第3章

信息加密技术

CHAPTER 3

加密学是一门古老而深奥的学科，是研究密码与密码活动的本质和规律，以及指导密码实践的科学，其历史可以追溯到几千年前，长期被军事、外交等部门用来传递重要信息。计算机信息加密技术是研究计算机信息加密、解密及其变换的学科，主要探索密码编码和密码分析的一般规律，是一门结合数学、计算机科学、信息通信系统等多门学科为一体的综合性学科。它不仅具有信息通信加密和解密功能，还具备身份认证、消息认证、数字签名等功能。它已经成为信息安全主要的研究方向以及网络空间安全的核心技术，也是网络安全教学中的主要内容。

学习目标

- 熟悉加密技术的基本概念，包括明文、密文、加密变换、解密变换以及密钥。
- 掌握对称加密算法的原理、典型的算法 DES 与 3DES，以及对称加密算法的优缺点。
- 掌握非对称加密算法的原理、典型的算法 RSA，以及非对称加密算法的优缺点。
- 掌握数据完整性原理，以及典型散列算法 MD5 与 SHA1，以及散列算法的特点。
- 掌握如何使用 PGP 软件，包括密钥管理、发送加密与解密邮件。

3.1 加密技术概述

在计算机网络中,为了保护数据在传输或存放的过程中不被别人窃听、篡改或删除,必须对数据进行加密。随着网络应用技术的发展,加密技术已经成为网络安全的核心技术,而且融合到大部分安全产品之中。加密技术是对信息进行主动保护,是信息传输安全的基础,通过数据加密、消息摘要、数字签名及密钥交换等技术,可以实现数据保密性、数据完整性、不可否认性和用户身份真实性等安全机制,从而保证了在网络环境中信息传输和交换的安全。

密码学(Cryptology)是一门具有悠久历史的学科。密码技术是研究数据加密、解密及加密变换的科学,涉及数学、计算机科学及电子与通信等学科。加密是研究、编写密码系统,把数据和信息转换为不可识别的密文的过程,而解密就是研究密码系统的加密途径,恢复数据和信息本来面目的过程。

网络通信的双方称为发送者与接收者。发送者发送消息给接收者时,希望所发送的消息能安全到达接收者手里,并且确信窃听者不能阅读发送的消息。这里的消息(Message)被称为明文(Plain Text),用某种方法伪装消息以隐藏它的内容过程称为加密(Encryption),加密后的消息称为密文(Cipher Text),而把密文转换为明文的过程称为解密(Decryption)。图3.1所示就是一个加密与解密的过程。

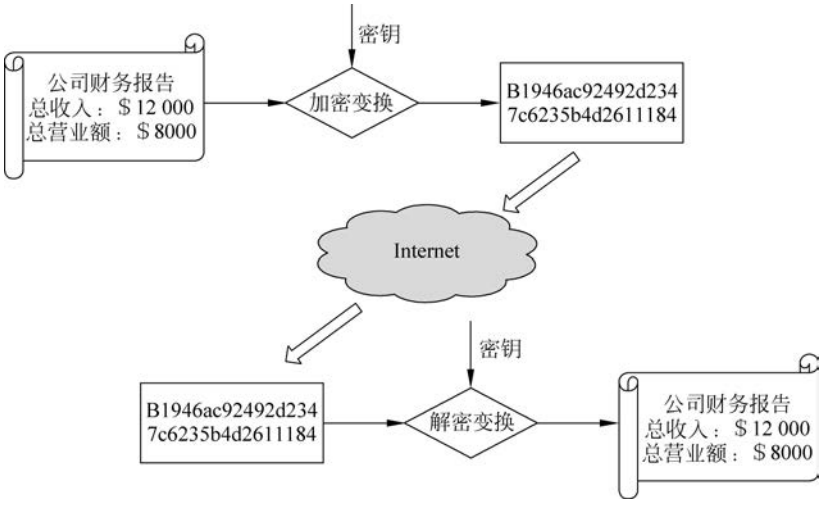

图3.1 加密与解密的过程

一个密码系统由算法和密钥两个基本组件构成。对于古典加密技术,其安全性依赖于算法,其保密性不易控制,如一个组织采用某种密码算法,一旦有人离开,这个组织的其他成员就不得不启用新的算法。另外,受限制的算法不能进行质量的控制和标准化,因为每个组织或个人都使用各自唯一的算法。而对于现代加密技术,算法是公开的,其保密性完全依赖于密钥。这个算法称为基于密钥的算法。基于密钥的算法通常分为两类:对称加密算法与非对称加密算法。

3.2　对称加密算法

3.2.1　对称加密算法原理

对称加密算法(Symmetric Algorithm)也称为传统密码算法,其加密密钥与解密密钥相同或很容易相互推算出来,因此也称为秘密密钥算法或单钥算法。这种算法要求通信双方在进行安全通信前,协商一个密钥,用该密钥对数据进行加密与解密。整个通信安全完全依赖于密钥的保密。对称加密算法的加密与解密过程可以用式子表示如下:

加密: $E_k(M)=C$

解密: $D_k(C)=M$

式中,E 表示加密运算,D 表示解密运算,M 表示明文(有的书用 P 表示),C 表示密文,K 表示密钥。

对称加密算法分为两类:一类称为序列密码算法;另一类称为分组密码算法。序列密码算法以明文中的单个位(有时是字节)为单位进行运算,分组密码算法则以明文的一组位(这样的一组位称为一个分组)为单位进行加密运算。相比之下,分组算法的适用性更强一些,适宜作为加密标准。

3.2.2　DES 算法

对称加密算法有很多种,如 DES(Data Encryption Standard)、Triple DES(3DES)、IDEA、RC2、RC4、RC5、RC6、GOST、FEAL、LOKI 等,下面以 DES 算法为例,讲述对称加密算法的实现过程。

