第4章

密码技术

密码学的起源可以追溯到人类出现的时候。在人类开始研究如何通信的时候，就已经意识到保密的重要性，最先有意识地使用一些技术手段来加密信息的可能是公元前的古希腊人。后来罗马的军队用凯撒密码进行通信。在随后的19世纪，有一些更为高明的加密技术出现，但是这些技术的安全性通常依赖于用户对它们的信任程度。19世纪荷兰密码学家Kerchoffs提出了密码学的一个基本原则：密码系统的安全性应该完全依赖于密钥的安全性。

进入20世纪70年代，随着信息化进程的加快，信息安全和密码学越来越受到人们的重视，此时，现代密码学已经初具模型。现代密码学的形成有两个标志性事件：一是美国国家标准局公开征集数据加密标准，并于1977年确定DES为数据加密标准；二是1976年Diffie和Hellman于1976年发表了“New direction in cryprography”一文，提出了公钥密码学的概念。公钥密码学在信息安全中担负了密钥协商、数字签名、消息认证等重要任务。

4.1 对称密钥加密体制

4.1.1 简 介

对称密钥加密体制，又称私钥加密，即信息的发送方和接收方用一个密钥去加密和解密数据。它的最大优势是加/解密速度快，适合于对大数据量进行加密，但密钥管理困难。

使用对称加密技术将简化加密的处理，每个参与方都不必彼此研究和交换专用设备的加密算法，而是采用相同的加密算法并只交换共享的专用密钥。如果进行通信的双方能够确保专用密钥在密钥交换阶段未曾泄露，那么机密性和报文完整性就可以通过使用对称加密方法对机密信息进行加密以及通过随报文一起发送报文摘要或报文散列值来实现。

对称的加密体制由一个映射

$$E: M \times K \rightarrow C$$

构成，对任意的 $k \in K$，映射

$$E_k: M \rightarrow C, c \mid \rightarrow E(k, m)$$

是可逆的。这里 m 表示消息，M 表示消息的集合，c 为密文，C 为密文集合，k 为密钥，K 为密钥集合。

目前常用的对称加密体制包括数据加密标准(DES)和高级的数据加密标准(AES)。这里我们将以 DES 为例介绍对称的加密体制。

4.1.2 数据加密标准

为了建立适用于计算机系统的商用密码,美国商业部的国家标准局 NBS 于 1973 年 5 月和 1974 年 8 月两次发布通告,向社会征求密码算法。在征得的算法中,由 IBM 公司提出的算法 lucifer 中选。1975 年 3 月,NBS 向社会公布了此算法,以求得公众的评论。于 1976 年 11 月被美国政府采用,DES 随后被美国国家标准局和美国国家标准协会(American National Standard Institute,ANSI) 承认。1977 年 1 月以数据加密标准 DES (Data Encryption Standard)的名称正式向社会公布,它是目前使用最广泛的对称密钥加密算法,广泛应用于政府、银行及商业机构。

DES 是一种分组乘积密码,包括 16 轮迭代。明密文分组长度为 64 位,密钥总长为 64 位,有效长度 56 位,其中第 8、16、…、64 位共 8 位是奇偶校验位。DES 是一种对和运算,除子密钥使用顺序逆序外,加密和解密算法相同。DES 是一种面向二进制的密码算法,能够加解密任何形式的计算机数据。

DES 的加密算法流程如图 4-1 所示,包括三大步骤。

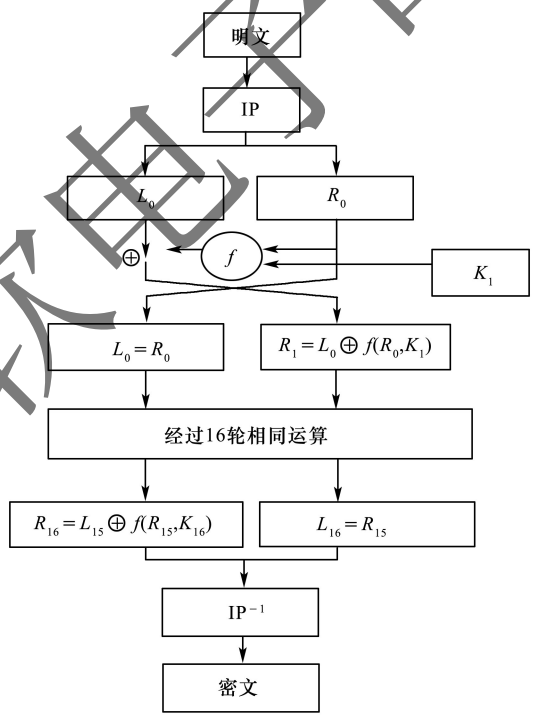

图 4-1 DES 加密过程

(1)初始置换。将输入的 64 位的明文进行初始置换 IP。然后,将变换后的数据平分成各 32 位的左右两部分,左部分记为 L_0 ,右部分记为 R_0 。

(2)16 轮的轮变换。对 R_0 实行在轮子密钥 K_1(轮子密钥由密钥扩展算法产生)控制下的变换 f,结果记为 $f(R_0,K_1)$,再与 L_0 做按位异或运算,其结果记为 R_1,R_0 则直接作为下一轮的 L_1,如此循环 16 轮,得到预输出结果 R_{16}、L_{16}。

$$\begin{cases} L_n = R_{n-1} \\ R_n = L_{n-1} \oplus f(R_{n-1},K_n) \end{cases} \quad n = 1,2,\cdots,16$$

