文章编号:1000 - 582X(2005)06 - 0077 - 04

# 基于 Microsoft 密码体系的数字信封的实现*

周 城,郭 正 荣
(重庆通信学院 研究生管理大队,重庆 400035)

**摘 要**:介绍了微软密码体系结构和组成、Microsoft 证书的管理和使用方法,详细说明了利用证书和 CryptoAPI(cryptographic application programming interface,加密应用程序接口)函数实现数字信封的原理、步骤以及算法. 最后,利用 Win2K 颁发的数字证书、算法对多个文本数据进行加解密处理,结果表明所实现的数字信封技术能够保证信息传输的保密性和真实性,算法速度快,能满足实际应用的要求.

**关键词**:加密应用程序接口;加密服务提供者;对称/对称加密算法;数字证书;数字信封
**中图分类号**:TP309.7 **文献标识码**:A

随着计算机网络技术的迅猛发展,网络安全问题变得日益突出和复杂,并受到前所未有的关注和重视. 特别是我国电子签名法颁布后,信息安全服务需求越来越大,人们对网络信息安全问题的研究也更加深入.

目前,加密技术在实际应用中有对称加密和非对称加密. 对称加密速度快,常用来加密大批量的数据,但需要预先分配密钥. 非对称加密克服了对称加密的一些诸如密钥分配和管理复杂、无法验证发送者和接收者身份等缺点,但是它运算量大,速度慢. 为此,笔者提出数字信封技术,主要通过数字证书的引入,将两种加密方法结合起来,用选定的对称密钥和对称加密算法加密明文,用非对称加密方法来加密这个对称密钥,实现密钥交换,从而保证加解密的高速要求以及数据与密钥的传输安全.

## 1 Microsoft 密码体系结构

微软密码系统主要包含 3 个要素:应用程序、操作系统和 CSP(cryptographic service provider 加密服务提供者)[1]. 应用程序通过 CryptoAPI 与操作系统通信,操作系统则通过 CryptoSPI(CSP 模块接口)与 CSP 通信. 应用程序调用操作系统动态链接库中的 CryptoAPI 函数,操作系统分析这些函数调用并通过 CryptoSPI 将这些调用传递给相应的 CSP,由 CSP 完成具体加密算法的实现.

其体系结构如图 1 所示[2].

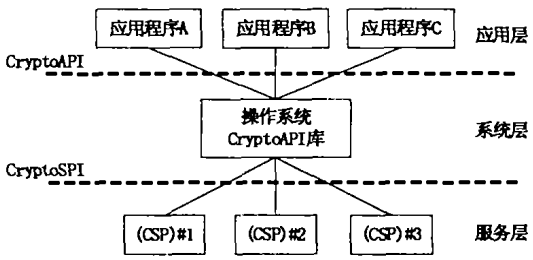



图 1 微软密码体系结构

## 2 Microsoft CryptoAPI

目前有关加密 API 国际标准和规范主要有:GSS - API V2.0, GCS - API, CDSA, RSA PKCS#11 Cryptographic Token Interface Standard V2.01, RSA BSAFE API, 微软 CryptoAPI V2.0. 其中,CDSA, RSA PKCS#11 和微软 CryptoAPI 在实际中应用得较多.

### 2.1 Microsoft CryptoAPI 体系结构

Microsoft CryptoAPI 是 Microsoft 公司提出的安全加密应用框架和服务. 它提供了在 Win32 环境下使用认证、编码、加密和签名等安全服务时的标准加密接口,用于增强应用程序的安全性与可控性. 应用开发者可以在不了解复杂的加密机制和加密算法情况下,简便、快速地开发出标准、通用和易于扩展的安全加密应用. 其体系结构如图 2 所示[3].

### 2.2 加密服务提供者 CSP

CSP 是微软提供的加密应用程序接口 CryptoAPI 所需的独立模块,它完成具体加密算法的实现,通常有

* 收稿日期:2005 - 01 - 23
作者简介:周城(1963 - ),男,江苏无锡人,重庆通信学院副教授,硕士,主要研究方向:信息安全,指挥自动化.

