后，所有存储在加密设备里的密钥都以加密的形式存放，而对这些密钥进行解密的操作口令应由密码操作人员掌握。这样即使装有密钥的加密设备被破译者拿到，也可以保证密钥系统的安全。

加密设备应具有一定的物理保护措施。最重要的密钥信息应采用掉电保护措施，使得在任何情况下只要一拆开加密设备，这部分密钥就会自动丢失。如果采用软件加密的形式，那么应有一定的软件保护措施。重要的加密设备应有在紧急情况下清除密钥的设计。在可能的情况下，应有对加密设备进行非法使用的审记设计，以把非法口令输入等事件的发生时间记录下来。高级的专用加密装置应做到：无论通过什么方法，如直观的、电子的或其他方法（X射线、电子显微镜），都不可能从加密设备中读出信息。对当前使用的密钥应有密钥的合法性验证措施，以防止其被篡改。

理想的情况是密钥永远不会以未加密的形式暴露在加密设备以外，但这是不可能的。最

简单的密钥存储方案是让用户自己记住密钥，当需要对文件进行加解密时再输入。其他的密钥存储方法：将密钥存储在磁卡中、使用嵌入式 ROM 芯片或智能卡。用户通过卡片使用密钥，但用户并不知道密钥，所以不能泄露它，只能使用它。

不同的存储介质，其安全性不同。如果密钥储存在计算机的硬盘里，那么计算机一旦受到黑客攻击（如被埋置了木马程序），密钥就可能被盗用。

使用软盘或存储型 IC 卡保存密钥的安全性要比硬盘好一些，因为这两种介质仅在使用时才与计算机相连，用完即被拔下，所以证书和私钥被窃取的可能性有所降低。但是黑客还是有机会的，由于软盘和存储型 IC 卡不具备计算能力，因此在进行加密运算时，用户的私钥必须被调出软盘或存储型 IC 卡，从而进入外部计算机。在这个过程中，可能会存在一定的安全隐患。

使用智能卡储存密钥是更为安全的方式。因为智能卡具有一定的计算机的功能，可以在卡内独立生成密钥和加密文件。

产生密钥的程序（指令集）是智能卡生产者烧制在芯片的 ROM 中的，密码算法程序也烧制在芯片的 ROM 中。公私钥对在智能卡中生成后，公钥可以导出到卡外，而私钥则存储在芯片的密钥区，且不允许外部访问。

智能卡中的密钥文件存储在 E2PROM 中。对密钥文件的读写和修改都必须由卡内的程序调用。从卡接口的外面，没有任何一条命令能够对密钥区的内容进行读出、修改、更新和删除等操作。除非设计和编写卡操作系统（COS）的人在 COS 上留了后门，因为只有他才知道如何从外部调出密钥区的内容。但我们可以排除黑客与 COS 设计者相互勾结的这种概率极小的可能性。

在加密和签名的运算过程中，外部计算机中的应用软件使用智能卡 API 调用的方式输入参数、数据和命令，以及启动智能卡内部的数字签名运算、密码运算等，并获得返回结果。由于智能卡内部的 CPU 可以完成这些操作，因此在全过程中，私钥可以不出智能卡介质，黑客的攻击程序也就没有机会截获私钥，这比证书和私钥放在软盘或硬盘上要安全得多。

从物理上讲，对智能卡芯片中的内容进行整体复制也是几乎不可能的。虽然听说有人能够从智能卡芯片在操作过程中发生的微弱电磁场变化或 I/O 接口上反映出的微弱电平变化中分析出芯片中的代码，但现在国际上对智能卡生产商的技术要求很高，要求上述指标要低到不能被测出来。国际上能够生产智能卡的公司只有少数几家，他们都采用了种种安全措施，以确保智能卡内部的数据不能用物理方法从外部复制。

USB Key 和智能卡除 I/O 物理接口不一样以外，内部结构和技术是完全一样的，其安全性也一样。只不过智能卡需要通过读卡器接到计算机的串行接口上，而 USB Key 通过计算机的通用串行总线（USB）接口就可直接与计算机相接。另外，USB 接口的通信速度要远高于串行接口的通信速度。现在出品的计算机已经把 USB 接口作为标准配置，而使用智能卡则需要加配读卡器。出于以上原因，各家 CA 都把 USB Key 作为首选的证书和私钥存储介质而加以推广。美中不足的是，目前 USB Key 的成本还略显昂贵。

3) 密钥的有效期

密钥不能无限期使用，因为密钥的使用时间越长，其泄露的可能越大，而且一旦泄露，损失很大。不同的密钥应具有不同的有效期，基于连接的系统，如电话将通话时间作为密钥

有效期，当再次通话时就启动新的密钥。密钥加密密钥无须频繁更换，因为它们只是偶尔进行密钥交换。而用来加密保存数据文件的加密密钥不能经常交换，因为文件可以加密存储在磁盘上数月或数年。在公钥应用中，私钥的有效期是根据应用的不同而变化的。例如，用于数字签名和身份认证的私钥必须持续数年甚至终身不换；用于抛掷硬币协议的私钥在协议完成后立即销毁。

4) 密钥的更换

一旦密钥的有效期到了，必须清除原密钥存储区，或者用随机产生的噪声重写。为了保证加密设备能连续工作，可以设计成新密钥生效后，旧密码还可以继续保持一段时间，以防止在更换密钥的期间出现不能解密的“死报”。

在密钥更换过程中，不应产生设备服务的中断。密钥更换可以采用批密钥的方式，即一次性注入多个密钥，在更换密钥时，可按照一个密钥的生效，另一个密钥废除的形式进行。替代的次序可采用密钥的序号。如果批密钥的生效与废除是按顺序进行的，那么序数低于正在使用的密钥序号的所有密钥都已过期，相应的存储区应清零。当为了跳过一个密钥而使用强制密钥更换时，由于被跳过的密钥不再使用，因此也应清零。

5) 密钥的销毁

在密钥定期更换后，旧密钥必须销毁。旧密钥是有价值的，即使不再使用，但有了它们，攻击者就能读到由它加密的一些旧消息。要想安全地销毁存储在磁盘上的密钥，应多次对磁盘存储的实际位置进行写覆盖或将磁盘切碎，并写下一个特殊的删除程序，让它查看所有磁盘，寻找在未用存储区上的密钥副本，并将它们删除。

下面是销毁密钥时使用的一些方法。

- (1) 当密钥写在纸上时，应把纸张切碎或烧毁。
- (2) 当密钥存储于 EEPROM 时，应对 EEPROM 进行多次重写。
- (3) 当密钥存储于 EPROM 或 PROM 时，应将 EPROM 或 PROM 打碎成小片。
- (4) 当密钥存储于磁盘时，应多次重写，以覆盖密钥的存储位置，或者将磁盘切碎。
- (5) 特别注意，应对存储于多个地方的密钥进行同时销毁。

本章小结

从对密码算法保密到对密钥保密，现代密码系统的安全取决于密钥的安全，而不是密码算法或加密设备本身的安全。密码算法可以公开，加密设备可以丢失，同一型号的加密设备可以继续使用，但密钥一旦丢失或泄露，那整个保密系统就失败了。本章主要讨论了密钥管理中密钥的组织、产生、分配、保护等一系列技术问题。

思考题

1. 密钥有哪几种分类方法？
2. 请列出几种对称密钥的分配方案。
3. 请简述真随机序列产生的方法。
4. 为保护密钥的安全，我们应该从哪几个方面着手？