第3章 密钥管理

CHAPTER 3

科技前沿 密钥管理发展趋势和研究热点

密钥管理是密码学体系中至关重要的一环，它负责生成、分发、存储和销毁加密密钥，直接关系到信息系统的整体安全性。随着云计算、物联网(Internet of Things，IoT)和区块链技术的迅速发展，密钥管理面临前所未有的复杂挑战。传统的密钥管理方案难以满足分布式环境下海量设备和数据的需求，进而催生了如基于区块链的去中心化密钥管理方案，以及硬件安全模块等新技术。近年来，量子计算的进步加速了对量子安全密钥管理的研究，量子密钥分发因其在理论上能够提供无条件的安全性，而逐步应用于高敏感度的通信领域。同时，后量子密码学也在开发抗量子攻击的密钥管理方案，以应对未来量子计算可能带来的安全威胁。此外，随着零信任架构和安全多方计算的兴起，密钥管理技术正在向更动态、更细粒度的方向演进，确保密钥在跨网络、跨平台环境中的安全流转。自动化的密钥生命周期管理和基于人工智能的密钥管理优化也成为近年来的研究热点，为确保未来数字世界中的信息安全提供了更具前瞻性的解决方案。

3.1 密钥的基本概念

在现代密码学研究中，加/解密算法一般都是公开的，所有的密码技术都依赖于密钥。密码算法确定后，密码系统的保密程度就完全取决于密钥的保密程度，因此，密钥管理是数据加/解密技术中的重要一环，在整个保密系统中占有重要地位。密钥管理方法因所使用的密码体制(对称密码体制和公钥密码体制)而异。如果密钥得不到合理的保护和管理，那么无论算法设计得多么精巧和复杂，保密系统也是脆弱的。密钥管理的目的就是确保密钥的安全性，即密钥的真实性和有效性，进而保证数据保密系统的安全性。一个好的密钥管理系统应该做到：

(1) 密钥难以被窃取；

(2) 在一定条件下密钥被窃取也无意义，因为密钥有使用范围和时间限制；

(3) 密钥的分配和更换过程对用户透明，用户不一定要亲自管理密钥。

密钥是密码学中的基本概念，是指用于加密和解密数据的一串信息。密钥的主要作用是在数据加密过程中将明文转换为密文，或者在解密过程中将密文还原为明文。密钥的安全性直接影响到整个加密系统的安全性。

在现代密码学中，密码算法是可以公开评估的，因而整个密码系统的安全性并不取决于对密码算法的保密或是对加密设备等的保护，决定整个密码算法性能的因素是密钥的保密性。也就是说，在设计密码系统时，需要解决的核心问题是密钥管理问题，而不是密码算法问题。由此带来的优点是：在密码系统中不用担心密码算法的安全性，只要保护好密钥就可以了。显然保护密钥比保护算法要容易得多。再者，在密码系统中可以使用不同的密钥保护不同的秘密信息，这意味着当攻破了一个密钥时，受威胁的只是这个被攻破的密钥所保护的秘密，其他秘密依然是安全的。由此可见，作为密码系统中的可变部分，密钥的安全性决定了密码系统的安全性。

密钥管理是一项综合性的系统过程，要求管理与技术并重，除了技术因素，还与人的因素密切相关，包括密钥管理相关的行政管理制度和密钥管理人员的素质等。密钥系统的安全性总是取决于系统最薄弱的环节，因此再好的技术，若失去了必要的管理的支持，终将使得技术毫无意义。

3.2 密钥的组织结构与分类

3.2.1 密钥的组织结构

为了适应密钥管理系统的要求，目前在现有的计算机网络系统和数据库系统的密钥管理系统的设计中，大都采用了层次化的密钥结构。这种层次化的密钥结构与整个系统的密钥控制关系是对应的。按照密钥的作用与类型及它们之间的相互控制关系，可以将不同类型的密钥划分为一级密钥、二级密钥、……、n 级密钥，从而组成一个 n 级密钥系统，如图 3-1 所示。

