此外，由于美国通信专家 Shannon 于 1949 年创立了信息论，人们知道的所有文本、声音、图像、视频信息都能够转换成数字形式，从而可以用功能强大的计算机来处理。到了 20 世纪 70 年代，美国政府已经拥有大量数字化的计算机文件，如何保证这些机密的计算机文件不被偷看、窃取和篡改，成为计算机时代下密码学的一个新任务。

与此同时，电子通信技术也在计算机的支持下迅猛发展。继电话和电报之后，又出现了计算机通信网络。这种通信网络很快遍布全球的每个角落，从而把整个世界联系在一起，从此人类进入信息时代。在信息时代如何保证计算机网络通信和数据传递的安全性，又成为密码学的一个全新任务。

由于计算机的出现，数字化信息的产生和网络通信的发展，促使密码学经历了一场比第二次世界大战时期的机器密码更彻底的革命。在这场革命中出现了一种新的加密对象，既不是几千年来的文字书写，也不是有 100 多年历史的电报字码，而是数字化的文本。

数字化的一个直接后果是，人们从此可以对文本和信息施以复杂的数字运算，以实现种种控制目的，包括加密和解密。于是，大量的代数、组合、数论、概率统计等数学知识被用于密码学，使得它成为数学的一个新分支。

现代密码学的任务已不只限于传统密码学的“保密通信”，而是含义更广的“信息安全”，其中包括“保密通信”、“数据加密”、“数字签名”等重要的功能，并且其应用也远远突破了军事、外交和捷报等传统的范围，开始全面进入经济、商务、科学、教育等人类社会活动的各个领域，从而给我们的工作和生活带来深远的影响。现代密码学已经成为信息时代无处不在且不可缺少的信息安全卫士。

与传统密码学不同，现代密码学设计时，一般总是假设密码系统的结构是公开的，或者至少为敌人所知。这一假设被称为科考夫原则（Kerckhoffs's Principle），是由 19 世纪荷兰密码专家 Auguste Kerckhoffs 首先提出的，该假设之所以在密码学界被普遍接受，是因为它基本符合实际情况，并且据此能简化密码系统的分析、设计和实施。密码系统的结构称作密码算法，进行加密或解密操作所需要的关键参数称作密钥。事实上，在日常社会活动领域中使用的密码算法基本上都是公开的。现代密码学的安全性主要取决于密钥的设计和使用。

根据技术特征，现代密码学可分为三类。

1．对称算法

对称算法是指加密密钥和解密密钥相同的密码算法，又称密码密钥算法或单密钥算法。该类算法又分为流密码算法和分组密码算法。

流密码算法又称序列密码算法，每次加密或解密一位或一字节的明文或密文。

分组密码算法将明文（密文）分成固定长度的数据块（比特块或字节块），用同一密钥和算法对每一明文（密文）块加密（解密）后得到等长的密文（明文）块，然后将密文（明文）块按照顺序组合起来最终得到密文（明文）。

常见的流密码算法包括 RC4；常见的分组密码算法包括 DES、IDEA、RC2、AES、SM4 等。

2．非对称算法

非对称算法是指加密密钥和解密密钥不相同的密码算法，从一个密钥很难推导出另一个密钥，又称公开密钥算法或公钥算法。该算法使用一个密钥进行加密，用另一个密钥进行解密，其中加密密钥可以公开，又称公开密钥或公钥；解密密钥必须保密，又称私有密钥或私钥。

常见的非对称算法包括 RSA、DH、DSA、ECDSA、ECC、SM2 等。

3．摘要算法

摘要算法是指把任意长的输入消息数据转化成固定长度的输出数据的一种密码算法，又称散列函数、哈希函数或杂凑函数、单向函数等。摘要算法所产生的固定长度的输出数据称作摘要值、散列值或哈希值。摘要算法没有密钥。