DES 算法被称为数据加密标准,是 1972 年美国 IBM 公司研制的对称密码体制加密算法。

DES 是一种分组密码。在加密前,先对整个明文进行分组。每组长为 64 位。然后对每个 64 位二进制数据进行加密处理,产生一组 64 位密文数据。最后将各组密文串接起来,即得出整个密文。使用的密钥为 64 位,实际密钥长度为 56 位,有 8 位用于奇偶校验。其加密算法如图 3.2 所示。

首先把明文分成若干 64b 的分组,算法以一个分组作为输入,通过一个初始置换(IP)将明文分组分成左半部分(L_0)和右半部分(R_0),各为 32b。然后进行 16 轮完全相同的运算,这些运算称为函数 f,在运算过程中数据与密钥相结合。经过 16 轮运算后,左、右两部分合在一起经过一个末转换(初始转换的逆置换 IP^{-1}),输出一个 64b 的密文分组。

每一轮的运算过程为:密钥位移位,从密钥的 56 位中选出 48 位。首先,通过一个扩展置换将数据的左半部分扩展成 48 位,并通过一个异或操作与 48 位密钥结合;其次,通过 8 个 S 盒(Substitution Box)将这 48 位替代成新的 32 位;最后,再依照 P 盒置换一次。以上 3 步构成复杂函数 f。然后通过另一个异或运算,将复杂函数 f 的输出与左半部分结合成为新的右半部分。

每一轮中子密钥的生成:密钥通常表示为 64b,但每个密钥有 8 位用作奇偶校验,实际的密钥长度为 56b。在 DES 的每一轮运算中,从 56b 密钥产生出不同的 48b 的子密钥(K1,

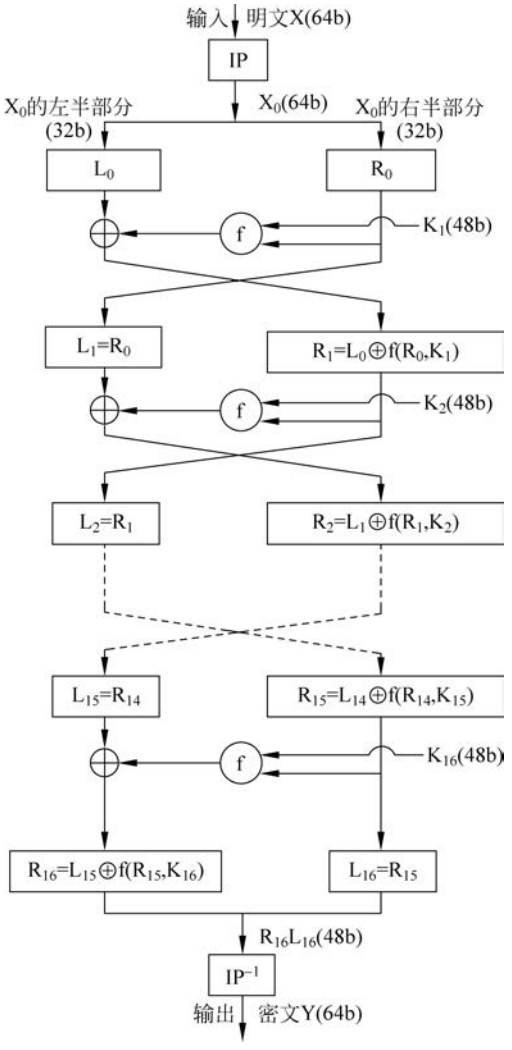

图 3.2 DES 算法流程

K2,…,K16)。首先,56b 密钥分成两部分(以 C、D 分别表示这两部分),每部分 28 位,然后每部分分别循环左移 1 位或 2 位(从第 1 轮到第 16 轮,相应左移位数分别为 1、1、2、2、2、2、2、2、1、2、2、2、2、2、2、1)。再将生成的 56b 组经过一个压缩转换(Compression Permutation),舍掉其中的某 8 位并按一定方式改变位的位置,生成一个 48b 的子密钥 Ki。

3.2.3 DES 算法强度

DES 的设计是密码学历史上的一个创新。自从 DES 问世至今,人们对它多次分析研究,从未发现其算法上的破绽。直到 1998 年,电子前沿基金会(EFF)动用一台价值 25 万美元的高速计算机,在 56 小时内利用穷尽搜索的方法破译了 56 位密钥长度的 DES。这说明 56 位的密钥和 DES 的迭代次数可能太少。

1982 年,已经有办法攻破 4 次迭代的 DES 系统。1985 年,对于 6 次迭代的 DES 系统也已破译。1990 年,以色列学者发明并运用差分分析方法证明,通过已知明文攻击,任何少

于 16 次迭代的 DES 算法都可以被比穷举法更有效的方法攻破。

尽管如此，DES 算法还是一个比较安全的算法，并且目前 DES 算法的软硬件产品在所有的加密产品中占非常大的比重，是密码学史上影响最大、应用最广的数据加密算法。

3.2.4　3DES 算法

3DES 是 DES 向 AES 过渡的加密算法（1999 年，NIST 将 3DES 指定为过渡的加密标准），是 DES 的一个更安全的变形。它以 DES 为基本模块，通过组合分组方法设计出分组加密算法，其具体实现如下：

设 $E_K()$ 和 $D_K()$ 代表 DES 算法的加密和解密过程，K 代表 DES 算法使用的密钥，M 代表明文，C 代表密文，3DES 算法表示为：

3DES 加密过程为：$C=E_{K3}(D_{K2}(E_{K1}(M)))$

3DES 解密过程为：$M=D_{K1}(E_{K2}(D_{K3}(C)))$

其中，K1、K2、K3 决定了算法的安全性，若三个密钥互不相同，本质上就相当于用一个长为 168 位的密钥进行加密。多年来，它在对付强力攻击时是比较安全的。若数据对安全性要求不那么高，则 K1 可以等于 K3，在这种情况下，密钥的有效长度为 112 位。

