在算法中使用的加密参数叫做密钥（key）。如果P代表明文，K_E代表加密密钥，C代表密文，E代表加密算法（即，函数），那么$C = E(P, K_E)$。这就是加密的定义。其含义是把明文P和加密密钥K_E作为参数，通过加密算法E就可以把明文变为密文。荷兰密码学家Kerckhoffs于19世纪提出了Kerckhoffs原则。该原则认为，加密算法本身应该完全公开，而加密的安全性由独立于加密算法之外的密钥决定。现在所有严谨的密码学家都遵循这一原则。

同样地，当D表示解密算法，K_D表示解密密钥时，$P = D(C, K_D)$。也就是说，要想把密文还原成明文，可以用密文C和解密密钥K_D作为参数，通过解密算法D进行运算。这两种互逆运算间的关系如图9-2所示。

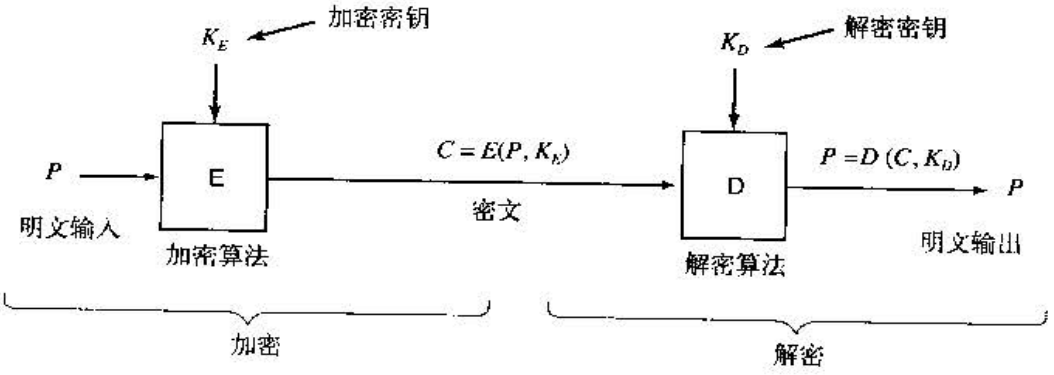

图9-2　明文和密文间的关系

9.2.1　私钥加密技术

为了描述得更清楚些，我们假设在某一个加密算法里每一个字母都由另一个不同的字母替代，如所有的A被Q替代，所有的B被W替代，所有的C被E替代，以下依次类推：

明文：A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

密文：Q W E R T Y U I O P A S D F G H J K L Z X C V B N M

这种密钥系统叫做单字母替换，26个字母与整个字母表相匹配。在这个实例中的加密密钥为：QWERTYUIOPASDFGHJKLZXCVBNM。利用这样的密钥，我们可以把明文ATTACK转换为QZZQEA。同时，利用解密密钥可以告诉我们如何把密文恢复为明文。在这个实例中的解密密钥为：KXVMCNOPHQRSZYIJADLEGWBUFT。我们可以看到密文中的A是明文中的K，密文中的B是明文中的X，其他字母依次类推。

从表面上看，这是一个安全的密钥机制，因为密码破译者虽然知道普通密钥机制（字母与字母间的替换），但他并不知道$26! \approx 4 \times 10^{26}$中哪一个是可能的密钥。但是，给定一小段密文，这个密码还是能够被轻易破译掉。破译的基础在于利用了自然语言的统计特性。在英语中，如e是最常用的字母，接下来是t，o，a，n，i等。最常用的双字母组合有th，in，er，re等。利用这类信息，破译该密码是较为容易的。

许多类似的密钥系统都有这样一个特点，那就是给定了加密密钥就能够较为容易地找到解密密钥，反之亦然。这样的系统采用了私钥加密技术或对称密钥加密技术。虽然单字母替换方式没有使用价值，但是如果密钥有足够的长度，对称密钥机制还是相对比较安全的。对严格的安全系统来说，最少需要使用256位密钥，因为它的破译空间为$2^{256} \approx 1.2 \times 10^{77}$。短密钥只能够抵挡业余爱好者，对政府部门来说却是不安全的。

9.2.2　公钥加密技术

由于对信息进行加密和解密的运算量是可控制的，所以私钥加密体系十分有用。但是它也有一个缺陷：发送者与接受者必须同时拥有密钥。他们甚至必须有物理上的接触，才能传递密钥。为了解决这个矛盾，人们引入了公钥加密技术（1976年由Diffie和Hellman提出）。这一体系的特点是加密密钥和解密密钥是不同的，并且当给出了一个筛选过的加密密钥后不可能推出对应的解密密钥。在这种特性下，加密密钥可被公开而只有解密密钥处于秘密状态。

为了让大家感受一下公钥密码体制，请看下面两个问题：