```
明文字母: 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
C1(k=5) : f g h i j k l m n o p q r s t u v w x y z a b c d e
C2(k=19) : t u v w x y z a b c d e f g h i j k l m n o p q r s
```

图 8-4 使用两个凯撒密码的多码代替密码

1. 块密码

我们现在跳回到现代社会中来，考察对称密钥加密今天的工作方式。对称加密技术有两种宽泛的类型：**流密码**（stream ciphers）和**块密码**（block ciphers）。当我们研究无线 LAN 的安全性时，将在 8.7 节中简要地研究流密码。在本节中，我们关注块密码，该密码用于多种因特网协议的加密中，包括 PGP（用于安全电子邮件）、SSL（用于使 TCP 连接更安全）和 IPsec（用于使网络层传输更安全）。

在块密码中，要加密的报文被处理为 k 比特的块。例如，如果 $k=64$，则报文被划分为 64 比特的块，每块被独立加密。为了加密一个块，该密码采用了一对一映射，将 k 比特块的明文映射为 k 比特块的密文。我们来看一个例子。假设 $k=3$，因此块密码将 3 比特输入（明文）映射为 3 比特输出（密文）。表 8-1 给出了一种可能的映射。注意到这是一个一对一的映射，即对每种输入有不同的输出。这种块密码将报文划分成 3 比特的块并根据映射关系进行加密。可以验证，报文 010110001111 被加密成了 101000111001。

表 8-1 一种特定的 3 比特块密码

输入	输出	输入	输出
000	110	100	011
001	111	101	010
010	101	110	000
011	100	111	001

继续这个 3 比特块的例子，注意到上述映射只是许多可能映射中的一种。有多少种可能的映射呢？要回答这个问题，观察到一个映射只不过是所有可能输入的排列。共有 $2^3(=8)$ 种可能的输入（排列在“输入”栏中）。这 8 种输入能够排列为 $8!=40\,320$ 种不同方式。因为这些排列的每种都定义了一种映射，共有 40 320 种可能的映射。我们能够将这些映射的每种视为一个密钥，即如果 Alice 和 Bob 都知道该映射（密钥），他们能够加密和解密在他们之间发送的报文。

对这种密码的蛮力攻击即通过使用所有映射来尝试解密密文。仅使用 40 320 种映射（当 $k=3$），这能够在一台桌面 PC 上迅速完成。为了挫败蛮力攻击，块密码通常使用大得多的块，由 64 比特甚至更多比特组成。注意到对于通常的 k 比特块密码，可能映射数量是 $2^k!$，对于即使不大的 k 值（如 $k=64$），这也是一个天文数字。

如刚才所述，尽管全表块密码对于不大的 k 值能够产生健壮的对称密钥加密方案，但不幸的是它们难以实现。对于 $k=64$ 和给定的映射，将要求 Alice 和 Bob 维护一张具有 2^{64} 个输入值的表，这是一个难以实现的任务。此外，如果 Alice 和 Bob 要改变密钥，他们将不得不每人重新生成该表。因此，全表块密码在所有输入和输出之间提供了预先决定的映射（如在上述例子中那样），这简直是不可能实现的事。

取而代之的是，块密码通常使用函数模拟随机排列表。在图 8-5 中显示了当 $k=64$ 时这种函数的一个例子（引自［Kaufman 1995］）。该函数首先将 64 比特块划分为 8 个块，