图 20-21 显示了解密电子邮件过程。

图 20-21　S/MIME 邮件解密过程

邮件加密和解密过程提供了电子邮件的保密性。此过程解决了 Internet 电子邮件中的重大缺陷：任何人都可以阅读任何邮件。

4．数字签名与邮件加密

数字签名和邮件加密并不是相互排斥的服务，每个服务都可解决特定的安全问题。数字签名解决身份验证和认可问题，而邮件加密则解决保密性问题。由于每个服务解决不同的问题，因此邮件安全策略通常同时需要这两个服务。这两个服务被设计为一起使用，因为它们分别针对发件人和收件人关系的某一方。数字签名解决了与发件人有关的安全问题，而加密则主要解决与收件人有关的安全问题。

同时使用数字签名和邮件加密时，用户会同时从这两个服务中受益。在邮件中采用这两个服务不会改变其中任何一个服务的处理过程。

（1）发送邮件

邮件签名与加密过程的具体步骤如下：

① 捕获邮件。

② 检索用来唯一标识发件人的信息。

③ 检索用来唯一标识收件人的信息。

④ 使用发件人的唯一信息对邮件执行签名操作，以产生数字签名。

⑤ 将数字签名附加到邮件中。

⑥ 使用收件人的信息对邮件执行加密操作，以产生加密的邮件。

⑦ 用加密后的邮件替换原始邮件。

⑧ 发送邮件。

图 20-22 显示了对电子邮件进行签名和加密的过程。

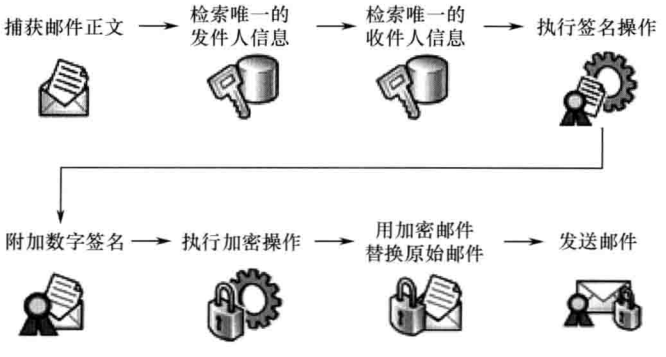

图 20-22　S/MIME 邮件签名与加密过程

（2）接收邮件

邮件解密和验签过程的具体步骤如下：

① 接收邮件。

② 检索加密邮件。

③ 检索用来唯一标识收件人的信息。

④ 使用收件人的唯一信息对加密邮件执行解密操作，以产生未加密的邮件。

⑤ 返回未加密的邮件。

⑥ 将未加密的邮件返回给收件人。

⑦ 从未加密的邮件中检索数字签名。

⑧ 检索用来标识发件人的信息。

⑨ 使用发件人的信息对未加密的邮件执行签名操作，以产生数字签名。

⑩ 将邮件所附带的数字签名与收到邮件后所产生的数字签名进行比较。如果数字签名匹配，则说明邮件有效。

图 20-23 显示了对数字签名进行解密和验证的过程。

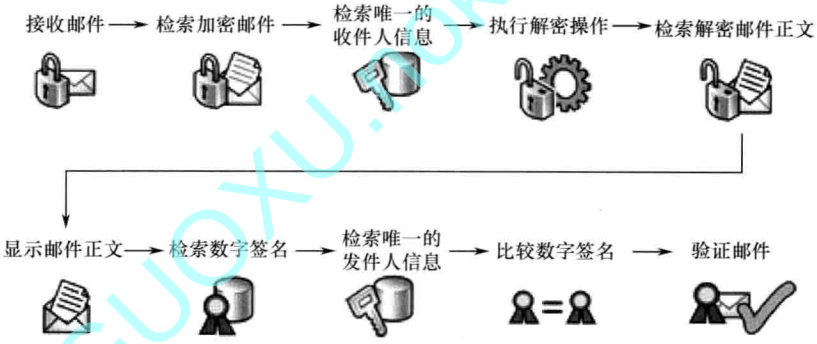

图 20-23　S/MIME 邮件解密与验签过程

5．三层包装邮件

S/MIME 版本 3 的一个值得注意的增强功能是“三层包装”。三层包装的 S/MIME 邮件是指经过签名、加密、再次签名的邮件。这个额外的加密层为邮件提供了更高一层的安全性。

第21章 常见应用

21.1 防止假网站与Web服务器证书

本节以网上银行为例来说明如何防止假网站诈骗。

21.1.1 假网站

1. 什么是假网站诈骗

假网站诈骗是“网络钓鱼”的一种，通常是指不法嫌疑人未经许可，以某家银行的名义，通过互联网建立貌似银行网站或网上银行的假网页，并借此发布虚假消息，搜集客户资料，骗取客户网上银行注册卡号（登录ID）、密码、口令等信息，进而达到非法窃取客户资金的目的。