常见的摘要算法包括 MD5、SHA1、SM3 等。

1.2　密码技术普及推动了密钥管理技术的发展

1.2.1　密钥管理

在密码算法公开的情况下，现代密码学的安全性主要取决于密钥的安全性。如果获得对方当前使用的密钥，密码破译者就可很轻易地从截获的密文中破解出明文来。由于现代密码学依据科考夫公开原则，算法的设计运用了多种数学知识，并经过了大量的学术研究，是很多人的智慧结晶，因此算法自身的安全性很高。密码破译者通过分析算法可能存在的安全漏洞或缺陷，来推测或演算出对方当前使用的密钥，这种方式难度很大，成本也很高。

聪明的密码破译者开始通过其他方式来获取对方当前使用的密钥。如果密钥使用生日、姓名、单词等符号组成，通过多次尝试就可被猜测出来。如果密钥存储不安全，就可以从对方计算机硬盘或内存中获得密钥。也可以在对方传递密钥过程中，截获或者替换密钥。还可以直接贿赂或收买关键人物，直接获得密钥。各种实例说明，从人身上找到漏洞比找到密码系统的漏洞更容易。

于是，密钥管理应运而生，通过对密钥全生命周期进行安全管理，从而实现密钥的安全性。密钥管理主要包括：密钥产生、密钥传输、密钥验证、密钥更新、密钥存储、密钥备份、密钥销毁、密钥有效期、密钥使用等。广义的密钥管理不仅包括密钥如何分发到用户，也包括密钥如何使用。狭义的密钥管理并不包括用户获得密钥后如何使用。

1．密钥产生

目前针对密钥有两种常见的攻击方法：穷举攻击法和字典攻击法。

穷举攻击法就是通过尝试所有可能的密钥来寻找当前使用的密钥。如果使用一台每秒尝试 100 万次密钥的计算机，只需 36 分钟就可以把由小写字母和数字组成的 6 位长的所有密码尝试一遍。2013 年 9 月，世界上最快的计算机每秒运算速度最快可达 5.49 亿亿次，而且计算机的计算能力几乎每 18 个月就增加一倍。

字典攻击法就是把人们最可能使用的所有密码汇聚成一本密码字典，攻击时只尝试该字典中的所有密码。字典攻击法常用于攻击系统口令，是一种特殊的穷举攻击法。计算机上 40% 的口令可以通过字典攻击法破译。

为了抵御穷举攻击法和字典攻击法，密钥长度应足够长，密钥复杂度应足够高，同时应避免出现弱密钥。一般来说，密钥长度越大，对应的密钥空间就越大，攻击者使用穷举猜测密码的难度就越大。由自动处理设备生成的随机比特串是好密钥。对公钥密码算法来说，密钥产生更加困难，因为密钥必须满足某些数学特征。

2. 密钥传输

甲乙双方需要共享一个相同密钥才能进行保密通信。通常由一方先产生一个密钥，然后通过安全方式传递给另一方。

密钥传输方式有多种形式。可以选择人工面对面方式，也可以选择邮寄或快递方式，将密钥副本交给对方。也可以将密钥分成许多不同的部分，然后采用不同方式发送出去：有的通过电话、有的通过快递等。

X9.17 标准描述了两种密钥：密钥加密密钥和数据密钥。密钥加密密钥加密其他需要分发的密钥；而数据密钥只对信息流进行加密。密钥加密密钥一般通过手工分发。

3. 密钥验证

有时密钥在传输中会发生错误。可以通过密钥后面附着一些检错和纠错位，来检测这种错误，如果发生错误，可要求重传密钥。

甲收到乙的密钥后，如何验证该密钥是乙的密钥，而不是丙的密钥呢？一种常用的验证方法是，乙选择一段内容用该密钥加密，然后发给甲，甲解密后如果明文正确，则可以确认该密钥是乙的密钥。

4. 密钥更新

当密钥需要改变时，如何方便地获得新密钥并不是一件容易的事。可以基于旧密钥产生新密钥。如果双方事先共享同一密钥并约定相同的计算方法（如摘要算法），每次密钥更新时对共享密钥或旧密钥计算一次，就可得到新密钥。

