这里我们假定加密密钥和解密密钥都是一样的。但实际上它们可以是不一样的（即使不一样，这两个密钥也必然有某种相关性）。密钥通常由密钥中心提供。当密钥需要向远地传送时，一定要通过另一个安全信道。

密码编码学(cryptography)是密码体制的设计学，而**密码分析学**(cryptanalysis)则是在未知密钥的情况下从密文推演出明文或密钥的技术。密码编码学与密码分析学合起来即为**密码学**(cryptology)。

如果不论截取者获得了多少密文，但在密文中都没有足够的信息来唯一地确定出对应的明文，则这一密码体制称为**无条件安全的**，或称为**理论上是不可破的**。在无任何限制的条件下，目前几乎所有实用的密码体制均是可破的。因此，人们关心的是要研制出**在计算上（而不是在理论上）是不可破的密码体制**。如果一个密码体制中的密码，不能在一定时间内被可以使用的计算资源破译，则这一密码体制称为**在计算上是安全的**。

早在几千年前人类就已经有了通信保密的思想和方法。直到 1949 年，信息论创始人香农(C. E. Shannon)发表著名文章[SHAN49]，论证了一般经典加密方法得到的密文几乎都是可破的。密码学的研究曾面临着严重的危机。但从 20 世纪 60 年代起，随着电子技术、计算技术的迅速发展以及结构代数、可计算性和计算复杂性理论等学科的研究，密码学又进入了一个新的发展时期。在 20 世纪 70 年代后期，美国的**数据加密标准** DES (Data Encryption Standard)和**公钥密码体制**（public key crypto-system，又称为公开密钥密码体制）的出现，成为近代密码学发展史上的两个重要里程碑。

7.2 两类密码体制

7.2.1 对称密钥密码体制

所谓**对称密钥密码体制**，即**加密密钥与解密密钥都使用相同密钥的密码体制**。例如图 7-2 所示的情况，通信的双方使用的就是对称密钥。

数据加密标准 DES 属于对称密钥密码体制。它由 IBM 公司研制出，于 1977 年被美国定为联邦信息标准后，在国际上引起了极大的重视。ISO 曾将 DES 作为数据加密标准。

DES 是一种分组密码。在加密前，先对整个的明文进行分组。每一个组为 64 位长的二进制数据。然后对每一个 64 位二进制数据进行加密处理，产生一组 64 位密文数据。最后将各组密文串接起来，即得出整个的密文。使用的密钥占有 64 位（实际密钥长度为 56 位，外加 8 位用于奇偶校验）。

DES 的机密性仅取决于对密钥的保密，而算法是公开的。DES 的问题是它的密钥长度。56 位长的密钥意味着共有 2^{56} 种可能的密钥，也就是说，共有约 7.6×10^{16} 种密钥。假设一台计算机 1 μs 可执行一次 DES 加密，同时假定平均只需搜索密钥空间的一半即可找到密钥，那么破译 DES 要超过 1000 年。

然而芯片的发展出乎意料地快。不久，56 位 DES 已不再被认为是安全的。

对于 DES 56 位密钥的问题，学者们提出了三重 DES（Triple DES 或记为 3DES）的方案，把一个 64 位明文用一个密钥加密，再用另一个密钥解密，然后再使用第一个密钥加密，即

$$Y = \mathrm{DES}_{K1}(\mathrm{DES}^{-1}{}_{K2}(\mathrm{DES}_{K1}(X)))$$

这里，X 是明文，Y 是密文，$K1$ 和 $K2$ 分别是第一个和第二个密钥，$DES_{K1}(\cdot)$表示用密钥 $K1$ 进行 DES 加密，而 $DES^{-1}{}_{K2}(\cdot)$表示用密钥 $K2$ 进行 DES 解密。

这种三重 DES 曾广泛用于网络、金融、信用卡等系统。

在 DES 之后，1997 年美国标准与技术协会(NIST)，对一种新的加密标准即**高级加密标准** AES (Advanced Encryption Standard)进行遴选，最后由两位年轻比利时学者 Joan Daemen 和 Vincent Rijmen 提交的 Rijndael 算法被选中，在 2001 年正式成为 NIST 的加密标准。在 2002 年成为美国政府加密标准。现在 AES 也是 ISO/IEC 18033-3 标准。

AES 是一种分组密码，分组长度为 128 位。AES 有三种加密标准，其密钥分别为 128 位、192 位和 256 位，加密步骤相当复杂，运算速度比 3DES 快得多，且安全性也大大加强。在 2001 年，NIST 曾有一个大致的估计，就是假定有一台高速计算机，仅用 1 秒钟就能够破译 56 位的 DES（也就是采用穷举法，在 1 秒钟内能够把 DES 所有的 2^{56} 个密钥逐个进行解密运算一遍），那么要破译 128 位的 AES，就需要 10^{12} 年！但是计算机运算速度的提高是很难预测的。因此美国国家安全局 NSA 认为，对于最高机密信息（这类信息必须保证数十年以上的安全性）的传递，至少需要 192 或 256 位的密钥长度。

到 2020 年 5 月为止，尚未见到能够成功破解 AES 密码系统的报道。有人认为，要破解 AES 可能需要在数学上出现非常重大的突破。

7.2.2 公钥密码体制

公钥密码体制的概念是由斯坦福(Stanford)大学的研究人员 Diffie 与 Hellman 于 1976 年提出的[DIFF76]。公钥密码体制**使用不同的加密密钥与解密密钥**。这种加密体制又称为**非对称密钥密码体制**。