假网站这种欺诈手法最初出现在北美，2003年开始在亚洲蔓延，并相继在中国香港地区发生了多宗利用假网站骗取客户网上银行账户口令和资金的案例。从2004年开始，假冒银行网站开始在中国大陆出现，网络安全事件也频繁见诸于媒体，使网上银行安全性问题成为公众关注的焦点。仅针对工商银行网银的诈骗假网站就多达几百个。

2. 假网站的表现形式

① 假网站的网址与真网站网址较为接近。由于注册域名的成本非常低，不法分子为增强假网站的欺骗性，往往使用和真实网站网址非常相似的域名。

② 假网站的页面形式和内容与真网站较为相似。假冒网站的页面往往使用正规网站的LOGO、图表、新闻内容和链接，而且在布局和内容上与真实网站非常相似。

3. 不法分子欺诈的通常手法

（1）通过病毒传播假网站信息

不法分子克隆一个与银行网站一模一样的网页，并且使用的登录地址也与银行网站的地址非常接近，然后使用一些电脑病毒程序、垃圾软件等将假网站地址发送到客户的电脑上，或放在搜索网站上诱骗客户登录，以窃取客户卡号、密码等信息。如工行曾经发现的“http://www.1cbc.com.cn”、“http://mybank.iclc.com.cn/”、“http://www.icbc.dizhen.com”等假网站，与工行网站地址http://www.icbc.com.cn、https://mybank.icbc.com.cn十分相似。

（2）通过手机短信，冒充银行名义发送诈骗短信

不法分子利用手机短信，冒充银行名义向客户发送诈骗短信，声称客户中奖或账户被他人盗用等，要求客户尽快登录到短信中指定的网站进行身份验证。而该网站是不法分子建立的、用于套取客户信息的假网站，如果客户登录该网站并进行操作，客户的卡号、密码、身份证件等信息将会被不法分子获悉。

（3）冒充银行邮箱，发送虚假信息引诱客户登录假网站

不法分子以垃圾邮件的形式大量发送欺诈性邮件，这些邮件多以中奖、顾问、对账等内容，或是以银行账号被冻结、银行系统升级等各种理由，要求收件人点击邮件上的链接地址，登录一个酷似银行网页的界面，而用户一旦在这个指定的登录界面输入了自己的卡（账）号、密码等，这些信息就会被窃取。近期发现，不法分子以所谓“中国工商银行网络安全科”的名义，向客户发送电子邮件，谎称持卡人账户被冻结，并要求客户到指定的网页修改密码。

（4）建立假电子商务网站，通过假的支付页面窃取客户网上银行信息

不法分子首先建立一个假的电子商务网站，然后在电子商务网站（如淘宝网、腾讯网等）发布虚假的商品信息，该信息中的商品价格往往比市场同类商品便宜很多，同时不法分子还会留下自己的 QQ 号或者 MSN 等即时通信工具号码以及假电子商务网站的网址。当客户对该网站销售的便宜商品动心，并通过该网站购物进行支付时，就会链接到一个假的银行支付页面，客户在假支付页面输入的卡号、密码等信息就会被不法分子获取。

21.1.2 使用 Web 服务器证书预防假网站

1. 网站申请 Web 服务器证书

（1）生成证书请求文件

不同 Web 服务器生成证书请求的方式不同。

针对支持 JSP 的 Web 服务器，如 Tomcat、WebSphere、WebLogic 等，需要使用 JDK 自带的工具 keytool 生成证书请求文件。keytool –genkey 产生密钥对。keytool –certreq 产生证书请求文件。