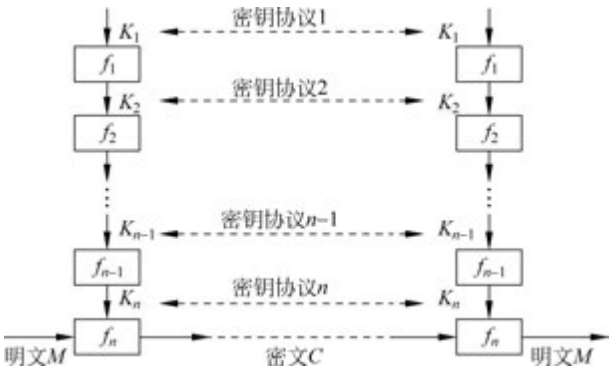

图 3-1 层次化的密钥结构

在图 3-1 中，系统使用一级密钥 K_1 通过算法 f_1 保护二级密钥（一级密钥使用物理方法或其他方法进行保护），使用二级密钥 K_2 通过算法 f_2 保护三级密钥，以此类推，直到最后使用 n 级密钥通过算法 f_n 保护明文数据。随着加密过程的进行，各级密钥的内容动态变化，而这种变化的规则由相应层次的密钥协议控制。

最下面一层的密钥 K_n 也叫工作密钥或数据加密密钥，它直接作用于对明文数据的加/解密。所有上级密钥可称为密钥加密密钥，它们的作用是保护数据加密密钥或作为其他更低级密钥的加密密钥。最上面一层的密钥 K_1 也叫主密钥。通常主密钥是整个密钥管理系

统的核心，应该采用最安全的方式来进行保护。数据加密密钥（即工作密钥）在平时并不存在，在进行数据的加/解密时，工作密钥将在上级密钥的保护下动态地产生（比如，在上级密钥的保护下，通过密钥协商产生本次数据通信所使用的数据加密密钥；或在文件加密时，产生一个新的数据加密密钥，在使用完毕后，立即使用上层密钥进行加密后存储。这样，除了加密部件外，密钥仅以密文的形式出现在密码系统其余部分中）；数据加密密钥在使用完毕后，将被立即清除，不再以明文的形式出现在密码系统中。

一般情况下，可以这样来理解层次化的密钥结构：某一级密钥 K_i 相对于更高级的密钥 K_{i-1} 是工作密码，而相对于低一级的密钥 K_{i+1} 是密钥加密密钥。

层次化的密钥结构意味着以密钥来保护密钥。这样，大量的数据可以通过少量动态产生的数据加密密钥（工作密钥）进行保护，而数据加密密钥又可以由更少量的、相对不变（使用期较长）的密钥加密密钥来保护。同理，在倒数第二层的密钥加密密钥可以由主密钥进行保护，从而保证了除了主密钥可以以明文的形式存储在有严密物理保护的主机密码器件中，其他密钥则以加密后的密文形式存储，这大大提高了密钥的安全性。

3.2.2 密钥的分类

一个密码系统中所使用的密钥的种类是非常繁杂的。对应于层次化的密钥结构，密钥种类的不同表现在层次结构上可能位于不同的层次上，但同时也可能是在相同的层次上具有不同的功能，例如，文件加密密钥和数据加密密钥等；此外，同一密钥在不同的使用环境中也可能属于不同的种类。从具体的功能来看，在一般的密码系统中，密钥可以分为基本密钥、会话密钥（数据加密密钥）、密钥加密密钥和主密钥。

（1）基本密钥（Base Key）：又称为初始密钥（Primary Key）或用户密钥（User Key）。它是由用户选定或由系统分配给用户的，可以在较长时间内（相对于会话密钥）由一对用户（例如，密钥分配中心与某一用户之间，或者两个用户之间）所专用的密钥。在某种程度上，基本密钥还起到了标识用户的作用。

（2）会话密钥（Session Key）：也称为工作密钥或数据加密密钥，是在一次通信或数据交换中，用户之间所使用的密钥，它可由通信用户之间进行协商得到。它一般是动态地、仅在需要进行会话数据加密时产生（或由用户双方进行预先约定），并在使用完毕后立即被清除。会话密钥可以使大家不必很频繁地去更换基本密钥，而是通过密钥分配或者密钥协商的方法得到某次数据通信所使用的数据加密密钥，这样就可以做到一次一密，从而大大提高通信的安全性，并方便密钥的管理。

（3）密钥加密密钥（Key Encrypting Key）：用来对传送的会话密钥或工作密钥或数据加密密钥进行加密时所采用的密钥，也可以称为二级密钥。密钥加密密钥所保护的对象是用来保护通信或文件数据的会话密钥或工作密钥或数据加密密钥。在通信网中，一般在每个节点都分配有一个这类密钥。同时，为了安全，各节点的密钥加密密钥应互不相同。节点之间进行密钥协商时，应用各节点的密钥加密密钥加以完成。

