此外，由于IV值在该帧中以明文形式传输，窃听者就会发现何时使用了一个重复的IV值。

为理解重复使用一个密钥可能出现的几个问题之一，考虑下面的选择明文攻击的情况，仍以Trudy对Alice进行攻击为例。假定Trudy（可能使用IP哄骗）向Alice发出一个请求（例如，一个HTTP或FTP请求），要求Alice传输内容已知的文件$d_1, d_2, d_3, d_4, \cdots$，Trduy也观察到Alice发送的已加密数据$c_1, c_2, c_3, c_4, \cdots$，由于$d_i = c_i \oplus k_i^{IV}$，如果在这个等式两边同时异或$c_i$，可得到：

$$d_i \oplus c_i = k_i^{IV}$$

根据这个关系，Trudy就可以使用已知的d_i和c_i值计算出k_i^{IV}。下一次Trudy看到使用同一IV值时，她将知道密钥流为$k_1^{IV}, k_2^{IV}, k_3^{IV}, \cdots$，并可使用这些密钥解密报文。

对于WEP还有其他几个值得关注的安全性问题。[Fluhrer 2001]描述了一种攻击方法，即当选择某些弱密钥时在RC4中暴露出的一种已知弱点。[Stubblefield 2002]讨论了实现和开发这种攻击的有效方法。对WEP的另一种关注与在图8-30中显示并在802.11帧中传输的用以检测载荷中改变的比特的CRC比特有关。然而，攻击者在改变加密内容（例如用乱七八糟的东西替代初始的加密数据）后，对这些被替换的东西计算出一个CRC，并将该CRC放置在WEP帧中产生一个将被接收方接受的802.11帧。此时所需要的是诸如我们在8.3节中学习的报文完整性技术来检测内容篡改或替换。有关WEP安全性更多的细节，参见[Edney 2003；Walker 2000；Weatherspoon 2000]及其中的参考文献。

8.8.2 IEEE 802.11i

在IEEE 802.11于1999年发布后不久，就开始研发具有更强安全性机制的802.11的新型、改进版本。这个新标准被称为802.11i，于2004年最终得到批准。如我们将看到的那样，虽然WEP提供了相对弱的加密、仅有单一方式执行鉴别并且没有密钥分发机制，但IEEE 802.11i却提供了强得多的加密形式、一种可扩展的鉴别机制集合以及一种密钥分发机制。下面我们概述一下802.11i；[TechOnline 2012]是一篇关于802.11i的优秀（流式音频）技术概述。

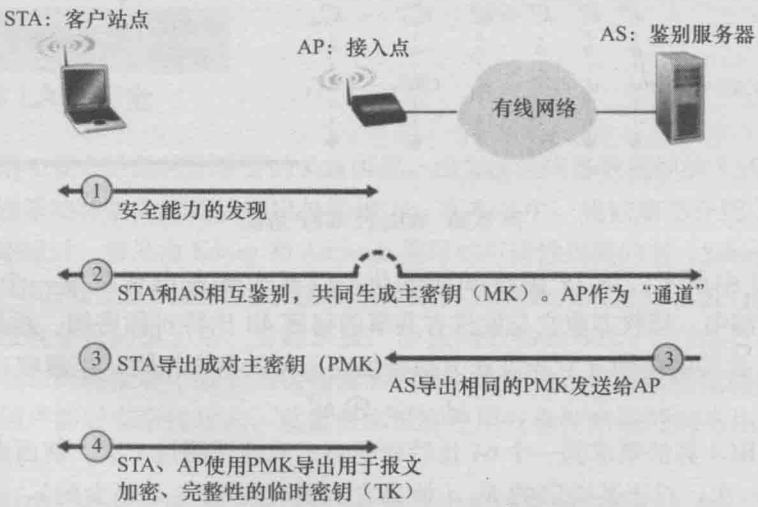

图8-31 802.11i：运行的4个阶段

图8-31概述了802.11i的框架。除了无线客户和接入点外，802.11i定义了一台鉴别服务器，AP能够与它通信。鉴别服务器与AP的分离使得一台鉴别服务器服务于许多AP，