(3)逆初始置换。对 R_{16}、L_{16} 组合后的 64 位预输出结果实行逆初始置换 IP^{-1},得到 64 位密文。

解密算法与加密算法基本相同,不同之处仅在于轮子密钥的使用顺序逆序,即解密的第 1 轮子密钥为加密的第 16 轮子密钥,解密的第 2 轮子密钥为加密的第 15 轮子密钥,……,解密的第 16 轮子密钥为加密的第 1 轮子密钥。

随着攻击技术的发展,DES 本身又有发展,如衍生出可抗差分分析攻击的变形 DES 以及密钥长度为 128 比特的三重 DES 等。2000 年 1 月 19 日,由电子边疆基金会组织研制的 25 万美元的 DES 解密机以 22.5 小时的战绩,成功地破解了 DES 加密算法。DES 已逐渐完成了它的历史使命。

2000 年 10 月,美国国家标准和技术协会宣布通过从 16 种候选算法中选出的一项新的对称加密标准——高级加密标准(Advanced Encryption Standard),由比利时研究人员 Daemen 和 Rijimen 提交的 Rijindael 算法被接受成为新的标准。AES 正日益成为加密各种形式的电子数据的实际标准。AES 算法基于排列和置换运算。排列是对数据重新进行安排,置换是将一个数据单元替换为另一个。AES 使用几种不同的方法来执行排列和置换运算。AES 是一个迭代的、对称密钥分组的密码,它可以使用 128、192 和 256 位密钥,并且用 128 位(16 字节)分组加密和解密数据。

4.2　非对称密钥加密体制

4.2.1　简　介

1976 年,美国学者 Diffie 和 Hellman 为解决密钥的分发与管理问题发表了著名论文《New Direction in Cryptography》,提出一种密钥交换协议,允许在不安全的媒体上通过通讯双方交换信息,安全地传送秘密密钥,并提出了建立“公开密钥密码体制”(Public Key)的新概念。

这篇文章中提出的公钥密码的思想:若每一个用户 A 有一个加密密钥 pk,不同于解秘密钥 sk,加密密钥 pk 公开,sk 保密,当然要求 pk 的公开不至于影响 sk 的安全。若 B 要向 A 保密送去明文 m,可查 A 的公开密钥 pk,若用 pk 加密得密文 c,A 收到 c 后,用只有 A 自己才掌握的解密密钥 sk 对 c 进行解密得到 m。当时他们还没有实现这种体制的具体算法。公开密钥密码基于单向陷门函数。一般地,加密密钥也称为公开密钥,解密密钥又称为秘密钥(Secret Key)。

所谓单向函数，就是指计算原函数值很容易，但是计算其反函数很困难，甚至于不可能。而单向陷门函数是有一个陷门的一类特殊单向函数，如果知道那个秘密陷门，则也能很容易计算其反函数的值。即已知 x，易于计算 $f(x)$，而已知 $f(x)$，却难于计算 x。然而，一旦给出 $f(x)$ 和一些秘密信息 y，就很容易计算 x。在公开密钥密码中，计算 $f(x)$ 相当于加密，陷门 y 相当于私有密钥，而利用陷门 y 求 $f(x)$ 中的 x 则相当于解密。

4.2.2 RSA

1977 年，Rivest，Shamir 和 Adlerman 提出了第一个公钥加密机制 RSA，它是基于整数的素数因子分解这个困难问题。

简单地讲，整数 n 的欧拉函数是指小于 n 且与 n 互素的数的个数，记做 φcos。我们说整数 n 与 m 互素，就是指 n 与 m 的最大公因子为 1，记做 $(n,m)=1$。

欧拉(Euler)定理：若 $(a,m)=1$，则 $a^{\varphi(m)}=1 \bmod m$。

欧拉定理是 RSA 能正确解密的关键。

RSA 由密钥生成算法、加密算法和解密算法构成。

1. 密钥生成算法

(1)选择两个大素数 p,q；

(2)计算 $n=p\times q,\varphi(n)=(p-1)(q-1)$，这里 $\varphi(n)$ 是欧拉函数；

(3)随机选择 $1<e<\varphi(n)$，且 $(e,\varphi(n))=1$；

(4)计算 d，且 $ed=1 \bmod \varphi(n)$。

公钥为 (e,n)，私钥为 (p,q,d)。

2. 加密算法

对于消息 m，其密文 $c=m^e \bmod n$。

3. 解密算法

对于密文 c，其明文 $m=c^d \bmod n$。

这是由于 $ed=1 \bmod \varphi(n)$，存在 $t\geqslant 1$ 使 $ed=t\varphi(n)+1$，对于明文 $m\in \mathbf{Z}_n^*$，有 $(m^e)^d=m^{t\varphi(n)+1}(\bmod n)=(m^{\varphi(n)})^t m(\bmod n)=1^t m \bmod n=m \bmod n$。

【例 4-1】 $p=3,q=11$，确定公钥和私钥。

解：密钥生成

(1)$p=3,q=11$；

(2)$n=33,\varphi(n)=20$；

(3)$e=7,(7,20)=1$；

(4)$ed=7d=\bmod \varphi(n),d=3$。

公钥(7,33)，私钥(3,33)。

加密：

给定 $m=2$，

$c=m^e \bmod n=2^7 \bmod 33=29$。

解密：

$m = c^d \bmod n = 29^3 \bmod 33 = 24389 \bmod 33 = 2$。

4.3 数字签名

4.3.1 简 介

数字签名(Digital Signature)，就是只有信息的发送者才能产生的别人无法伪造的一段数字串，这段数字串同时也是对信息的发送者发送信息真实性的一个有效证明。简单地说，所谓数字签名就是附加在消息上的一些数据，或是对消息所作的密码变换。这种数据或变换允许消息的接收者用以确认消息的来源和完整性，防止被人(例如接收者)进行伪造。它是对电子形式的消息进行签名的一种方法。基于公钥密码体制和私钥密码体制都可以获得数字签名，目前主要是基于公钥密码体制的数字签名。