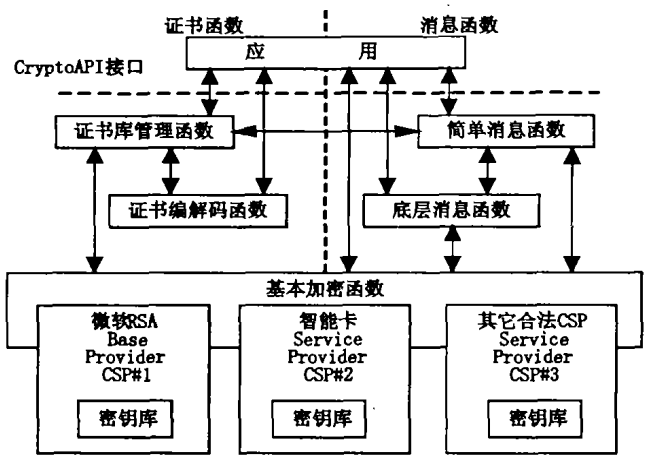



**图 2 微软 CryptoAPI 体系结构**

硬件实现和软件实现两种情况. 用软件实现的 CSP 以加密方式把密钥对存储在注册表中,硬件 CSP 将密钥对存储在永久的硬件中. 任何一个加密服务提供者若想成为微软合法 CSP,就必须获得微软授予的一个签名文件,该签名文件保证了微软 CryptoAPI 识别该 CSP[3]. 并且,微软要定期验证其签名,验证完整性,以保证 CSP 没有被非法修改.

每个 CSP 都有一个名字和类型,在类型中列出了它们各自支持的密钥交换算法、签名算法、对称加密算法和 hash 算法(哈希算法);每个 CSP 都有一个用于存储密钥的密钥库,密钥库中有一个或多个密钥容器. 每个密钥容器都有一个惟一的名字,它包含一个特定用户所有的密钥对,比如,签名密钥对,交换密钥对等.

### 2.3 CryptoAPI 函数组成

CryptoAPI 通过一系列的库函数来对应用程序提供安全功能,目前 CryptoAPI 的最新版本是 2.0 版,在包含 CryptoAPI 1.0 的全部功能外,还增加了证书管理功能,为网络身份认证提供了保证. 它共有 5 部分函数组成:简单消息函数、低层消息函数、基本加密函数、证书编解码函数和证书库管理函数. 其中前三者可用于对敏感信息进行加密或签名处理,保证网络传输信息的保密性、完整性;后两者通过对证书的使用,保证网络信息的可认证性[4].

## 3 基于 Microsoft 证书和 CryptoAPI 函数的数字信封的实现

### 3.1 Microsoft 证书的管理和使用

数字证书,又叫数字标识,是由认证中心发放并经认证中心数字签名的一种电子文件. 它包含公开密钥拥有者相关信息、颁发者(认证中心)相关信息以及公开密钥相关信息等[5]. 用数字证书标识用户身份是网络中身份认证的主要途径之一. Microsoft 所有的证书都在证书库中,证书一般都存储到永久介质中,如电子令牌、IC 卡中. 每个用户都有存放自己证书的证书库(MY 库),用户拥有包含证书颁发机构的公钥的根证书,根证书一般存放在注册表中 ROOT 库中[6].

微软证书的管理一般经历打开证书库,查找证书,增加、删除、修改和保存证书,最后关闭证书库等步骤. 微软证书的使用一般经历打开证书库,查看证书及证书属性,利用证书进行身份认证、加密与解密、数字签名与验证等安全处理,最后关闭证书库等步骤.

### 3.2 数字信封的实现原理及步骤

数字信封的实现的基本原理是发送方首先随机生成一对称(会话)密钥,利用该对称密钥加密明文,再用接收方的公钥加密对称密钥,最后将密文及加密后的对称密钥一起传递给接收方;接收方收到信息后,首先将自己的私钥解密对称密钥,再用对称密钥解密密文,这样就得到了明文.

下面介绍利用证书和 CrytptoAPI 函数的一种数字信封的具体实现方法.

