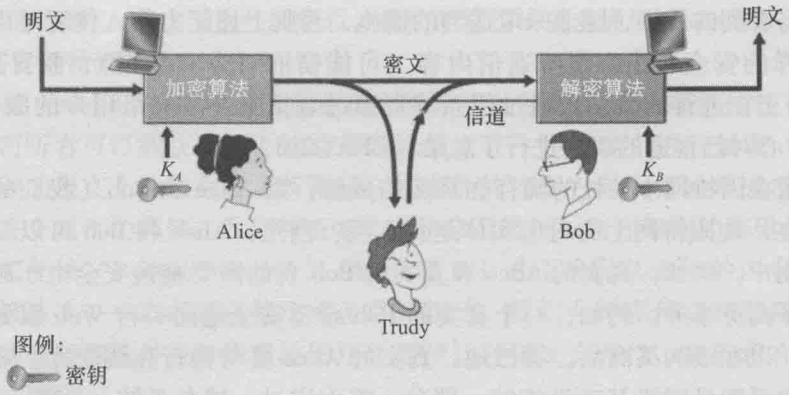

图 8-2 密码学组成部分

在图 8-2 中，Alice 提供了一个**密钥**（key）K_A，它是一串数字或字符，作为加密算法的输入。加密算法以密钥和明文报文 m 为输入，生成的密文作为输出。用符号 $K_A(m)$ 表示（使用密钥 K_A 加密的）明文报文 m 的密文形式。使用密钥 K_A 的实际加密算法显然与上下文有关。类似地，Bob 将为**解密算法**（decryption algorithm）提供密钥 K_B，将密文和 Bob 的密钥作为输入，输出初始明文。也就是说，如果 Bob 接收到一个加密的报文 $K_A(m)$，他可通过计算 $K_B(K_A(m)) = m$ 进行解密。在**对称密钥系统**（symmetric key system）中，Alice 和 Bob 的密钥是相同的并且是秘密的。在**公开密钥系统**（public key system）中，使用一对密钥：一个密钥为 Bob 和 Alice 俩人所知（实际上为全世界所知），另一个密钥只有 Bob 或 Alice 知道（而不是双方都知道）。在下面两小节中，我们将更为详细地考虑对称密钥系统和公钥系统。

8.2.1 对称密钥密码体制

所有密码算法都涉及用一种东西替换另一种东西的思想，例如，取明文的一部分进行计算，替换适当的密文以生成加密的报文。在分析现代基于密钥的密码系统之前，我们首先学习一下**凯撒密码**（Caesar cipher）找找感觉，这是一种加密数据的方法。这种非常古老而简单的对称密钥算法由 Julius Caesar 发明。

凯撒密码用于英语文本时，将明文报文中的每个字母用字母表中该字母后第 k 个字母进行替换（允许回绕，即把字母“a”排在字母“z”之后）。例如，如果 $k=3$，则明文中的字母“a”变成密文中的字母“d”；明文中的字母“b”变成密文中的字母“e”，依此类推。因此，k 的值就作为密钥。举一个例子，明文报文“bob, i love you. alice”在密文中变成“ere, l oryh brx. dolfh”。尽管密文看起来像乱码，但如果你知道使用了凯撒密码加密时，因为密钥值只有 25 个，所以用不了多久就可以破解它。

凯撒密码的一种改进方法是**单码代替密码**（monoalphabetic cipher），也是使用字母表中的一个字母替换该字母表中的另一个字母。然而，并非按照规则的模式进行替换（例如，明文中的所有字母都用偏移量为 k 的字母进行替换），只要每个字母都有一个唯一的替换字母，任一字母都可用另一字母替换，反之亦然。图 8-3 为加密明文的一种可行替换规则。

```
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
密文字母: m n b v c x z a s d f g h j k l p o i u y t r e w q
```

图 8-3 单码代替密码