数字签名包括普通数字签名和特殊数字签名。常见的普通数字签名算法有 RSA、ElGamal、Fiat-Shamir、Guillou-Quisquarter、Schnorr、Ong-Schnorr-Shamir 数字签名算法、Des/DSA 等。特殊数字签名有盲签名、代理签名、群签名、不可否认签名、公平盲签名、门限签名、具有消息恢复功能的签名等，它与具体应用环境密切相关。显然，数字签名的应用涉及到法律问题，美国联邦政府的基于有限域上的离散对数问题为基础制定了自己的数字签名标准(DSS)。

数字签名技术是不对称加密算法的典型应用。数字签名的应用过程是，数据源发送方使用自己的私钥对数据校验或对其他与数据内容有关的变量进行加密处理，完成对数据的合法“签名”，数据接收方则利用对方的公钥来解读收到的“数字签名”，并将解读结果用于对数据完整性的检验，以确认签名的合法性。数字签名技术是在网络系统虚拟环境中确认身份的重要技术，完全可以代替现实过程中的“亲笔签字”，在技术和法律上有保证。在数字签名应用中，发送者的公钥可以很方便地得到，但他的私钥则需要严格保密。

4.3.2 数字签名的功能

数字签名的功能包括：

(1)消息的完整性：即消息在传递过程中不能被其他人所窜改。

(2)不可抵赖性：签名方一旦对消息签名后，其他人就可以很方便的用签名方的公钥验证签名。

数字签名技术是将摘要信息用发送者的私钥加密，与原文一起传送给接收者。接收者只有用发送者的公钥才能解密被加密的摘要信息，然后用哈希(Hash)函数对收到的原文产生一个摘要信息，与解密的摘要信息对比。如果相同，则说明收到的信息是完整的，在传输过程中没有被修改，否则说明信息被修改过，因此数字签名能够验证信息的完整性。

归结起来，数字签名的产生过程就是用公钥加密机制中的私钥进行加密，而数字签名验证是就是用公钥进行解密的过程。根据数字签名的这个性质，我们可以看出，签名的产

生只能有一个人完成，即私钥的拥有者，而签名的验证可以由任何一个人完成。公钥密码学自诞生以来，数字签名一直是公钥密码学研究的重点，出现了许多新的有影响力的成果。

4.3.3 签名的生成与验证

1. 签名过程

发送方用一个哈希函数计算要发送的消息摘要，然后用自己的私人密钥对这个摘要进行加密，这个加密后的摘要将作为数字签名和消息一起发送给接收方。

2. 签名的验证

接收方收到签名和消息后，首先用与发送方一样的哈希函数从接收到的原始消息计算出消息摘要，接着再用发送方的公用密钥来对报文附加的数字签名进行解密，如果这两个摘要相同、那么接收方就能确认该数字签名是发送方的。

4.4 身份认证技术

4.4.1 简 介

网络世界中一切信息包括用户的身份信息都是用一组特定的数据来表示的，计算机只能识别用户的数字身份，所有对用户的授权也是针对用户数字身份的授权。

身份认证技术就是解决如何保证以数字身份进行操作的操作者就是这个数字身份合法拥有者，也就是说保证操作者的物理身份与数字身份相对应，作为防护网络资产的第一道关口，身份认证在信息安全中起着举足轻重的作用。

认证与加密不同，认证的目的是要检验对方身份的真实性，即对方确实是自己所要通信的对象，而不是其他的假冒者。

4.4.2 常见的身份认证因素

目前，对用户身份的认证基本上可以分为这三种：

(1)根据你所知道的信息来证明你的身份，如口令（what you know，你知道什么）；

(2)根据你所拥有的东西来证明你的身份，如智能卡、令牌等（what you have，你有什么）；

(3)直接根据独一无二的身体特征来证明你的身份（who you are，你是谁），包括人体的生理和行为特征两类。人的生理特征如指纹、视网膜、虹膜、脸型等，人的行为特征如声音、步态等。

有时为了达到更高的身份认证安全性，某些场景会从上面 3 种因素中挑选 2 种甚至 3 种混合使用，即形成所谓的双因素认证和多因素认证。

4.4.3 RFID 电子标签的身份机制

电子标签一般分为存储型和逻辑加密型两种。存储型 RFID 电子标签的应用主要是通过快速读取 ID 号来达到识别的目的，主要应用于动物识别、跟踪等。这种应用要求是

完整性，对于存储数据的安全要求不高，一般用一个唯一序列号自动识别。逻辑加密型的 RFID 电子标签应用极其广泛，且其中还可能涉及小额交易等，因此其安全性要求很高。逻辑加密型的 RFID 电子表签内部存储区一般按块分区，且有密钥控制位控制块的安全。下面我们就以介绍一种在逻辑加密型 RFID 标签中常见的身份认证协议。

(1)应用程序通过 RFID 读写器向 RFID 标签发出认证请求；

(2)RFID 标签收到请求后，向读写器发出一个一次性的随机数 B；

(3)读写器收到 B 后，生成一个随机数 A，然后将 A 和 B 加密后发给 RFID 电子标签；

(4)RFID 电子标签收到后，用存储在标签内部的密钥解密得到 A 和 B。然后比较两次的 B 是否相同。如果相同，转(5)；否则，终止协议。

(5)RFID 电子标签再用刚才的密钥加密 A，并发给读写器。

(6)读写器收到后解密得到 A，比较两次的 A 是否相同。如果相同，协议成功；否则，终止协议。

实训 1　RSA 加密实训

RSA 是由 Ronald Rivest、Adi Shamir 和 Leonard Adleman 在 1977 年开发的公开密钥算法，图 4-2 所示为 RSA-Tool 的主界面。