3.3　非对称加密算法

3.3.1　非对称加密算法原理

非对称加密算法（Asymmetric Cryptographic Algorithm）又名“公开密钥加密算法”。非对称加密算法需要两个密钥：公开密钥（Public Key，又称公钥）和私有密钥（Private Key，又称私钥）。

公钥与私钥是成对存在的，如果用公钥对数据进行加密，只有用对应的私钥才能解密；如果用私钥对数据进行加密，那么只能用对应的公钥才能解密。因为加密和解密使用的是两个不同的密钥，所以这种算法称为非对称加密算法。非对称加密算法实现机密信息交换的基本过程是：接收方生成一对密钥并将其中的公钥向其他方公开；得到该公钥的发送方使用该密钥对机密信息进行加密后再发送给接收方；接收方再用自己保存的私钥对加密后的信息进行解密，如图 3.3 所示。

另外，接收方可以使用自己的私钥对机密信息进行加密后再发送给发送方；发送方再用接收方的公钥对加密后的信息进行解密。接收方只能用其私钥解密由其公钥加密后的任何信息。非对称加密算法的保密性比较好，它消除了最终用户交换密钥的需要。非对称密钥体制的特点是算法复杂、强度大，使得加密解密速度没有对称加密解密的速度快。对称密钥体制中只有一种密钥，并且是非公开的，如果要解密就得让对方知道密钥，所以保证其安全性就是保证密钥的安全。而非对称密钥体制有两种密钥，其中一个是公开的，这样就可以不需要像对称密钥那样传输对方的密钥了，因此安全性就大了很多。

非对称加密算法典型的算法主要有 RSA、Elgamal、背包算法、Rabin、HD、ECC（椭圆曲线加密算法）。其中使用最广泛的是 RSA 算法。

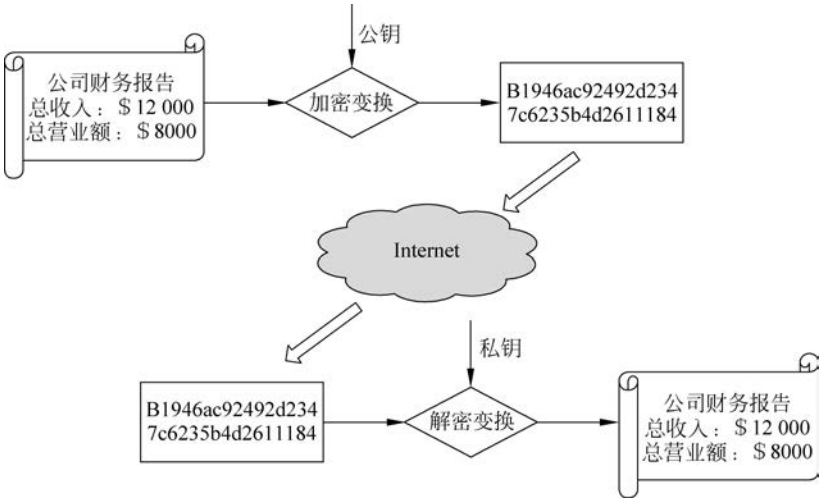

图 3.3 非对称加密算法实现机密信息交换的基本过程

3.3.2 RSA 算法

RSA 算法是 1977 年由 Ron Rivest、Adi Shamirh 和 Len Adleman 在美国麻省理工学院开发的。RSA 取名来自三位开发者的名字。RSA 算法是目前最有影响力的公钥加密算法，它能够抵抗到目前为止已知的所有密码攻击，已被 ISO 推荐为公钥数据加密标准。RSA 算法基于一个十分简单的数论事实：将两个大素数相乘十分容易，但对其乘积进行因式分解却极其困难，因此可以将乘积公开作为加密密钥。

RSA 算法的思路为：为了产生两个密钥，先取两个大素数 p 和 q，为了获得最大程度的安全性，两数的长度一样，计算乘积 $n=p\times q$，然后随机选取加密密钥 e，使 e 和 $(p-1)\times(q-1)$ 互素。最后用欧几里得(Euclid)扩展算法计算解密密钥 d，d 满足 $ed\equiv 1 \bmod [(p-1)(q-1)]$，即 $d\equiv e^{-1} \bmod [(p-1)(q-1)]$。则 e 和 n 为公开密钥，d 是私人密钥。两个大数 p 和 q 应该立即丢弃，不让任何人知道。一般选择公开密钥 e 比私人密钥 d 小。最常选用的 e 值有 3、17 和 65 537。

加密消息时，首先将消息分成比 n 小的数据分组(采用二进制数，选到小于 n 的 2 的最大次幂)，设 m_i 表示消息分组，c_i 表示加密后的密文，它与 m_i 具有相同的长度。

加密过程：$c_i=m_i^e \bmod n$

解密过程：$m_i=c_i^d \bmod m$

3.3.3 RSA 算法的安全性与速度

RSA 算法的安全性依赖于大数分解，但是否等同于大数分解一直未能得到理论上的证明，因为没有证明破解 RSA 就一定需要作大数分解。假设存在一种无须分解大数的算法，那它肯定可以修改成为大数分解算法。目前，RSA 算法的一些变种算法已被证明等价于大数分解。不管怎样，分解 n 是最直接的攻击方法。现在，人们已能分解多个十进制位的大素数。因此，模数 n 必须选大一些，具体数值因具体适用情况而定。