（4）主密钥（Master Key）：对应于层次化密钥结构中的最上面一层，它是对密钥加密密钥进行加密的密钥，通常主密钥都受到了严格的保护。

在实际应用中，除了上述几种密钥外，还有其他类型的密钥，例如：算法更换密钥（Algorithm Changing Key）等。如果从广义的角度来看，它的某些作用是完全可以归结为

上述几类密钥的作用。

3.3 密钥生成和管理

密钥管理包括管理方式、密钥的生成、存储、协商与分配、使用、备份与恢复、更新、撤销和销毁等，涵盖了密钥的整个生存周期。

1. 管理方式

在层次化的密钥管理方式下，用于数据加密的工作密钥需要动态产生；工作密钥由上层的加密密钥来保护，最上层的密钥称为主密钥，是整个密钥管理系统的核心；多层密钥管理体系大大加强了密码系统的可靠性，因为用得最多的工作密钥经常更换，而高层密钥用得较少，使得破译的难度增大。

2. 密钥的生成

密钥的生成是密钥管理的首要环节，如何产生好的密钥是保证密码系统安全的关键。密钥产生设备主要是密钥生成器，一般使用性能良好的生成器产生伪随机序列，以确保产生密钥的随机性。好的密钥生成器应该做到：生成的密钥是随机等概率的、避免弱密钥的使用。假如使用一个弱的密钥产生方法，那么整个系统的安全性将是较弱的。数据加密标准 DES 有 56 位密钥，正常情况下任何 56 位的数据串都可以成为密钥，所以共有 2^{56} 种可能的密钥。在具体实现中，一般仅允许使用 ASCII 码的密钥，并强制每一字节的最高位为 0。在一些实现中，甚至只是将大写字母转换成小写字母，这些密钥程序使得 DES 的攻击难度比正常情况下容易许多。因此，在现代加密技术中，密钥的生成方法必须高度重视。

密钥长度足够长也是保证安全通信的必要条件之一，决定密钥长度需要考虑多方面的因素：数据价值有多大？数据要多长的安全期？攻击者的资源情况怎样？应该注意到，计算机的计算能力和加密算法的发展也是考虑密钥长度的重要因素。随着计算机计算能力的不断提高（根据摩尔定律粗略估计，计算机的计算能力每 18 个月翻一番或以每 5 年 10 倍的速度增长），目前安全的密码长度，或许很快就会变得不安全了，在生成密钥时必须考虑这一点。

还应注意，密钥的生成一般与生成的算法有关。大部分密钥生成算法采用随机或伪随机过程来产生随机密钥。随机数在加密技术中起着重要的作用，随机过程通常采用随机数发生器（实际中是伪随机数发生器），其输出是一个不确定的值；伪随机过程通常采用噪声源技术。常用的噪声源有基于力学、基于电子学和基于混沌理论的噪声源。假如密钥生成的强度并不相等，即采用某种特殊的保密形式，密钥会进行正常的加/解密（称为强算法密钥），而其他密钥都会使得加/解密设备采用非常弱的算法加/解密（称为弱算法密钥），该算法生成的密钥是属于非线性密钥空间，否则属于线性密钥空间。使用非线性密钥空间仅当密钥生成算法是安全的，并且攻击者不能对其进行反控制，或者密钥强度的差异非常细微，以至于攻击者不能感觉或计算出来时才是可行的。

在 ANSI X9.17 标准中规定了一种密钥生成法，这种方法适合在系统中产生会话密钥或伪随机数，是密码强度较高的伪随机数生成器之一，目前已经在 PGP 等许多应用中得到了广泛使用。其中用来生成密钥的加密算法采用的是三重 DES。设 k 为主密钥，W_i 为一

个保密的 64 比特的随机数种子，T_i 为时间戳，E_k 为加密算法，如图 3-2 所示，其中，$R_i = E_k(E_k(T_i) \oplus W_i)$；$W_{i+1} = E_k(E_k(T_i) \oplus R_i)$；$R_i$ 为每次生成的密钥。