#### 3.2.1 数字信封的包装

数字信封的包装流程如图 3 所示,假定双方都拥有对方的加密证书,数字信封包装的主要步骤如下:

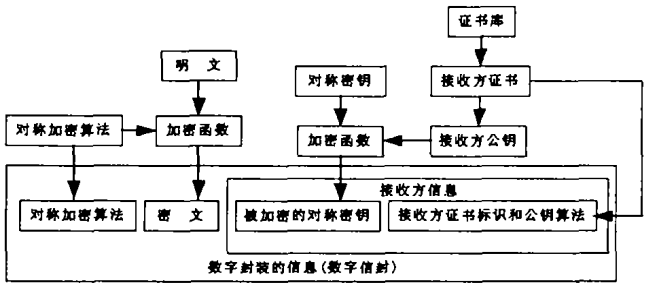



**图 3 数字信封的包装**

1) 取得需要加密的数据;

2) 产生随机对称(会话)密钥;

3) 利用对称密钥和选定的对称加密算法对需要加密的数据进行加密;

4) 打开本地证书库,获取接收方的证书及其对应的公钥;

5) 从接收方证书属性中判断所使用的公钥算法;

6) 利用接收方的公钥和公钥算法加密对称密钥;

7) 获取接收方证书 ID,并将有关信息打包.

这样,在一个数字信封中包含了以下信息:数据加密算法(对称加密算法)、被加密的数据(密文)、被加密的对称密钥、接收方 ID 和公钥算法等.

#### 3.2.2 数字信封的拆解

数字信封的拆解实际上是上述封装过程的一个逆过程,如图 4 所示.

主要步骤如下:

1) 接收数字信封,取得数字封装的数据;

2) 接收方打开本地证书库,获取与证书公钥相对

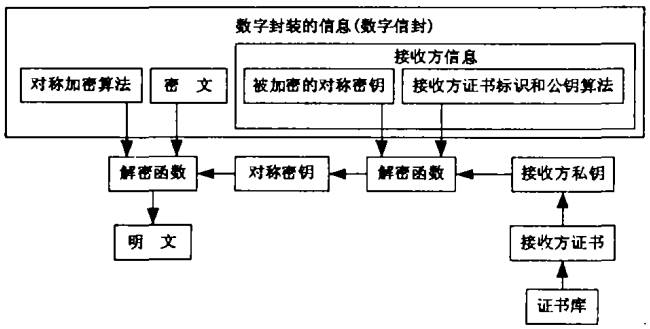



图 4　数字信封的拆解

应的私钥;

3) 接收方利用私钥和公钥算法解密被加密的对称密钥;

4) 利用对称密钥和对称密码算法解密被加密的数据,得到数据明文.

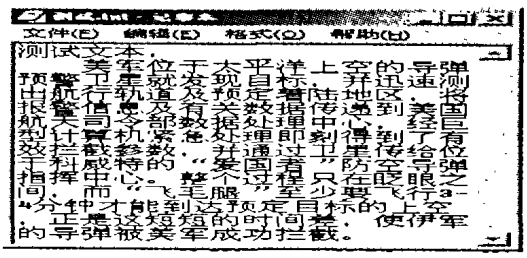
数字信封技术保证只有规定的接收者才能阅读信息的内容,并且,用户每次加密信息时都使用不同的随机会话密钥,密码破译的可能性很小,即使某次会话密钥被破译了,也只会泄露该次会话的信息,不会影响到其他密文的传递. 因此,数字信封技术保证了网络信息的保密性和真实性.

## 4　程序实现及实验结果

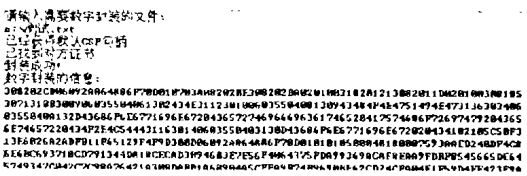
在利用数字证书实现数字信封的包装与拆解的过程中,主要用到的 CryptoAPI 函数有: CryptAcquireContext 函数(获得 CSP 的句柄)、CertOpenStore 函数(取得本地证书库句柄)、CertFindCertificateInStore 函数(在本地证书库中查找接收方的证书)、CryptEncryptMessage 函数(数字信封的包装)和 CryptDecryptMessage 函数(数字信封的拆解)等,其关键代码如下:

```
//获得默认 CSP 句柄
if ( CryptAcquireContext ( &hCryptProv, NULL, NULL, PROV_RSA_FULL,0) )
        ……
//打开证书库
if( ! ( hStoreHandle = CertOpenStore ( CERT_STORE_PROV_SYSTEM, 0, NULL, CERT_SYSTEM_STORE_CURRENT_USER,CERT_STORE_NAME) ) )
        ……
//获取对方证书的指针
if ( pRecipientCert = CertFindCertificateInStore ( hStoreHandle,MY_ENCODING_TYPE,0,CERT_FIND_SUBJECT_STR,ENCRYPT_NAME,NULL) )
        ……
//定义加密算法变量,加密消息参数变量 CRYPT_ALGORITHM_IDENTIFIER  EncAlgm;
CRYPT_ENCRYPT_MESSAGE_PARA  EncPrms;
//设对称算法为 RC4,公钥算法为 RSA
EncAlgm. pszObjId = szOID_RSA_RC4;
//初始化 CRYPT_ENCRYPT_MESSAGE_PARA 结构
EncPrms. dwMsgEncodingType = MY _ ENCODING _ TYPE;
EncPrms. hCryptProv = hCryptProv;
EncPrms. ContentEncryptionAlgorithm = EncAlgm;
……
//调用 CryptEncryptMessage 函数实现数字信封的包装
if( CryptEncryptMessage ( &EncPrms, 1, RecipientCertArray, pbContent, cbContent, pbEncryptedBlob, &cbEncryptedBlob) )
        ……
//调用 CryptDecryptMessage 函数实现数字信封的拆解
        ……
//释放证书指针
CertFreeCertificateContext( pRecipientCert) ;
//关闭证书库
CertCloseStore ( hStoreHandle, CERT_CLOSE_STORE_CHECK_FLAG)
//释放 CSP 句柄
CryptReleaseContext( hCryptProv,0) ;
        ……
```