由于进行的都是大数计算，无论是软件还是硬件实现，RSA 算法最快的情况也比 DES 算法慢很多。速度一直是 RSA 算法的缺陷。一般来说它只用于少量数据加密。

3.3.4　非对称与对称加密算法的比较

对于非对称加密算法而言，首先，用于消息解密的密钥值与用于消息加密的密钥值不同。其次，非对称加密算法比对称加密算法慢很多，但在保护通信安全方面，非对称加密算法却具有对称密码难以企及的优势。为说明这种优势，使用对称加密算法的例子来强调：Alice 使用密钥 K 加密消息并将其发送给 Bob，Bob 收到加密的消息后，使用密钥 K 对其解密以恢复原始消息。这里存在一个问题，即 Alice 如何将用于加密消息的密钥值发送给 Bob？答案是，Alice 发送密钥值给 Bob 时必须通过独立的安全通信信道（即没人能监听到该信道中的通信）。这种使用独立安全信道来交换对称加密算法密钥的需求会带来更多问题：首先，存在独立的安全信道，但是安全信道的带宽有限，不能直接用它发送原始消息。其次，Alice 和 Bob 不能确定他们的密钥值可以保持多久而不泄露（即不被其他人知道）以及何时交换新的密钥值。当然，这些问题不只 Alice 会遇到，Bob 和其他人都会遇到，他们都需要交换密钥并处理这些密钥管理问题（事实上，X9.17 是一项 DES 密钥管理 ANSI 标准[ANSI X9.17]）。如果 Alice 要给数百人发送消息，那么事情将更麻烦，她必须使用不同的密钥值来加密每条消息。例如，要给 200 个人发送通知，Alice 需要加密消息 200 次，对每个接收方加密一次消息。显然，在这种情况下，使用对称加密算法来进行安全通信的开销相当大。非对称加密算法的主要优势就是使用两个而不是一个密钥值：一个密钥值用来加密消息；另一个密钥值用来解密消息。这两个密钥值在同一个过程中生成，称为密钥对。用来加密消息的密钥称为公钥，用来解密消息的密钥称为私钥。用公钥加密的消息只能用与之对应的私钥来解密，私钥除了持有者外无人知道，而公钥却可通过非安全通道来发送或在目录中发布。Alice 需要通过电子邮件给 Bob 发送一个机密文档。首先，Bob 使用电子邮件将自己的公钥发送给 Alice。然后 Alice 用 Bob 的公钥对文档加密并通过电子邮件将加密消息发送给 Bob。由于任何用 Bob 的公钥加密的消息只能用 Bob 的私钥解密，因此即使窥探者知道 Bob 的公钥，消息也仍是安全的。Bob 在收到加密消息后，用自己的私钥进行解密从而恢复原始文档。

3.4　数据完整性

仅用加密方法实现消息的安全传输是不够的，攻击者虽无法破译加密消息，但如果攻击者篡改或破坏了消息，会使接收者也无法收到正确的消息，因此，需要有一种机制来保证接收者能够辨别收到的消息是否是发送者发送的原始数据，这种机制称为数据完整性机制。

数据完整性验证是通过下述方法来实现的。消息的发送者用要发送的消息和一定的算法生成一个附件，并将附件与消息一起发送出去。消息的接收者收到消息和附件后，用同样的算法将接收到的消息生成一个新的附件。把新的附件与接收到的附件相比较，如果相同，则说明收到的消息是正确的，否则说明消息在传送中出现了错误。其一般过程如图 3.4 所示，Hash 表示一种单向的散列函数，通过这种函数可以生成一个固定长度的值，此值即为校验值。

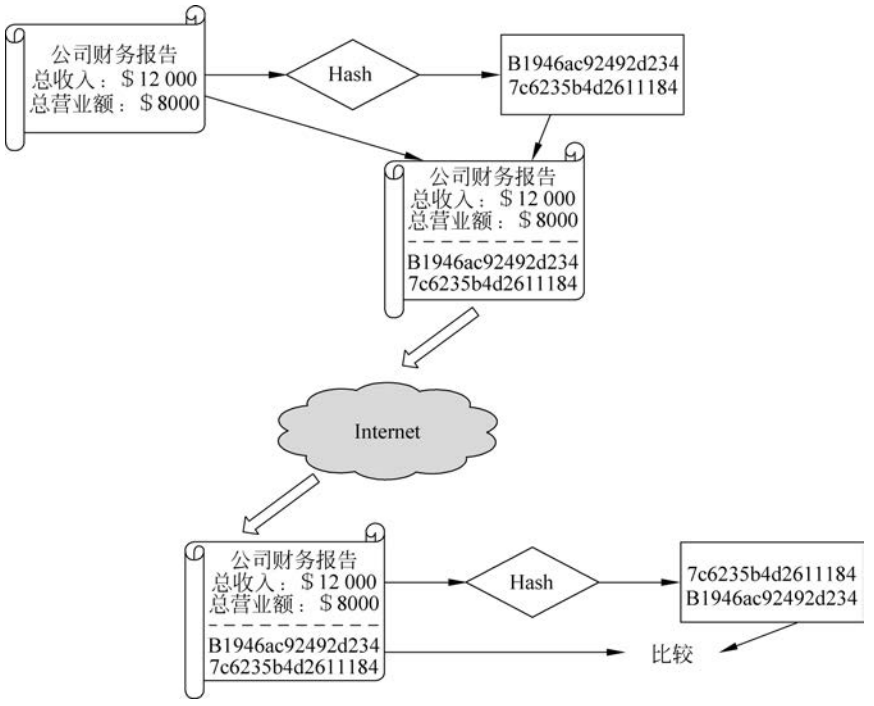

图 3.4 消息完整性验证

所有散列函数都有一个基本特性：如果两个散列值不同(根据同一函数)，那么这两个散列值的原始输入也不相同。这个特性使散列函数具有确定性的结果。但散列函数的输入和输出不是一一对应的，如果两个散列值相同，两个输入值很可能是相同的，但并不能绝对肯定二者一定相等。输入一些数据计算出散列值，然后部分改变输入值，一个具有强混淆特性的散列函数会产生一个完全不同的散列值。