5. 密钥存储

密钥可以记忆在大脑中，也可以直接存储到计算机硬盘、智能卡，还可以把密钥分成多个部分，分别存储到不同位置，另外还可以采用其他密钥进行加密保存。

6. 密钥备份

密钥备份可以采用密钥托管、密钥分割、密钥共享等方式。

密钥托管是把密钥交给第三方中心进行保管（如锁在保险柜里或用主密钥加密保存），一旦该密钥丢失（如遗忘密钥或用户意外死亡），按照一定的规章制度，可从该中心索取或恢复该密钥。

密钥分割是把密钥分割成许多碎片，每一碎片本身并不代表什么，但把这些碎片放到一块，就可合成该密钥。

密钥共享是将密钥分成 n 块，知道任意 m（$m<n$）或更多块就能够计算出该密钥，但知道任意 $m-1$ 或更少的块都无法计算出该密钥，该方法又称作（m, n）门限（阈值）方案。

7. 密钥销毁

如果密钥必须替换，旧密钥就必须销毁。旧密钥是有价值的，即使不再使用，有了它们，攻击者就能读到由它加密的一些旧信息。

密钥必须安全地销毁。如果密钥写在纸上，这张纸必须切碎或烧掉。如果密钥存储在硬盘或内存中，存储位置必须使用其他数据多次重写。由于密钥在计算机中很容易被复制并存储到多个地方，应编写特殊的删除程序，查看所有硬盘或内存，寻找可能出现的密钥副本，

彻底删除干净；同时需要记住彻底删除所有临时文件或交换文件的内容。

8．密钥有效期

加密密钥不能无限期使用，主要原因包括：密钥使用时间越长，它泄露的机会就越大；如果密钥已泄露，那么密钥使用越久，损失就越大；密钥使用越久，人们花费精力破译它的诱惑力就越大；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。

对任何密码应用，必须有一个策略能够检测密钥的有效期。不同密钥应有不同的有效期。密钥有效期主要依赖数据的价值和给定时间里加密数据的数量。数据价值越大，加密数据数量越多，所用密钥的有效期就越短，更换越频繁。

9．密钥使用

安全获得密钥后，就可以使用密钥进行保密通信了。进行保密通信时，可以直接使用该密钥对数据进行加解密，但该方式容易造成密钥泄露或容易被对方破解。为避免密钥泄露或破解风险，在进行保密通信时，并不直接使用共享密钥，而是首先基于该密钥产生会话密钥，然后再使用会话密钥对数据进行加解密。

1.2.2　对称密钥管理技术

基于数字化信息和网络通信的现代密码学，其应用范围已远远超出传统的谍报、外交和军事领域，开始向人类几乎所有的社会活动领域渗透，甚至已进入普通民众的日常生活。显然，密码应用的普及推动了密钥管理技术的发展。

19 世纪 70 年代公钥密码思想提出之前，包括传统密码学在内的所有密码技术均属于对称密码范畴，因此密钥管理技术的研究最早是从对称密钥管理入手的。对称密钥管理技术可分为两种模式，如图 1-2 所示。