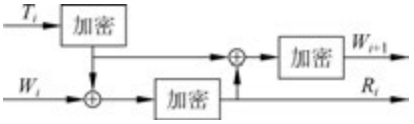

图 3-2　ANSI X9.17 密钥生成

3. 密钥的存储

对所有的密钥都必须有强有力的保护措施，提供密钥服务的密钥装置要求绝对安全，密钥存储要求保证密钥的机密性、认证性和完整性，而且要尽可能减少系统中驻留的密钥量。

密钥的存储分为无介质、记录介质和物理介质等几种。无介质就是不存储密钥，或者说靠记忆来存储密钥。这种方法也许是最安全的，也许是最不安全的。但是一旦遗忘了密钥，其结果就可想而知了。对于只使用短时间通信的密钥而言，也许并不需要存储密钥。记录介质就是将密钥存储在计算机等设备的磁盘上。当然这要求存储密钥的计算机只有授权人才可以使用，否则就不是安全的。如果有非授权的人要使用该计算机，对存储密钥的文件进行加密或许也是一个不错的选择。物理介质是指将密钥存储在一个特殊介质上，如 IC 卡等，显然这种物理介质存储密钥便于携带、安全、方便。

4. 密钥的协商与分配

典型的密钥分配主要有两种形式：集中式和分布式分配。前者主要依靠网络系统中的“密钥管理中心”根据用户需求来分配密钥，后者是根据网络系统中用户主机相互协商来生成(共享)密钥。生成的密钥可以通过安全信道秘密传送(分配)。

5. 密钥的使用

密钥的使用是指从存储介质上获得密钥并进行加密和解密的技术活动。在密钥的使用过程中，要防止密钥被泄露，同时也要在密钥过了使用期时更换新的密钥。在密钥的使用过程中，如果密钥的使用期已到、确信或怀疑密钥已被泄露，或者已被非法更换等，则应该立即停止密钥的使用，并从存储介质上删除密钥。

6. 密钥的备份与恢复

由于密钥在保密通信中具有重要的地位，因此应尽全力对密钥进行保护，密钥备份是指在密钥使用期内，存储一个受保护的副本，用于恢复遭到破坏的密钥。密钥的恢复是指当一个密钥由于某种原因被破坏了，在还没有被泄露出去以前，从它的一个备份重新得到密钥的过程。密钥的备份与恢复保证了即使密钥丢失，由该密钥加密保护的信息也能够恢复。

为了保证安全性，密钥的备份应该以两个或两个以上的密钥分量形式存储，当需要恢复密钥时必须知道该密钥的所有分量。密钥的每个分量应该交给不同的人保管，保管密钥分量的人的身份应该被记录在安全日志上。恢复密钥时，所有保存该密钥分量的人都应该到场，并负责自己保管的那份密钥分量的输入工作。密钥恢复工作同样也应该被记录在安全日志上。

7. 密钥的更新、销毁和撤销

任何密钥的使用都应该遵循密钥的生存周期，绝不能超期使用。因为密钥使用时间越长，重复的概率越大，外泄和被破译的可能性就越大。密钥一旦外泄，必须更换与撤销。在

密钥有效期快要结束时，如果需要继续对该密钥加密的内容进行保护，则需要由一个新密钥来代替，这就是密钥更新。密钥更新可以通过再生密钥来取代原有密钥的方式实现。

没有哪个加密密钥能无限制地使用，对任何密钥的应用，必须像许可证、护照一样能够自动失效，否则可能带来不可预料的后果。主要原因如下所述：密钥使用时间越长，它被泄露的机会就越大；如果密钥已被泄露，那么密钥使用越久，损失就越大；密钥使用越久，人们花费精力来破译它的诱惑力就越大，甚至可能采用穷举法进行攻击；对用同一密钥加密的多个密文进行密码分析一般比较容易。因此，任何密钥都有它的有效期。

密钥必须定期更换，更换密钥后原来的密钥必须销毁。密钥不再使用时，必须删除该密钥的所有副本，生成或构造该密钥的所有信息也应该被全部删除。

在密钥正常的生命周期结束之前，有时需要对密钥进行撤销，比如密钥的安全受到威胁时或实体发生组织关系变动等。密钥的撤销包括撤销相应的证书。

3.4 密钥分配

密钥分配是密码学中的一个重要过程，是指密钥产生后到使用者获得密钥的全过程，也就是如何安全地将密钥在通信双方之间进行传递或共享，以便双方能够加密和解密数据。一般需要完成两个功能，即将密钥分配给通信双方和双方相互认证。但随着网络通信中用户数量的不断增加，密钥的传递与分配将会成为严重的负担。由于密钥的安全性直接决定了加密通信的安全性，因此密钥分配的方式至关重要。密钥的传递分集中传送和分散传送两类。集中传送是指将密钥整体传送，这时需要使用主密钥来保护会话密钥的传递，并通过安全渠道传递主密钥。分散传送是指将密钥分解成多个部分，用秘密分享的方法传递密钥，只要有部分到达就可以恢复密钥。这种方法适合在不安全的信道中传输密钥。