MD5 和 SHA1 可以说是目前应用最广泛的散列(Hash)算法，它们都是以 MD4 为基础设计的。

1. MD4

MD4(RFC 1320)是 MIT 的 Ronald L. Rivest 于 1990 年设计的，MD 是 Message Digest 的缩写。它需要在 32 位字长的处理器上用高速软件实现，是通过基于 32 位操作数的位操作来实现的。

2. MD5

MD5(RFC 1321)是 Ronald L. Rivest 于 1991 年对 MD4 的改进版本。它的输入仍以 512 位分组，其输出是 4 个 32 位字的级联，与 MD4 相同。MD5 比 MD4 复杂，并且速度较之要慢一点，但更安全，在抗分析和抗差分方面表现更好。

3. SHA1

SHA1 是由 NIST 和 NSA 设计为同 DSA 一起使用的算法，它对长度小于 2^{64} 位的输入产生长度为 160b 的散列值，因此抗穷举性更好。SHA1 设计时基于和 MD4 相同原理，并且模仿了该算法。

3.5　PGP 加密系统

3.5.1　PGP 简介

PGP 全称为 Pretty Good Privacy，是一种在信息安全传输领域首选的加密软件，其技术特性是采用了非对称的加密体系。由于美国对信息加密产品有严格的法律约束，特别是对向美国、加拿大之外的国家散播该类信息，以及出售、发布该类软件的约束更为严格，因此限制了 PGP 的一些发展和普及，现在该软件的主要使用对象为情报机构、政府机构、信息安全工作者（例如较高水平的安全专家和有一定资历的黑客）。PGP 最初的设计主要是用于邮件加密，如今已经发展到了可以加密整个硬盘、分区、文件、文件夹，还可以与邮件软件集成进行邮件加密，甚至可以对 ICQ 的聊天信息实时加密。你和对方只要安装了 PGP，就可利用其 ICQ 加密组件在你和对方聊天的同时进行加密或解密，和正常使用没有什么差别，最大限度地保证了你和对方的聊天信息不被窃取或监视。现版本最大支持 4096 位加密强度。

以下实验环境所使用到的 PGP 加密软件的版本为 Gpg4win，在 GPG 官方网站可以直接下载，该软件为开源免费软件，所采用的操作系统为 Windows 10。

3.5.2　GPG 的安装

下载 Gpg4win 后，双击 Gpg4win 自动解压文件，运行安装文件，系统自动进入安装向导，主要步骤如下。

（1）双击运行安装程序，单击“下一步”按钮，进到下安装引导界面，如图 3.5 所示，选择默认项即可，然后单击“下一步”按钮。

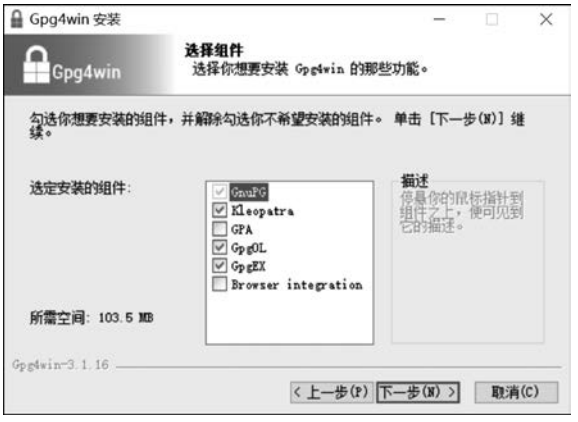

图 3.5　安装引导

（2）如图 3.6 所示，选择软件所安装的路径，可以是默认路径，也可以自定义路径。如果是自定义路径，\Gpg4win 的前面只能是盘符，不能有上一级的文件夹。作为演示这里就直接选择默认路径，单击“安装”按钮。

（3）如图 3.7 所示，单击“完成”按钮，则视为该软件已经成功安装。

图 3.6　选择安装路径

图 3.7　完成安装

3.5.3　创建密钥对

(1) 完成安装之后双击运行 Kleopatra 软件,单击左上角的“文件”按钮,接着单击“新建密钥对”按钮,在如图 3.8 所示的界面中选择“创建个人 OpenPGP 密钥对”选项,然后单击“下一步”按钮。

图 3.8　创建个人 OpenPGP 密钥对

（2）如图 3.9 所示，在“名字”和“电子邮件”文本框中分别输入目的名字和目的电子邮件，这里以 Alice 为例，在输入完名字和电子邮箱之后单击“高级设置”按钮。如图 3.10 所示，将默认的 3072 比特改为 4096 比特，选择框下方可以更改该密钥的有效期，然后单击 OK 按钮，再单击“新建”按钮。

图 3.9　创建密钥的名字

图 3.10　高级设置

(3) 如图 3.11 所示,直接单击“完成”按钮,证书界面下就会有刚刚新建的密钥对,如图 3.12 所示。

图 3.11 完成创建密钥对

图 3.12 查看现有的密钥对

3.5.4 加密文件

(1) 如图 3.13 所示,右击所需要的加密的文件,在弹出的快捷菜单中选择 More GpgEX options→Encrypt 选项进行加密。如图 3.14 所示,在“为我加密”栏中选择加密所用到的公

