14.2.2 密码

密码学基于一种名为*密码*（cipher）的秘密代码。密码是一套编码方案——一种特殊的报文编码方式和一种稍后使用的相应解码方式的结合体。加密之前的原始报文通常被称为*明文*（plaintext 或 cleartext）。使用了密码之后的编码报文通常被称作*密文*（ciphertext）。图 14-3 显示了一个简单的例子。

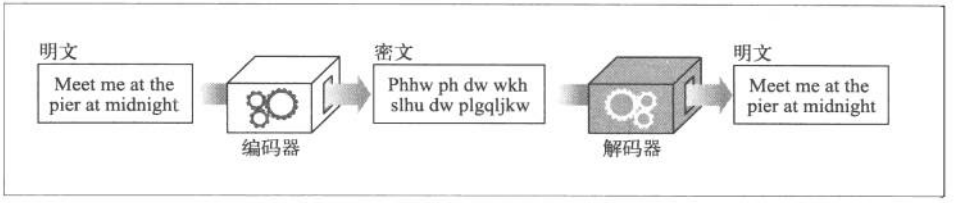

图 14-3　明文和密文

用密码来生成保密信息已经有数千年了。传说尤利乌斯·凯撒（Julius Caesar）曾使用过一种三字符旋转密码，报文中的每个字符都由字母表中三个位置之后的字符来取代。在现代的字母表中，“A”就应该由“D”来取代，“B”就应该由“E”来取代，以此类推。

比如，在图 14-4 中，用 rot3（旋转 3 字符）密码就可以将报文“meet me at the pier at midnight”编码为密文“phhw ph dw wkh slhu dw plgqljkw”。[1] 通过解码，在字母表中旋转 -3 个字符，就可以将密文解密回原来的明文报文。

图 14-4　旋转 3 字符密码实例

310

注 1：为了简化这个例子，我们没有对标点和空格进行旋转，但你可以自己试一试。