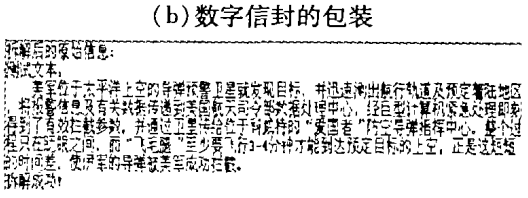
为了实际验证数字信封实现效果,笔者利用 Win2K 公钥体系下 CA 颁发的数字证书,分别对文本数据进行数字信封的包装与拆解,实验结果如图 5 所示.




(a)原始数据



(b)数字信封的包装




(c)数字信封的拆解

图 5　文本的数字信封包装与拆解

通过对不同大小的文本数据进行多次实验,可以发现该数字信封技术加解密效率高、速度快.在相同环境下,对同一文本数据进行加解密处理,该数字信封技术采用 RC4 对称加密算法所用的加解密处理时间大约为 RSA 公钥加密算法的 1/400 ~ 1/500.

## 5 结束语

数字信封技术不但具有加解密数据效率高、速度快的特点,而且通过和数字证书结合使用,能够保证网络中数据的保密性和真实性.因此,数字信封技术在网络信息安全倍受关注的今天必然会有广泛的应用前景.

**参考文献:**

[1] 孔斌. Microsoft CryptoAPI 应用概述[J]. 计算机安全, 2002, 17(7): 26 - 28.

[2] 姚世军. 加密服务程序 CSP 的建立方法[J]. 计算机系统应用,2003,18(5): 46 - 47.

[3] 冉春玉,汪学舜,吕恢艳. 加密服务提供(CSP)的实现与开发[J]. 武汉理工大学报,2003,25(10):87 - 89.

[4] 李明柱. VC + + 最新编程实例与技巧[M]. 北京:北京航空航天大学出版社,2001.

[5] 杨雪涛. 基于 PKI 的安全电子邮件系统的设计与实现[D]. 四川: 四川大学计算机系,2003. 19 - 20.

[6] 马军, 周艳梅. 基于 Microsoft 密码体系的信息安全的实现[J]. 计算机系统应用, 2002,10(2):34 - 36.

# Realization of Digital Envelope Based on Microsoft Cryptographic Architecture

*ZHOU Cheng, GUO Zheng-rong*

(Graduate School of Chongqing Communication Institute, Chongqing 400035, China)

**Abstract**: Digital Envelope utilizes the advantage of Symmetric and Asymmetric encryption algorithm and it is a safety and efficient encryption technique. The cryptographic architecture of Microsoft OS, the use and management of Microsoft certificate are introduced. Then, the principle, step and the algorithm of how to realize digital Envelope with the digital certificate and CryptoAPI functions is described. The experiments of many encrypting text data with the certificate of Win2K are done. These experiments prove that the Digital Envelope technique can ensure the data transmissions's confidentiality and authenticity, and it's high encryption speed can meet the requirement of actually application.

**Key words**: CryptoAPI; CSP; symmetric/asymmetric encryption algorithm; digital certificate; digital envelope

(编辑 张 苹)