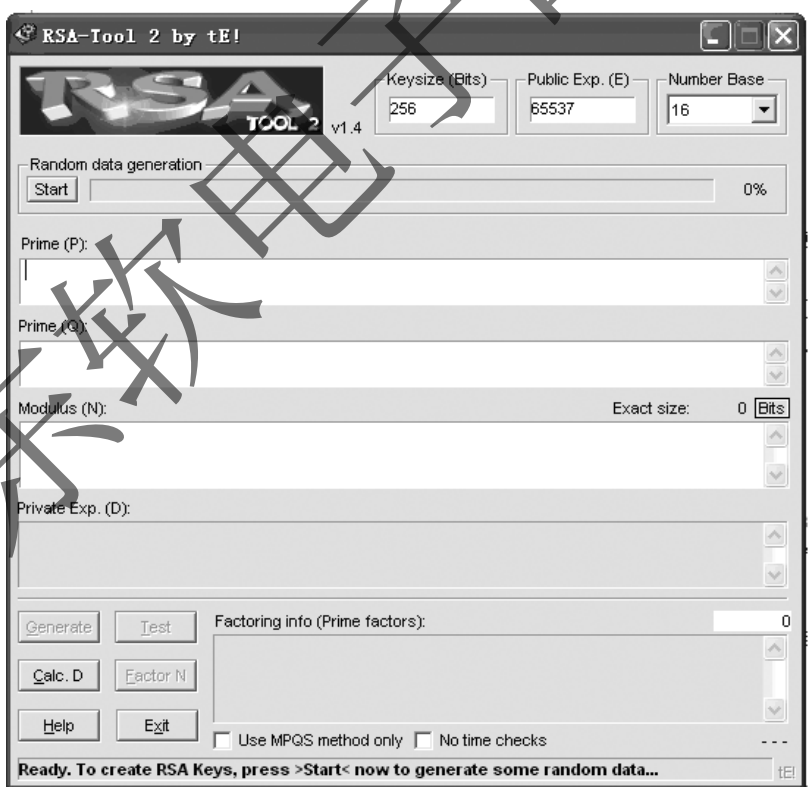

图 4-2　RSA-Tool 2 主界面

1. 实训目的

(1)了解 RSA-Tool 的基本功能及用法;

(2)掌握 RSA 算法的密钥生成、加密及解密的方法。

2. 实训步骤

(1)按下“Start”按钮,通过移动鼠标指针得到密钥生成所需要的随机数,如图4-3所示。

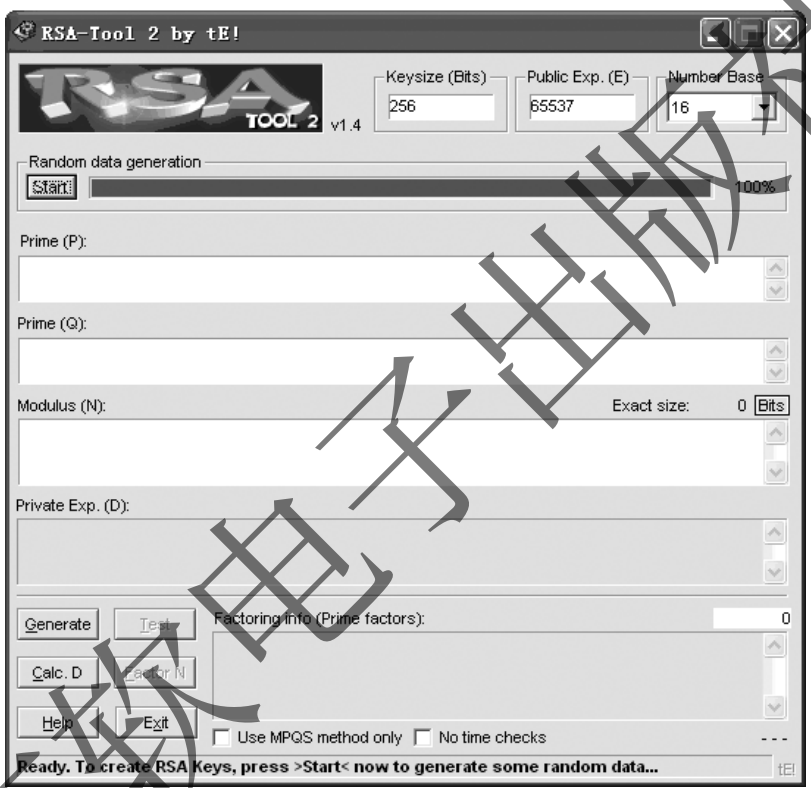

图 4-3 生成随机数

(2)在 Keysize 中输入要生成的密钥的长度。最大为 4096 位。在 Number Base 中选择显示的数据的进制:十进制、十六进制等,如图 4-4 所示。