密钥分配技术解决的是网络环境中需要进行安全通信的端实体之间建立共享的对称密钥问题，最简单的解决办法是预先约定一个对称密钥序列并通过安全渠道送达对方，以后按约定使用并更换密钥。这种方式对于具备安全渠道（它本身就可能直接用来传输数据内容）且密钥使用量不大的通信双方是合适的。如果密钥用量较大，更换频繁，则密钥的传递就会成为沉重负担，而且多数用户之间可能并不存在安全的传输渠道，因此需要研究在不安全的通信信道中传递对称密钥的方法。

密钥分配技术一般需要解决两个方面的问题：为减轻负担，提高效率，引入自动密钥分配机制；为提高安全性，尽可能减少系统中驻留的密钥量。为了解决这两个问题，目前有两种类型的密钥分配方案：集中式和分布式密钥分配方案。集中式密钥分配方案是指由密钥分配中心（KDC）或者由一组节点组成层次结构，负责密钥的产生并分配给通信双方。分布式密钥分配方案是指网络通信中各个通信方具有相同的地位，它们之间的密钥分配取决于它们之间的协商，不受任何其他方的限制（更进一步，可以把密钥分配中心分散到所有的通信方，即每个通信方同时也是密钥分配中心）。此外，密钥分配方案也可能采取上面两种方案的混合：上层（主机）采用分布式密钥分配方案，而上层对于终端或它所属的通信子网采用集中式密钥分配方案。

3.4.1 密钥分配的基本方法

在使用对称密码算法进行保密通信时，通信双方必须有一个共享的密钥，并且这个密钥还要防止被他人获得。此外，密钥还必须时常更新。从这点上看，密钥分配技术直接影响密钥分配系统的强度。对于通信双方 A 和 B，密钥分配可以有以下几种方法。

(1) 密钥由 A 选定，然后通过物理方法安全地传递给 B。

(2) 密钥由可信赖的第三方 C 选取并通过物理方法安全地发送给 A 和 B。

(3) 如果 A 和 B 事先已有一密钥，那么其中一方选取新密钥后，用已有的密钥加密新密钥并发送给另一方。

(4) 如果 A 和 B 都有一个到可信赖的第三方 C 的保密信道，那么 C 就可以为 A 和 B 选取密钥后安全地发送给 A 和 B。

(5) 如果 A 和 B 都在可信赖的第三方 C 发布自己的公开密钥，那么 A 和 B 会用彼此的公开密钥进行保密通信。

前两种方法已不适合于大量连接的现代通信(因为需要对密钥进行人工传送)；对于第(3)种方法，由于要对所有的用户分配初始密钥，代价也很大，也不适用于现代通信；对于第(4)种方法采用密钥分配技术，可信赖的第三方 C 就是密钥分配中心，常用于对称密码技术的密钥分配；对于第(5)种方法采用的是密钥认证中心技术，可信赖的第三方 C 就是证书授权中心，常用于非对称密码技术的公钥分配。接下来，分别介绍对称密码算法和非对称密码算法的密钥分配方案。

3.4.2 对称密码算法的密钥分配方案

1. 集中式密钥分配方案

集中式密钥分配方案是指由密钥分配中心(KDC)或者由一组节点组成层次结构，负责密钥的产生并分配给通信双方。在这种方式下，用户不需要保存大量的会话密钥，只需保存同 KDC 通信的加密密钥。其缺点是通信量大，同时要求具有较好的鉴别功能，以鉴别 KDC 和通信方。

图 3-3 就是具有密钥分配中心的密钥分配方案。图 3-3 中假定 A 和 B 分别与 KDC 有一个共享的密钥 K_a 和 K_b，A 希望与 B 建立一个逻辑连接，并且需要一次性会话密钥来保护经过这个连接传输的数据，具体过程如下。

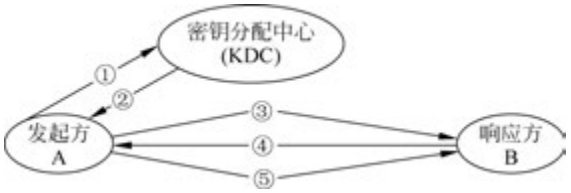

图 3-3 具有密钥分配中心的密钥分配方案

(1) A→KDC：$ID_A // ID_B // N_1$。

A 向 KDC 发出会话密钥请求。请求的消息由两个数据项组成：一是 A 和 B 的身份 ID_A 和 ID_B；二是本次业务的唯一标识符 N_1，每次请求所用的 N_1 都应不同，常用一个时间