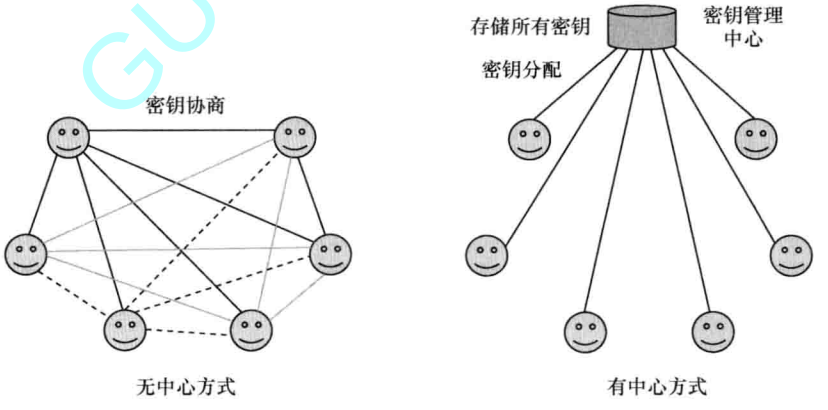

图 1-2　对称密钥管理技术的两种模式

1．无中心模式

每对用户通过协商获得一个共享密钥。为避免两个用户之间共享密钥的安全性不受第三个用户密钥泄露的影响，每对用户之间密钥应互相独立。

当两个用户之间需要保密通信时，为避免密钥泄露，并不直接使用共享密钥对数据进行加解密，而是基于共享密钥产生会话密钥后，使用会话密钥对数据进行加解密。

无中心模式具有以下特点：

（1）密钥协商次数随用户数目呈指数增长。N 个用户时，共需要密钥协商次数为 $N(N-1)/2$。如，N=6 时为 15 次协商，N=1000 时为 500 000 次协商。

（2）每个用户需保存与所有用户的共享密钥。N 个用户时，每个用户需保管 $N-1$ 个密钥。

（3）每对用户之间密钥协商自由灵活，不受其他用户的任何影响。

由于密钥协商次数随用户数目呈指数增长，且每个用户都需要管理与所有用户的共享密钥，因此该模式只适合用于小规模用户场合。

2．有中心模式

存在一个独立的密钥管理中心，每个用户均信任该中心。密钥管理中心为每个用户分配一个密钥，并负责存储和管理所有的用户密钥。当某用户的密钥泄露后，密钥管理中心将该密钥标记为失效。

当两个用户之间需要保密通信时，需要通过密钥管理中心动态验证对方密钥的合法性：（1）该密钥是否失效；（2）该密钥是否是当前用户的。

有中心模式具有以下特点：

（1）密钥分配次数与用户数目呈线性关系。N 个用户时密钥分配次数为 N，且每个用户只需保管 1 个密钥。

（2）由于密钥是随机产生的，无法判断属于哪个用户，因此密钥管理中心需保存密钥与用户的映射关系，存在密钥被泄露和映射关系被篡改的安全风险。

（3）用户之间进行保密通信时，需要通过密钥管理中心动态验证对方密钥的合法性，既无法实现脱机保密通信，又容易导致密钥管理中心成为性能瓶颈。

由于密钥管理中心需安全存储所有密钥及其与用户的映射关系，且需在线验证密钥的合法性，因此该模式不适合于大规模的公众服务领域。

该模式目前比较成熟的应用是磁条卡密码应用体系，已经成为银行体系事实上的密码应用标准，广泛应用于几乎所有国内外银行，通过对区域（如分行、网点等）或终端（如 ATM、POS 等）分配对称密钥，实现银行卡交易过程中的数据安全。具体技术细节，请参考《商业银行密码技术应用》“第三章 磁条卡密码应用体系”。

为避免存储大量的用户密钥，同时实现脱机交易，电子钱包密码应用体系中引入“父子密钥机制”，即基于用户唯一标识（如卡号）由父密钥直接产生子密钥；在所有设备和用户端预先安全存储父密钥，无需保存任何用户密钥，当验证密钥与用户是否匹配时，通过本地存储的父密钥和用户唯一标识就可计算出该用户的密钥，从而实现脱机验证。具体技术细节，请参考《商业银行密码技术应用》“第四章 电子钱包/存折密码应用体系”。

1.2.3 非对称密码技术简化了密钥管理

由于对称密钥管理模式中加密和解密采用相同密钥，在密钥协商或分配时，容易造成密钥泄露且很难发现，直至 19 世纪 70 年代公钥密码思想提出“公钥”和“私钥”之后，才根本性地解决了这个难题。由于公钥可以公开，不存在泄露的风险，因此采用非对称密码技术可以简化密钥管理。同对称密钥管理技术类似，非对称密钥管理技术也可分为两种模式，如图 1-3 所示。