(3)在 Public Exp 中输入公钥(E)。常用的 E 有(考虑到计算速度的原因):3,17,257 和 65537(十进制)。

(4)按下“Generate”按钮生成加密密钥,等到密钥生成完成,程序输出的 D 就是密钥。

(5)按下 Test 按钮进入加密与解密窗口,如图 4-5 所示。

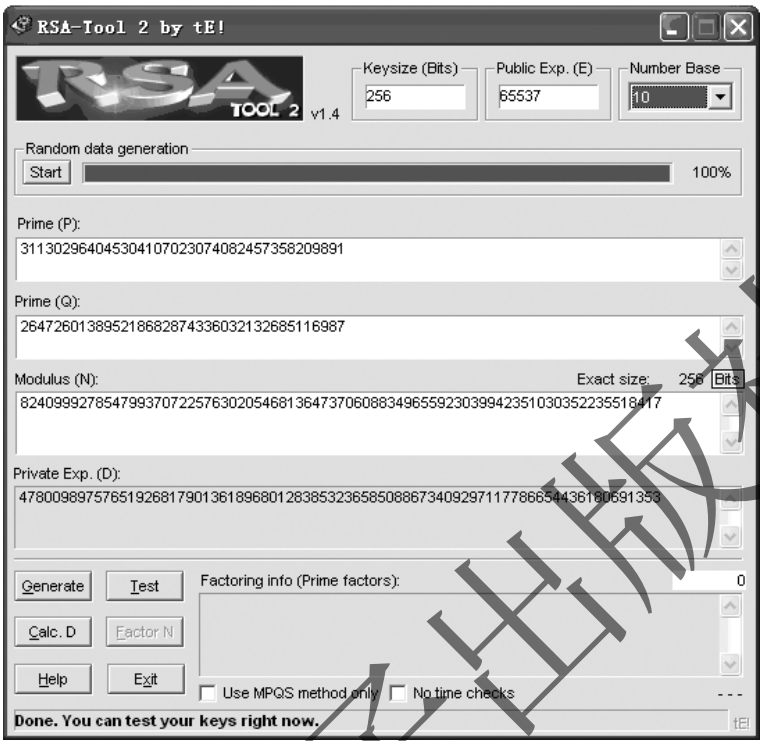

图 4-4　密钥的生成

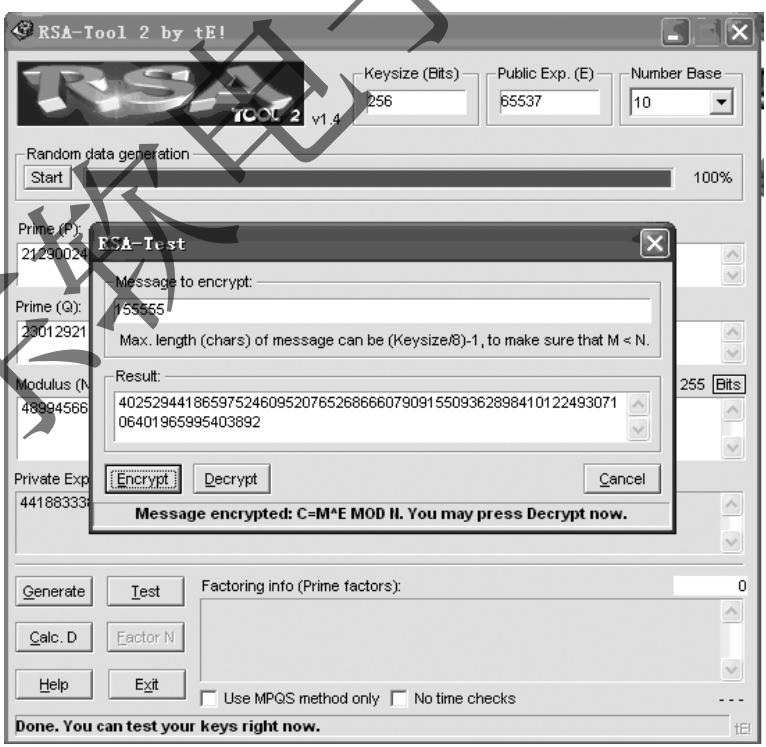

图 4-5　加密与解密

实训 2　PGP 软件及应用

1. 简介

RSA 公钥体系的特点使它非常适合用来满足两个要求：保密性(Privacy)和认证性(Authentication)。PGP(Pretty Good Privacy)，是一个基于 RSA 公钥加密体系的邮件加密软件，它提供了非对称加密和数字签名。其创始人是美国的 Phil Zimmermann，他把 RSA 公钥体系的方便和传统加密体系的高速结合起来，并且在数字签名和密钥认证管理机制上有巧妙的设计，因此 PGP 成为目前非常流行的公钥加密软件包。PGP 有以下主要功能：

(1)邮件加密，以防止非法阅读；

(2)给邮件加上数字签名，从而使收信人收到信后，对发信人的身份进行验证和确保邮件的内容不被窜改，也可防止声明人抵赖，这一点在商业领域有很大的应用前景；

(3)能够加密文件，包括图形文件、声音文件以及其他各类文件。

2. 实训目的

(1)掌握 PGP 软件的安装方法；

(2)掌握公钥与私钥生成与备份方法；

(3)掌握 PGPKeys 管理密钥的方法；

(4)掌握使用 Outlook 发送加密邮件；

(5)掌握使用 PGP 加密信息；

(6)掌握 PGPDisk 的使用。

3. 实训环境

(1)安装 Windows 2000 Server 的局域网环境；

(2)PGP 8.1 软件；

(3)计算机接入 Internet。

4. 实训步骤

(1)安装 PGP 软件、软件注册：双击 PGP 安装文件进行安装。完成后必须重启计算机。PGP 软件将出现注册窗口，此时输入提供的用户名、组织名、序列号及授权信息等内容后，点击“认证”即可完成安装。安装时选择新用户，并注意输入通行码。安装过程如图 4-6～图 4-10 所示。