钥(一般默认情况下就是你刚刚所创建的密钥对),在“输出”栏中可以选择加密后的文件所存放的路径,单击“加密”按钮,生成的加密文件的扩展名为.gpg。

图 3.13　加密文件 1

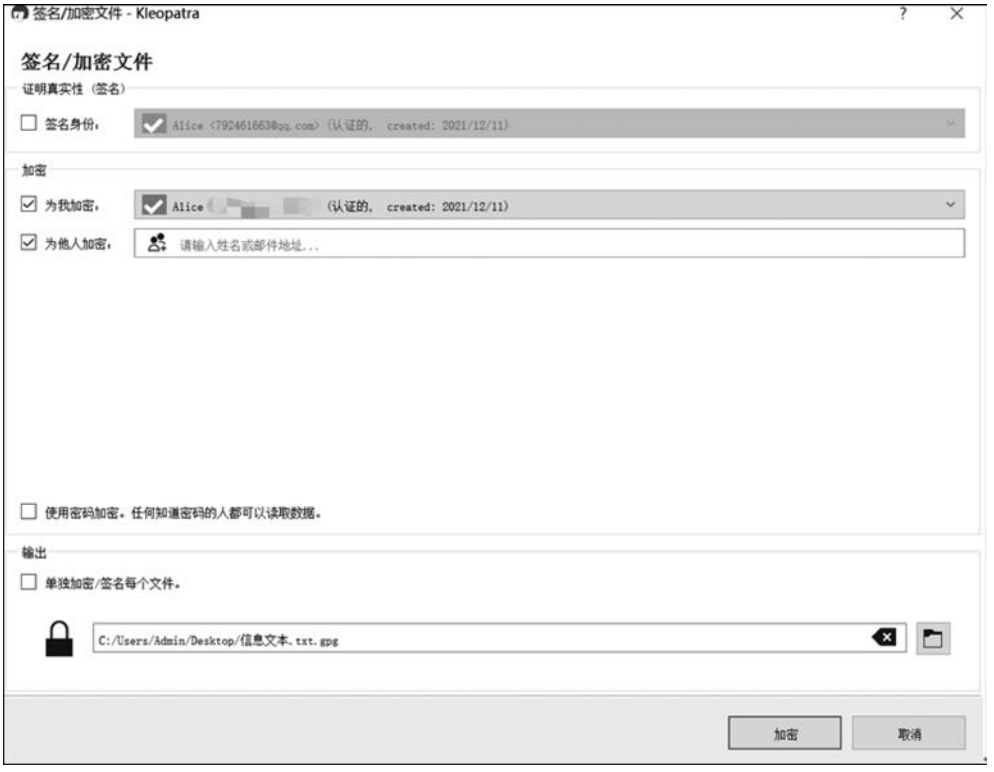

图 3.14　加密文件 2

(2) 如图 3.15 所示,单击“完成”按钮,在上一步选择的路径下多出一个.pgp 文件,这个文件就是加密后的文件,直接打开后发现是一串乱码,如图 3.16 所示。

