14.3 对称密钥加密技术

我们来更详细地看看密钥和密码是怎样配合工作的。很多数字加密算法都被称为对称密钥（symmetric-key）加密技术，这是因为它们在编码时使用的密钥值和解码时一样（e=d）。我们就将其统称为密钥 k。

在对称密钥加密技术中，发送端和接收端要共享相同的密钥 k 才能进行通信。发送端用共享的密钥来加密报文，并将得到的密文发送给接收端。接收端收到密文，并对其应用解密函数和相同的共享密钥，恢复出原始的明文（参见图 14-7）。

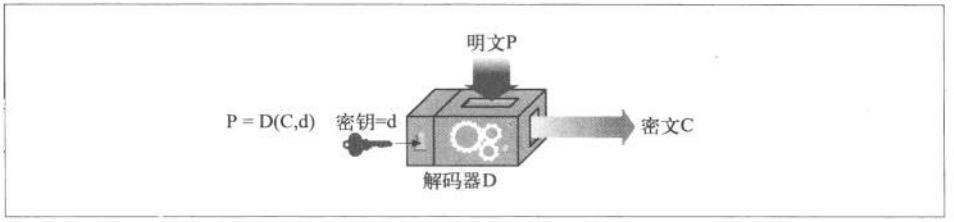

图 14-7 对称密钥加密算法为编 / 解码使用相同的密钥

流行的对称密钥加密算法包括：DES、Triple-DES、RC2 和 RC4。

14.3.1 密钥长度与枚举攻击

保持密钥的机密状态是很重要的。在很多情况下，编 / 解码算法都是众所周知的，因此密钥就是唯一保密的东西了。

好的加密算法会迫使攻击者试遍每一个可能的密钥，才能破解代码。用暴力去尝试所有的密钥值称为*枚举攻击*（enumeration attack）。如果只有几种可能的密钥值，居心不良的人通过暴力遍历所有值，就能最终破解代码了。但如果有大量可能的密钥值，他可能就要花费数天、数年，甚至无限长的时间来遍历所有的密钥，去查找能
313 够破解密码的那一个。

可用密钥值的数量取决于密钥中的位数，以及可能的密钥中有多少是有效的。就对称密钥加密技术来说，通常所有的密钥值都是有效的。[4] 8 位的密钥只有 256 个可能的密钥值，40 位的密钥可以有 2^{40} 个可能的密钥值（大约是一万亿个密钥），128 位的密钥可以产生大约 340 000 000 000 000 000 000 000 000 000 000 000 000 个可能的密钥值。

注 4：有些加密技术中只有部分密钥值是有效的。比如，在最知名的对称密钥加密系统 RSA 中，有效密钥必须以某种方式与质数相关。可能的密钥值中只有少量密钥具备此特性。