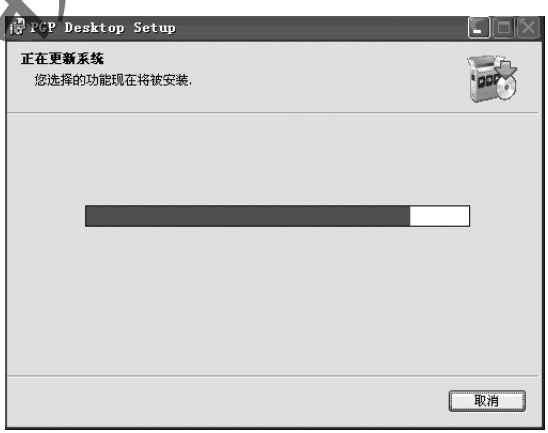

图 4-6　安装界面

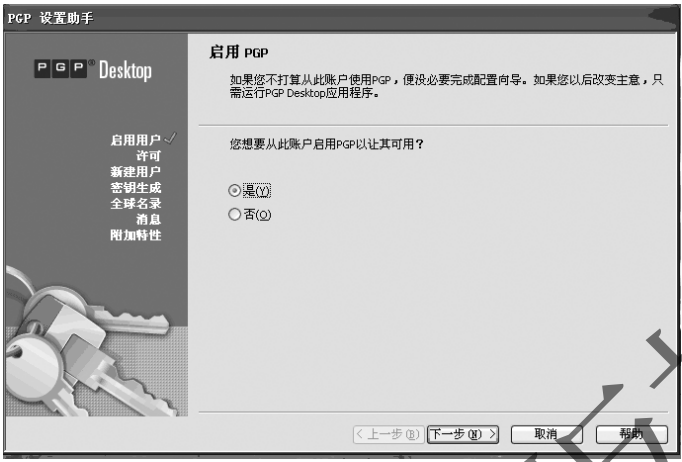

图 4-7　PGP 设置助手

图 4-8　PGP 设置助手之许可

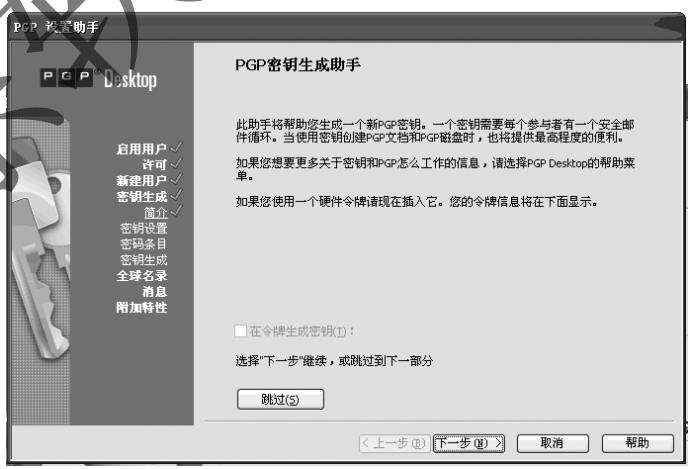

图 4-9　PGP 设置助手之密钥生成助手

图 4-10 PGP 设置助手之创建密码

(2)公钥与私钥的生成与管理:进入 PGP 密钥,可以看到注册的邮箱已有对应密钥管理内容,如图 4-11 所示。此时我们可导出自己的公钥,生成 ASC 文件。方法:右击“邮箱”,选择“Export”,输入文件名即可,此文件可交流、发布等。

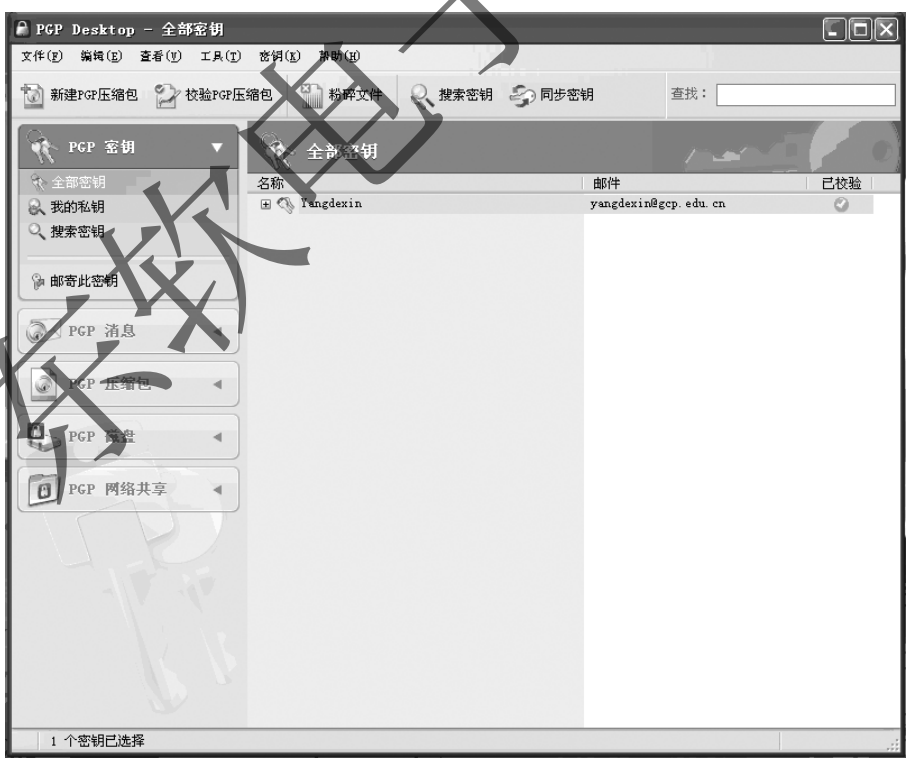

图 4-11 PGP 设置密钥管理

(3)加密信息:打开记事本程序,输入内容 1234abcd。右击 PGP 图标,选择 Current Window→Encrypt,进行记事本内容加密,完成后观察结果。

(4)解密信息:同样将光标保持在记事本中,右击 PGP 图标后,选择 Current Window →Decrypt 即可解密信息,当然需要输入通行码,解密结果显示在“Text Viewer”中。