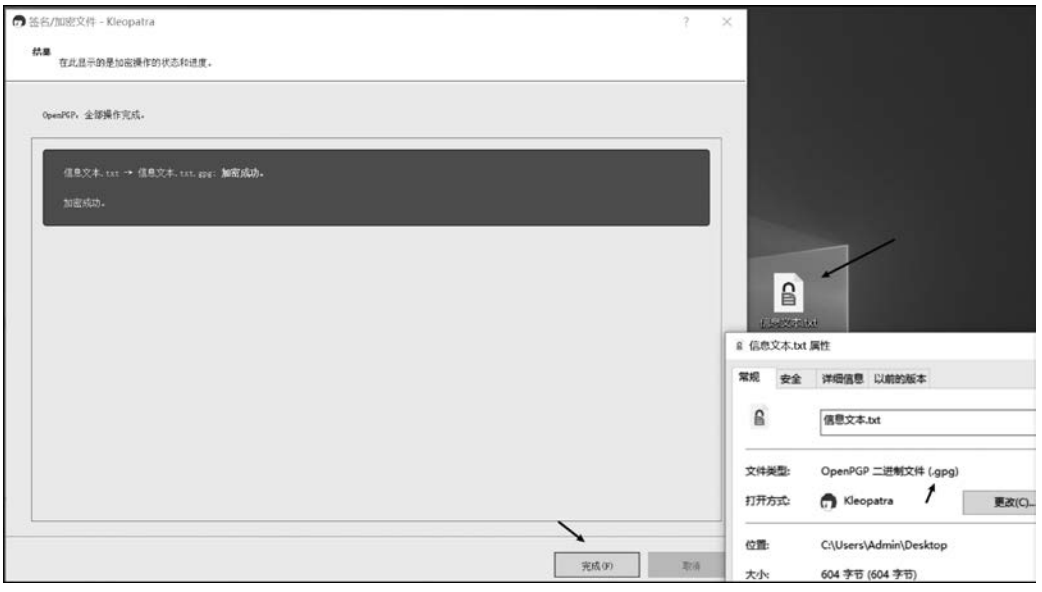

图 3.15 完成加密

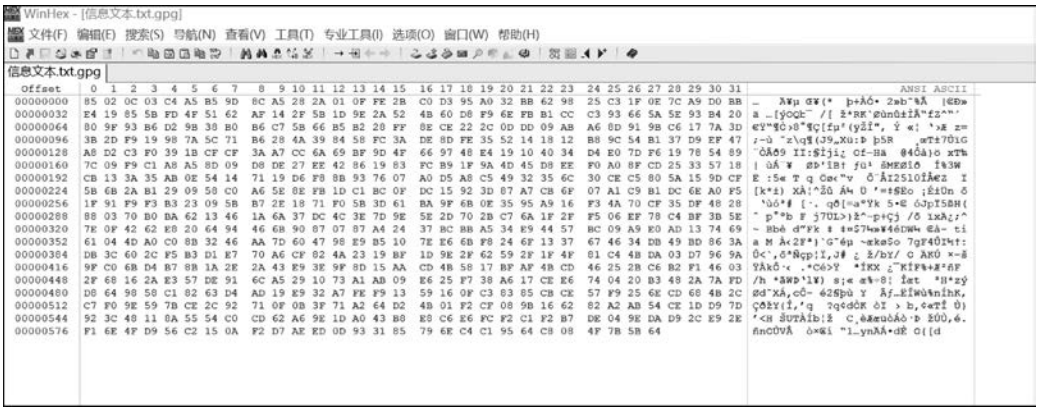

图 3.16 查看加密后的文件

3.5.5 解密文件

(1) 接下来就对刚刚加密的文件使用密钥对它进行解密。如图 3.17 所示,右击加密后的文件,在弹出的快捷菜单中选择 More GpgEX options→Decrypt 选项进行解密。如图 3.18 所示,在“输出文件夹”栏中可以选择解密后文件的存放路径,其下可以看到加密的文件.gpg 已经解密成功,在选择完存放路径之后,单击 Save All 按钮。

(2) 如图 3.19 所示,进入刚刚所选择的存放路径,双击文件,查看原文件。

图 3.17　解密文件

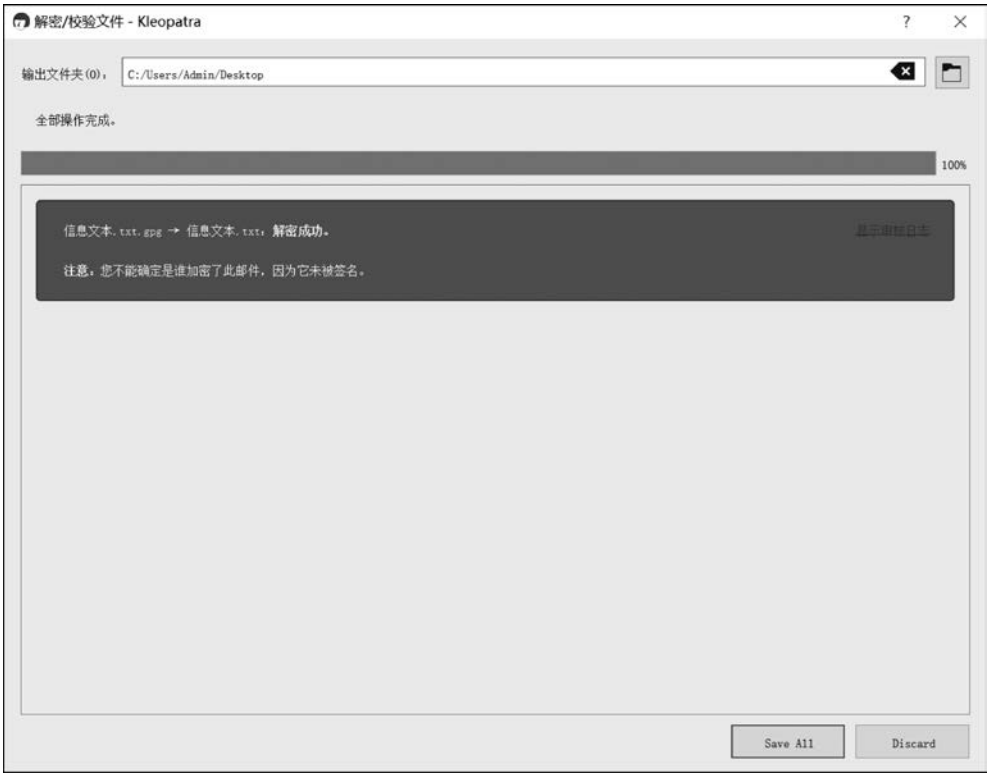

图 3.18　解密成功

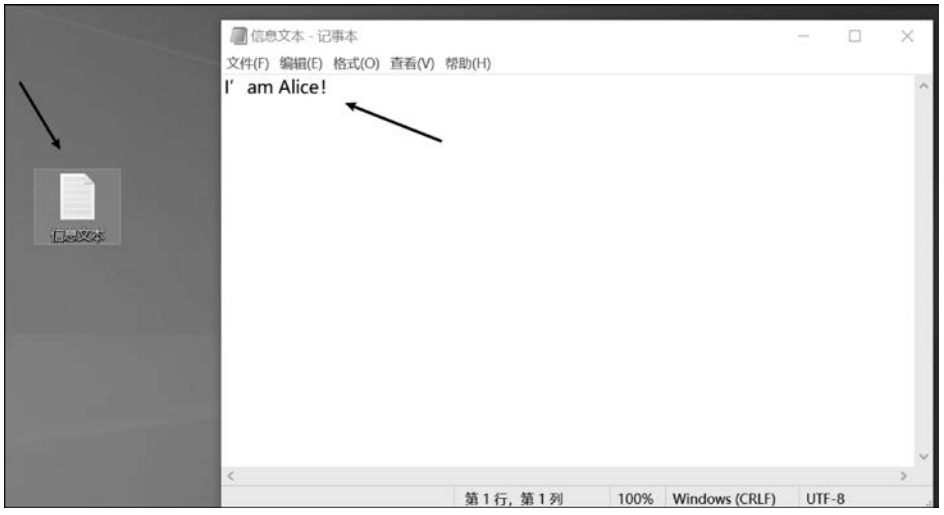

图 3.19　验证

3.5.6　导入其他人的公钥进行加密

课业任务 3-1

课业任务 3-1

Alice 是 WYL 公司的一个技术人员，Bob 是 WYL 公司分部的技术开发人员。身处异地的 Bob 与 Alice 现需要合作开发一套软件，考虑文件的重要性跟机密性，Bob 将生成的公钥给予 Alice 对相对应的文件进行加密。