戳、一个计数器或一个随机数作为这个标识符。为防止攻击者对 N_1 的猜测，用随机数作为这个标识符最合适。

(2) KDC→A：$E_{K_a}[K_s//\mathrm{ID_A}//\mathrm{ID_B}//N_1//E_{K_b}[K_s//\mathrm{ID_A}]]$。

KDC 对 A 的请求发出应答。应答是由 K_a 加密的信息，因此只有 A 才能成功地对这一信息解密，并且 A 相信信息的确是由 KDC 发出的。

信息中包括 A 希望得到的两项数据：一次性会话密钥 K_s；A 在步骤(1)中发出的请求，包括一次性随机数 N_1(其目的是使 A 将收到的应答信息与发出的请求相比，看是否匹配。因此 A 能验证自己发出的请求在被 KDC 收到之前，未被篡改，而且 A 还能根据一次性随机数确认自己收到的应答没有被重放)。

此外，信息中还包括 B 希望得到的两项数据：一次性会话密钥 K_s；A 的身份 $\mathrm{ID_A}$。这两项由 K_b 加密，将由 A 转发给 B，以建立 A 和 B 之间的连接并用于向 B 证明 A 的身份。

(3) A→B：$E_{K_b}[K_s//\mathrm{ID_A}]$。

A 收到 KDC 响应的信息后，同时将会话密钥 K_s 存储起来，同时将经过 KDC 与 B 的共享密钥加密过的信息传送给 B。B 收到后，得到会话密钥 K_s，并从 $\mathrm{ID_A}$ 可知对方是 A，而且还从 E_{K_b} 知道 K_s 确实来自 KDC。由于 A 转发的是加密后的密文，所以转发过程不会被窃听。

(4) B→A：$E_{K_s}[N_2]$。

B 用会话密钥加密另一个随机数 N_2，并将加密结果发送给 A，并告诉 A，B 当前是可以通信的。

(5) A→B：$E_{K_s}[f(N_2)]$。

A 响应 B 发送的信息 N_2，并对 N_2 进行某种函数变换(如 f 函数)，同时用会话密钥 K_s 进行加密，发送给 B。

实际上，在步骤(3)已经完成了密钥的分配，步骤(4)和步骤(5)两步结合步骤(3)执行的是认证功能，使 B 能够确认所收到的信息不是一个重放。

另外，如果网络中的用户太多，且地域分布很广，那么一个 KDC 将无法承担所有用户的密钥分配任务，一种解决方法是采用分层的 KDC 结构。根据网络中用户数目及分布的地域可以建立两层或两层以上 KDC。

2. 分布式密钥分配方案

分布式密钥分配方案是指网络通信中各通信方具有相同的地位，它们之间的密钥分配取决于它们之间的协商，不受其他方的限制。这种密钥分配方案要求有 n 个通信方的网络需要保存$[n(n-1)/2]$个主密钥。对于较大型的网络，这种方案是不适用的，但是在一个小型网络或一个大型网络的局部范围内，这种方案还是有用的。

如果采用分布式密钥分配方案，则通信双方 A 和 B 建立会话密钥的过程包括以下过程(如图 3-4 所示)。

图 3-4　分布式密钥分配方案

(1) A→B：$ID_A // N_1$。

A向B发出需要会话密钥的请求，内容包括A的标识符ID_A和一次性随机数N_1，告知B(A希望与B通信)，并请B产生一个会话密钥用于安全通信。

(2) B→A：$E_{MK_m}[K_s // ID_A // ID_B // f(N_1) // N_2]$。

B使用与A共享的主密钥M_{K_m}对应答的信息进行加密并发送给A。应答的信息包括B产生的会话密钥K_s，A的标识符ID_A、B的标识符ID_B、$f(N_1)$和一次性随机数N_2。

(3) A→B：$E_{K_s}[f(N_2)]$。

A使用B产生的会话密钥K_s对$f(N_2)$进行加密，并发送给B。

在分布式密钥分配方案中，每个通信方都必须保存$n-1$个主密钥，但是需要多少会话密钥就可以产生多少。由于使用主密钥传送的信息少，所以对主密钥的分析是十分困难的。

3.4.3 非对称密码算法的密钥分配方案

非对称密码算法的密钥分配方案和对称密码算法的密钥分配方案有着本质的区别。在对称密码算法的密钥分配方案中，要求将一个密钥从通信的一方通过某种方式发送到另一方，只有通信双方知道密钥，其他任何人都不知道密钥；而在非对称密码算法的密钥分配方案中，要求私钥只有通信一方知道，其他任何方都不知道，与私钥匹配使用的公钥则是公开的，任何人都可以使用该公钥和拥有私钥的一方进行保密通信。