公钥密码体制的产生主要有两个方面的原因，一是由于对称密钥密码体制的**密钥分配**问题，二是由于对**数字签名**的需求。

在对称密钥密码体制中，加解密的双方使用的是相同的密钥。但怎样才能做到这一点呢？一种是事先约定，另一种是用信使来传送。在高度自动化的大型计算机网络中，用信使来传送密钥显然是不合适的。如果事先约定密钥，就会给密钥的管理和更换带来极大的不便。若使用高度安全的**密钥分配中心** KDC (Key Distribution Center)，也会使得网络成本增加。

对数字签名的强烈需要也是产生公钥密码体制的一个原因。在许多应用中，人们需要对纯数字的电子信息进行签名，表明该信息确实是某个特定的人产生的。

公钥密码体制提出不久，人们就找到了三种公钥密码体制。目前最著名的是由美国三位科学家 Rivest, Shamir 和 Adleman 于 1976 年提出并在 1978 年正式发表的 **RSA 体制**，它是一种基于数论中的大数分解问题的体制[RIVE78]。

在公钥密码体制中，**加密密钥** PK（Public Key，即**公钥**）是向公众公开的，而**解密密钥** SK（Secret Key，即**私钥**或**密钥**）则是需要保密的。加密算法 E 和解密算法 D 也都是公开的。

公钥密码体制的加密和解密过程有如下特点：

(1) **密钥对**产生器产生出接收者 B 的一对密钥：加密密钥 PK_B 和解密密钥 SK_B。发送者 A 所用的加密密钥 PK_B 就是接收者 B 的公钥，它向公众公开。而 B 所用的解密密钥 SK_B 就是接收者 B 的私钥，对其他人都保密。

(2) 发送者 A 用 B 的公钥 PK_B 通过 E 运算对明文 X 加密，得出密文 Y，发送给 B。

$$Y = E_{PK_B}(X) \tag{7-3}$$

B 用自己的私钥 SK_B 通过 D 运算进行解密，恢复出明文，即

$$D_{SK_B}(Y) = D_{SK_B}(E_{PK_B}(X)) = X \tag{7-4}$$

(3) 虽然在计算机上可以容易地产生成对的 PK_B 和 SK_B，但从已知的 PK_B 实际上不可能推导出 SK_B，即从 PK_B 到 SK_B 是“**计算上不可能的**”。这就是说，除了 B 以外，其他任何人都无法解密出明文 X。

(4) 虽然公钥可用来加密，但却不能用来解密，即

$$D_{PK_B}(E_{PK_B}(X)) \neq X \tag{7-5}$$

(5) 先后对 X 进行 D 运算和 E 运算或进行 E 运算和 D 运算，结果都是一样的：

$$E_{PK_B}(D_{SK_B}(X)) = D_{SK_B}(E_{PK_B}(X)) = X \tag{7-6}$$

请注意，通常都是先加密然后再解密。但仅从运算的角度看，D 运算和 E 运算的先后顺序则可以是任意的。对某个报文进行 D 运算，并不表明是要对其解密。

图 7-3 给出了用公钥密码体制进行加密的过程。

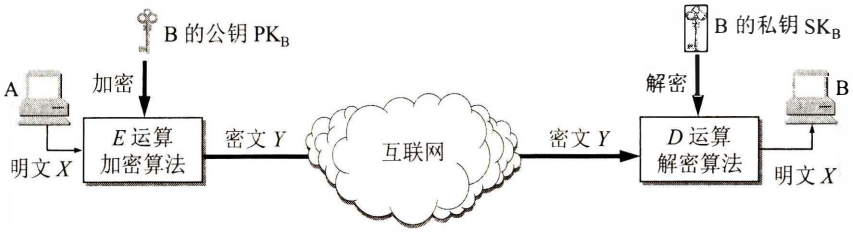

图 7-3　公钥密码体制

公开密钥与对称密钥在使用通信信道方面有很大的不同。在使用对称密钥时，由于双方使用同样的密钥，因此在通信信道上可以进行**一对一的双向保密通信**，每一方既可用此密钥加密明文，并发送给对方，也可接收密文，用同一密钥对密文解密。这种保密通信仅限于持有此密钥的双方（如再有第三方就不保密了）。但在使用公钥密码体制时，在通信信道上可以是**多对一的单向保密通信**。例如在图 7-3 中，可以有很多人同时持有 B 的公钥，并各自用此公钥对自己的报文加密后发送给 B。只有 B 才能够用其私钥对收到的多个密文一一进行解密。但使用这对密钥进行反方向的保密通信则是不行的。在现实生活中，这种多对一的单向保密通信是很常用的。例如，在网购时，很多顾客都向同一个网站发送各自的信用卡信息，就属于这种情况。

请注意，**任何加密方法的安全性取决于密钥的长度，以及攻破密文所需的计算量**，而不是简单地取决于加密的体制（公钥密码体制或传统加密体制）。我们还要指出，公钥密码体制并没有使传统密码体制被弃用，因为目前公钥加密算法的**开销较大**，在可见的将来还不会放弃传统加密方法。