14.2.3 密码机

最初，人们需要自己进行编码和解码，所以起初密码是相当简单的算法。因为密码很简单，所以人们通过纸笔和密码书就可以进行编解码了，但聪明人也可以相当容易地“破解”这些密码。

随着技术的进步，人们开始制造一些机器，这些机器可以用复杂得多的密码来快速、精确地对报文进行编解码。这些密码机不仅能做一些简单的旋转，它们还可以替换字符、改变字符顺序，将报文切片切块，使代码的破解更加困难。[2]

14.2.4 使用了密钥的密码

编码算法和编码机都可能会落入敌人的手中，所以大部分机器上都有一些号盘，可以将其设置为大量不同的值以改变密码的工作方式。即使机器被盗，没有正确的号盘设置（密钥值），解码器也无法工作。[3]

这些密码参数被称为*密钥*（key）。要在密码机中输入正确的密钥，解密过程才能正确进行。密码密钥会让一个密码机看起来好像是多个虚拟密码机一样，每个密码机都有不同的密钥值，因此其行为都会有所不同。

图 14-5 显示了使用密钥的密码实例。加密算法就是普通的“旋转 *–N* 字符”密码。*N* 的值由密钥控制。将同一条输入报文“meet me at the pier at midnight”通过同一台编码机进行传输，会随密钥值的不同产生不同的输出。现在，基本上所有的加密算法都会使用密钥。

14.2.5 数字密码

随着数字计算的出现，出现了以下两个主要的进展。

311

- 从机械设备的速度和功能限制中解放出来，使复杂的编 / 解码算法成为可能。
- 支持超大密钥成为可能，这样就可以从一个加密算法中产生出数万亿的虚拟加密算法，由不同的密钥值来区分不同的算法。密钥越长，编码组合就越多，通过随机猜测密钥来破解代码就越困难。

注 2：最著名的机械编码机可能就是第二次世界大战期间德国的 Enigma 编码机了。尽管 Enigma 密码非常复杂，但阿兰·图灵（Alan Turing）和他的同事们在 20 世纪 40 年代初期就可以用最早的数字计算机破解 Enigma 代码了。

注 3：在现实中，机器逻辑可能会指向一些可利用的模式，所以拥有机器逻辑有时会有助于密码的破解。现代的加密算法通常都设计为，即使大家都知道这些算法，恶意的攻击者也很难发现任何有助于破解代码的模式。实际上，很多功能最强大的密码都会将其源代码放在公共域中，供大家浏览和学习！