(5)PGPDisk 的使用:右击 PGP 图标,选择 PGPDisk→NewDisk,根据提示选择 PGPDisk 加密盘的大小(只与硬盘容量有关,如 100MB)。加密时可选择使用私钥文件或通行码,完成后即可在资源管理器中使用该盘。使用通行码加密的 PGPDisk 盘可用于所有安装 PGP 软件的计算机中。

(6)PGPDisk 的启用与关闭:在启用状态下,PGP 图标会处于开锁状态。若要关闭 PGPDisk,则选择“Unmount”,注意编辑位置不要处于 PGPDisk 中。

(7)熟悉 PGPMail 的功能:文件粉碎、空间填充等。

(8)熟悉 PGP 的选项设置:Options。

(9)公钥的发布与利用 Outlook 发送加密电子邮件过程如图 4-12～图 4-16 所示。

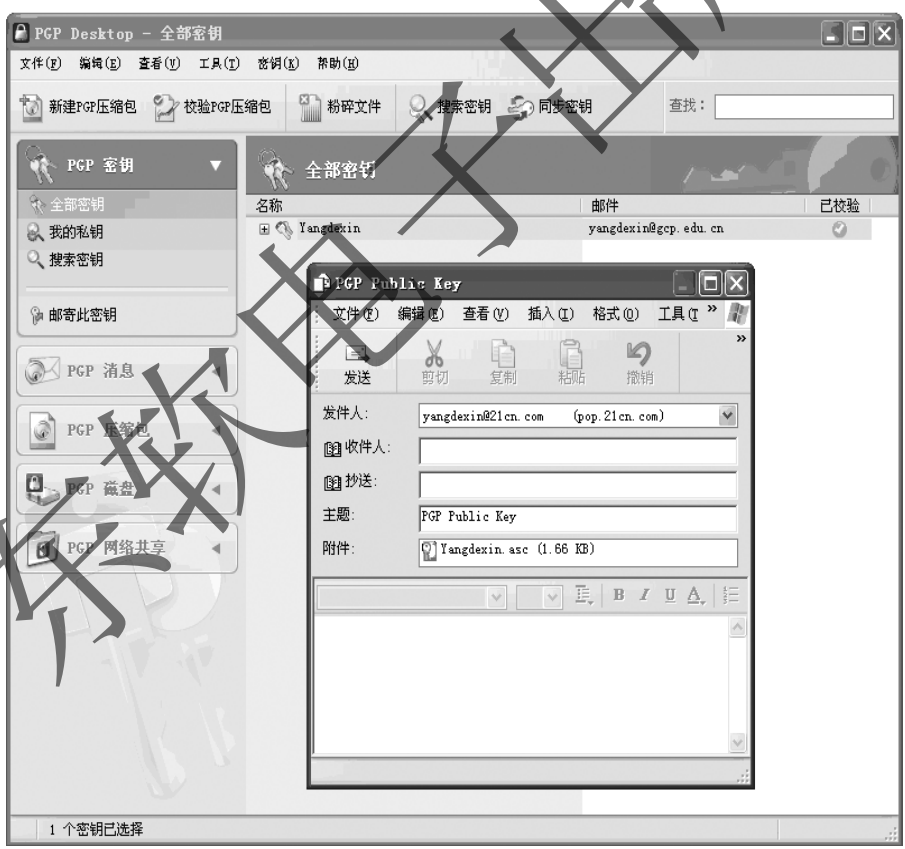

图 4-12　邮寄我的公钥

图 4-13 主要功能

图 4-14 原始邮件

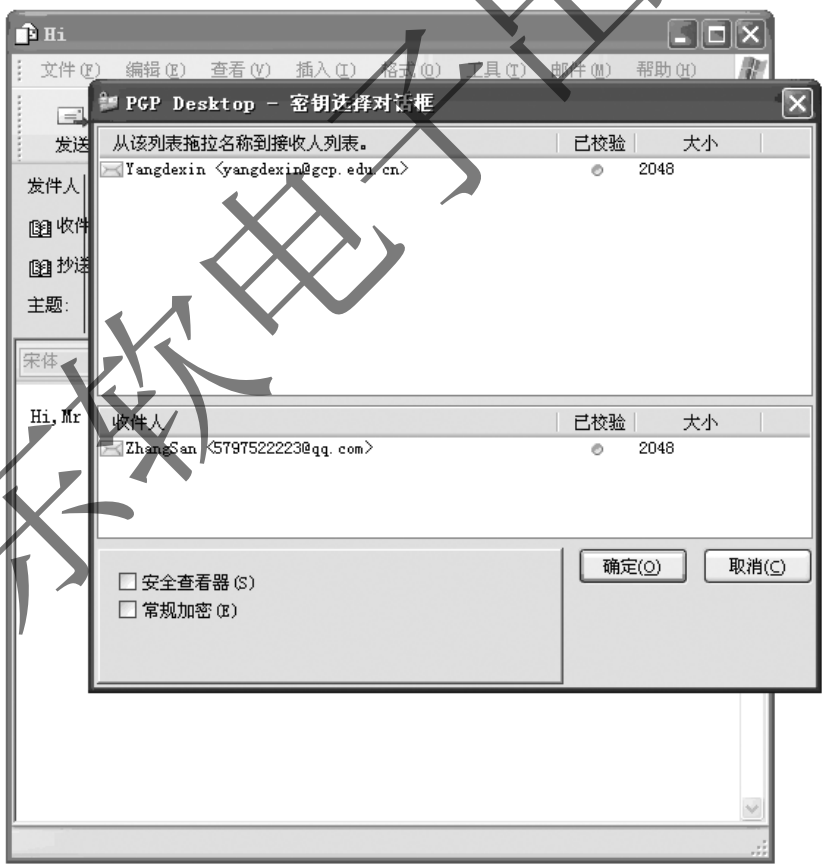

图 4-15 选择收件人

图 4-16　加密后的邮件

进入 Outlook，若你的邮箱地址不是 Outlook 默认的邮箱或无邮箱，则应进入工具→账户，进行添加。