非对称密码算法的密钥分配方案主要包括两方面的内容：非对称密码算法所用的公钥的分配和利用非对称密码算法来分配对称密码算法中使用的密钥。

1. 公钥的分配

非对称密码算法使得密钥分配变得较容易，但也存在一些问题。在网络系统中无论有多少人，每个人只有一个公钥。获取公钥的途径有多种，包括公开发布、公用目录、公钥机构和公钥证书。

1) 公开发布

公开发布是指用户将自己的公钥发送给另外一个参与者，或者将公钥广播给相关人群。如PGP中使用的RSA算法，用户将自己的公钥附加到消息上，然后发送到公共区域(比如邮件列表中)。但这种方法有一个非常大的缺点：任何人都可以伪造一个公钥冒充他人。

2) 公用目录

公用目录是由一个可信任的系统或组织建立和管理维护的，该公用目录维护一个公开动态目录。公用目录为每个参与者维护一个目录项{标识符，公钥}，每个目录项的信息必须进行安全认证。任何人都可以从这里获得需要保密通信的公钥。与公开发布公钥相比，这种方法的安全性更高。但也有一个致命的弱点，如果攻击者成功地得到目录管理机构的私钥，则可以伪造公钥，并发送给其他人以达到欺骗的目的。

3) 公钥机构

为更严格地控制从目录分配出去的公钥，使之更加安全，需引入一个公钥管理机构来为各个用户建立、维护和控制动态的公用目录。为达到这个目的，必须满足：每个用户都能可靠地知道管理机构的公钥，且只有管理机构知道自己的私钥。这样任何通信双方都可以向该管理机构获得他想要得到的任何其他通信方的公钥，通过该管理机构的公钥便可以判断它所获得的其他通信方的公钥可信度。与单纯的公用目录相比，该方法的安全性更高。但

这种方式也有它的缺点：由于每个用户要想和其他人通信，都需求助于公钥管理机构，因而管理机构可能会成为系统的瓶颈，而且由管理机构维护的公用目录也容易被攻击者攻击。

4）公钥证书

为解决公开密钥管理机构的瓶颈问题，可以通过公钥证书来实现。也就是说，不与公钥管理机构通信，又能证明其他通信方的公钥的可信度，这实际上完全解决了公开发布及公用目录的安全问题。

目前，公钥证书即数字证书是由授权中心（Certificate Authority，CA）颁发的，其中的数据项包括与该用户的私钥相匹配的公钥及用户的身份和时间戳等，所有的数据项由 CA 用自己的私钥签字后形成证书，证书的格式遵循 X.509 标准。证书的格式为：CA＝ESKCA［T，IDA，PKA］，其中，IDA 是用户 A 的身份标识符，PKA 是 A 的公钥，T 是当前时间戳，SKCA 是 CA 的私钥。证书的发放（产生）过程如图 3-5 所示。

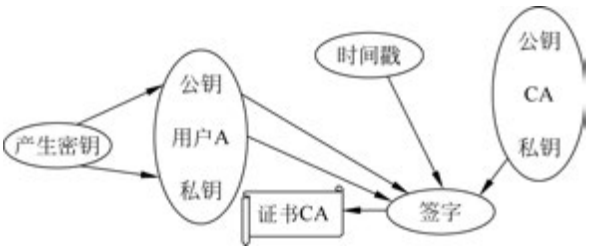

图 3-5　公钥证书的发放过程

用户还可以把自己的公钥通过公钥证书发给另一用户，接收方使用 CA 的公钥 PKCA 对证书加以验证，DPKCA［ESKCA［T，ID_A，PK_A］］＝［T，ID_A，PK_A］。由于只有用 CA 的公钥才能解读证书，这样接收方就验证了证书确实是由 CA 发放的，同时还获得了发送方的身份标识 ID_A 和公钥 PK_A。而时间戳是为了保证接收方收到的证书的有效性，用于防止发送方或攻击方重放一个旧证书（也就是说，时间戳可以被当作截止时间，如果证书过期则被吊销）。