针对 IIS 系统，使用 Microsoft 提供的管理工具，按照 IIS 证书向导的操作提示即可生成证书请求文件。

证书请求文件内容的格式遵循 PKCS#10 规范，其中包含网站基本信息和网站 RSA 公钥，如下例所示：

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDSDCCArECAQAwbTESMBAGA1UEAxMJbG9jYWxob3N0MRUwEwYDVQQLHgxbiVFo
i6SLwU4tX8MxETAPBgNVBAoeCFMXedFmelNaMQ8wDQYDVQQHHgZtd23AUzoxDzAN
BgNVBAgeBlMXTqxeAjELMAkGA1UEBhMCQ04wgZ8wDQYJKoZIhvcNAQEBBQADgY0A
MIGJAoGBAMFbTnn0+hOmJc+jSV3FJDpe0seH2ojbzESzEudIoMxNfSTlg3Vi0gyx
0WP1JYbnXMB1g6q/ZAUOtU0nCCs9hVqFj2irrm66GN1UjhqrcWsJjbgNSAf2C3Nx
O0ygc91/Dl0LHXhcs5p3p5cv6bTcC0wEh7G3wGYH7ZG/PM3CDcs3AgMBAAGgggGZ
MBoGCisGAQQBgjcNAgMxDBYKNS4xLjI2MDAuMjB7BgorBgEEAYI3AgEOMW0wazAO
BgNVHQ8BAf8EBAMCBPAwRAYJKoZIhvcNAQkPBDcwNTAOBggqhkiG9w0DAgICAIAw
DgYIKoZIhvcNAwQCAgCAMAcGBSsOAwIHMAoGCCqGSIb3DQMHMBMGA1UdJQQMMAoG
CCsGAQUFBwMBMIH9BgorBgEEAYI3DQICMYHuMIHrAgEBHloATQBpAGMAcgBvAHMA
bwBmAHQAIABSAFMAQQAgAFMAQwBoAGEAbgBuAGUAbAAgAEMAcgB5AHAAdABvAGcA
cgBhAHAAaABpAGMAIABQAHIAbwB2AGkAZABlAHIDgYkAbII1TrHis4afw+wbLrZI
OYe1boagX3QNyHNj4kpktRyBgIFt6WofQ1nXK6TXmpAm2/AmY20/h+a1GZ1/vn7E
EzHcNQfjvHoSZH7yU5FzvBVs5PGGZ//dlrlYX0iY8qhQicTdPQT3MRoYjUKBvi7I
```

RJnfbWbpQKIZSweblEKN1IYAAAAAAAAAADANBgkqhkiG9w0BAQUFAAOBgQCtkhCM
XPmXwVw2TXBSLHXmj+21LD4VPF5pi/rg+itp3iFxQQ9A7hmaH8ICIFlBjx6dQUda
De1fNCa34E1nOfP3epZQAGqdyO2ulQ9CsTkmi+bP705tj9t2zU6G7gfYh+qvWnO4
ByupOjtwjLPzAlRBPX7SRPaKcgnlH+YMAJVI5Q==
-----END NEW CERTIFICATE REQUEST-----

（2）签发证书

将证书请求文件内容提交给 CA 系统，CA 系统解析该 PKCS#10 请求包，获得网站基本信息和网站 RSA 公钥，然后使用 CA 私钥为该网站签发 Web 服务器证书。

（3）安装证书

不同 Web 服务器安装证书的方式不同。

针对支持 JSP 的 Web 服务器，如 Tomcat、WebSphere、WebLogic 等，需要使用 JDK 自带的工具 keytool 安装证书。用 keytool –import 导入证书。

针对 IIS 系统，使用 Microsoft 提供的管理工具，按照 IIS 证书向导的操作提示即可完成证书安装。

（4）启用 SSL

不同 Web 服务器启用 SSL 的方式不同。

有些 Web 服务器需要手工修改配置文件来配置并启用 SSL。如 Tomcat，需要修改 server.xml 文件。有些 Web 服务器使用管理工具配置并启用 SSL。如 IIS，使用 Microsoft 提供的管理工具。

2．用户鉴别真假网站

（1）核对网站域名

假网站的网址与真网站网址较为接近，需要自己辨别其不同之处。如假冒网站通常将英文字母 I 替换为数字 1，CCTV 被换成 CCYV 或者 CCTV-VIP 这样的仿造域名。

（2）关注浏览器提示

当用户访问安装 Web 服务器证书的网站时，用户浏览器与网站之间将建立 SSL 加密通道。鉴于数字证书技术的复杂性，为降低该技术使用的复杂性和提高用户使用的方便性，浏览器中已经预装多个可信的 CA 证书，同时浏览器将帮助用户对 Web 服务器证书的有效性进行自动验证。

当发现如下疑问或异常时，浏览器将向用户进行提示，部分情况将由用户选择是否继续进行：

① 浏览器没有找到可信的 CA 证书来验证 Web 证书中数字签名是否正确。

② Web 证书中起始日期 NotBefore 在当前日期之后，或终止日期 NotAfter 在当前日期之前。

③ Web 证书中申请者的 CN 项与当前访问的网站域名或 IP 不一致。

④ Web 证书中密钥用途 KeyUsage、ExtKeyUsage 不正确。

（3）核对安全证书

用户浏览器与网站建立 SSL 加密通道成功后，IE 浏览器右下角的状态栏上会显示一个“挂锁”图形的安全证书标识。单击挂锁，将显示该网站证书的内容，如图 21-1 所示。