撰写邮件，选择 PGP 加密并发送即可。

(10)签名邮件如图 4-17 所示，前面为原始邮件地址，后面为数字签名。签名后的邮件如图 4-18 所示。

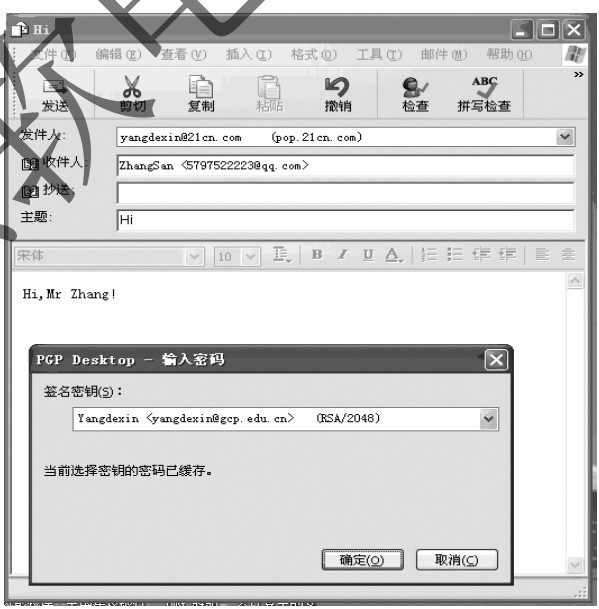

图 4-17　选择发件人

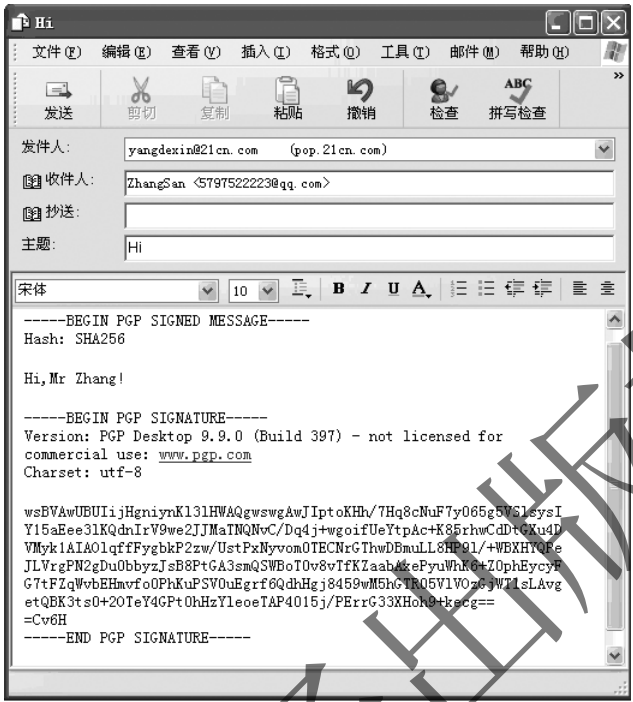

图 4-18 签名后的邮件

(11)加密后签名邮件,对邮件先加密然后再对密文签名,如图 4-19 所示。

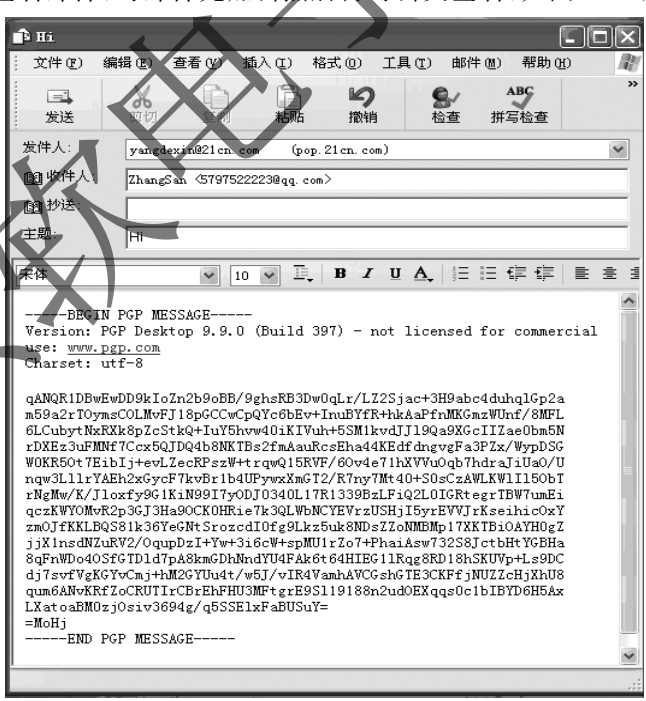

图 4-19 加密签名后的邮件

本章小结

本章简要介绍了与信息安全相关的密码学技术，包括加密（对称与非对称加密），数字签名、身份认证等技术，以及在物联网中可能用到的一些密码学算法等。

练习题

1. 简述常用的对称加密算法及其特点。
2. 什么是对称加密和非对称加密？二者有何差异？
3. 举例说明常见的非对称加密算法。
4. 什么是数字签名？简述其用途。
5. RSA 算法中取 p＝3，q＝11，请计算出公开钥和秘密钥；并计算出消息 m＝2 时的密文。
6. 什么是身份验证？请举例说明身份验证技术的用途。
7. 请给出常用的两种数字签名方案。
8. 简述身份认证机制的作用。