2. 利用非对称密码算法进行对称密码算法密钥的分配

利用非对称密码算法进行保密通信可以很好地保证数据的安全性，但是由于其加密和解密的速度非常慢，实际上非对称密码算法更多的时候是用于对称密码算法密钥的分配。这种分配方式将非对称密码算法和对称密码算法的优点整合在一起，即用非对称密码算法来保护对称密码算法密钥的传送，保证了对称密码算法密钥的安全性；用对称密码算法进行保密通信，由于密钥是安全的，因而通信的信息也是安全的，同时还利用了对称密码算法加密速度快的特点，因此这种方法具有很强的适应性，在实际应用中已被广泛采用。常用的分配方法有以下两种。

1）简单分配

如图 3-6 所示是用非对称密码算法建立会话密钥的过程。假如 A 希望和 B 通信，可以这样建立会话密钥：A 产生一对密钥［PK_A，SK_A］，并把［PK_A // ID_A］（ID_A 是 A 身份标识符）发送给 B；B 产生会话密钥 K_S，并利用 A 的公钥进行加密后得到的 $E_{PK_A}[K_s]$ 发送给 A；A 通过 $D_{SK_A}[E_{PK_A}[K_s]]$ 得到会话密钥 K_S（由于只有 A 才能解密，所以 A 和 B 共享了会话密钥 K_S）；A 销毁［PK_A，SK_A］，B 销毁 PK_A。

2）具有保密和认证功能的密钥分配

针对简单分配密钥的缺点，人们又设计了具有保密和认证功能的非对称密码算法的密钥分配，如图 3-7 所示。

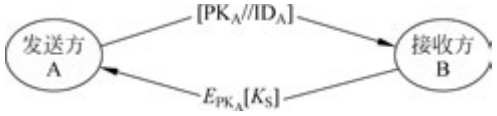

图 3-6　用非对称密码算法建立会话密钥

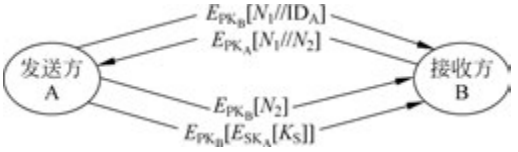

图 3-7　具有保密和认证功能的密钥分配

在图 3-6 中，假定 A 和 B 已经完成了公钥交换，可以这样来建立会话密钥：A 用 B 的公钥 PK_B 加密 A 的身份 ID_A 和一次性随机数（$E_{PK_B}[N_1 // ID_A]$），该随机数唯一地标识本次业务；B 用 A 的公钥 PK_A 加密 A 的一次性随机数 N_1 和 B 新产生的一次性随机数 N_2（$E_{PK_A}[N_1 // N_2]$），由于只有 B 才能对上一步的加密进行解密，所以 B 发送来的信息中的 N_1 的存在使 A 相信对方的确是 B；A 用 B 的公钥 PK_B 对 N_2 加密（$E_{PK_B}[N_2]$）后返送给 B，使 B 相信对方的确是 A；A 选择会话密钥 K_S，然后将 $E_{PK_B}[E_{SK_A}[K_S]]$ 发送给 B（使用 B 的公钥加密是为了保证只有 B 才能解密加密的结果，使用 A 的私钥加密是为了保证该加密结果只有 A 才能发送）；B 使用 $D_{PK_A}[D_{SK_B}[E_{PK_B}[E_{SK_A}[K_S]]]]$ 得到 K_S，从而获得与 A 共享的使用对称密码算法加密的密钥，所以通过 K_S 可以安全地通信。

上述密钥分配过程既具有保密性，又具有认证性，因此既可以防止被动攻击，也可以防止主动攻击。

拓展阅读——密码保护刻不容缓

本章小结

本章介绍了密钥的类型，重点讲解了密钥管理技术的内涵，涉及密钥的整个生存周期，这对我们理解密钥的管理十分重要。随后讲解了对称密钥的分配技术方案、非对称密钥的分配技术方案。通过本章的学习，可掌握密钥的分配技术。

习题与思考题

1. 在现代密码学中，为什么密钥管理起着至关重要的作用？
2. 在密钥管理中为何要引入层次化的结构？密钥有哪些分类？
3. 密钥管理的整个生存周期包括哪些环节？
4. 密钥分配的基本方法有哪些？请说明它们的优势与不足。
5. 对称密码算法的密钥分配方案有哪两类？请分别予以说明。
6. 非对称密码算法的公钥的分配有哪些方案？请说明它们的优势与不足。
7. 利用非对称密码算法进行对称密码算法密钥的分配方案有哪些？请分别予以说明。