(1) 双击并运行 Kleopatra 软件，进入界面后，如图 3.20 所示，单击“导入”按钮，选择 Bob 的证书文件，单击“打开”按钮。如图 3.21 所示，导入成功后，单击 OK 按钮。

图 3.20　导入证书

图 3.21　导入成功

（2）如图 3.22 所示，右击需要的加密的文件，在弹出的快捷菜单中选择 More GpgEX options→Encrypt 选项进行加密。如图 3.23 所示，在“为他人加密”栏中输入刚刚导入的 Bob 名称并选择，在“输出”栏中选择要输出加密后文件的位置，选择完之后单击“加密”按钮（下一步会有一个自动加密的警告直接单击“继续”按钮即可），在显示加密完成后单击“完成”按钮。

图 3.22　加密文件操作

（3）双击加密后的文件，发现是一串乱码，如图 3.24 所示，如果直接去解密那个文件，就会发现解密失败。其原因是利用了 Bob 的公钥进行加密，但是没有 Bob 的私钥，所以就会出现解密失败的情况。为了保证数据的安全性，一般是将公钥给到需要执行加密的一方，加密完成后的文件传回给对方，然后对方使用私钥对加密的文件进行解密，最终得到加密前的文件。

图 3.23 选择加密的路径

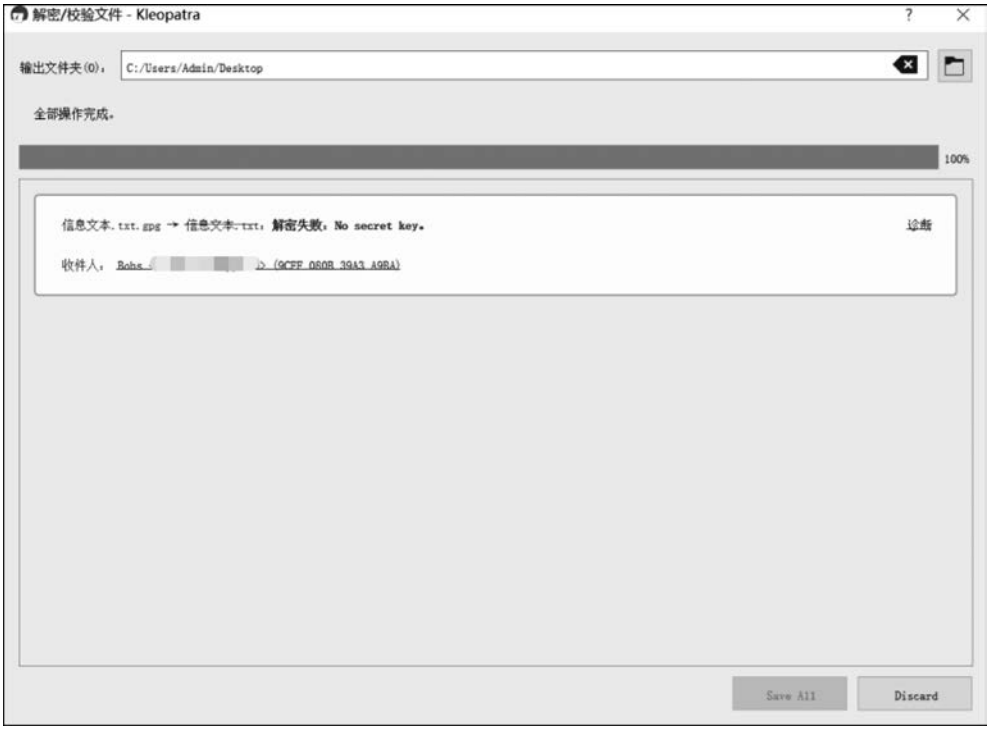

图 3.24 解密失败

3.5.7　加密电子邮件

课业任务 3-2

课业任务
3-2

Alice 是 WYL 公司总部的技术开发人员，Bob 是 WYL 公司分部的技术开发人员。身处异地的 Bob 与 Alice 现需要合作开发一套软件，经常需要通过互联网使用邮件交换数据，而这套软件里的文件涉及公司的核心机密，故需要在传输的过程中注意保密性。

(1) 打开 Outlook 邮箱，单击“新建电子邮件”按钮进入编写邮件界面，如图 3.25 所示，在“收件人”栏中输入收件人的邮箱，在“主题”栏中输入邮件的主题，在下方的空白处输入邮件的正文内容，在完成编辑之后，单击“邮件”按钮，将鼠标移至“…”，选择 Secure→Encrypt 选项进行邮件加密，单击“发送”按钮。如图 3.26 所示在单击完“发送”按钮之后，选择所使用加密的公钥，单击 OK 按钮即可完成发送。

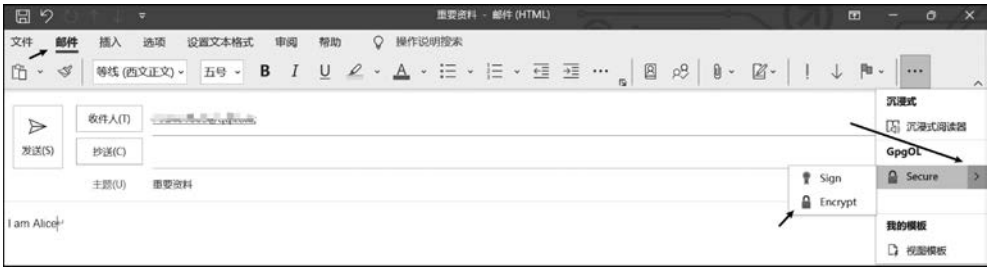

图 3.25　编写加密邮件

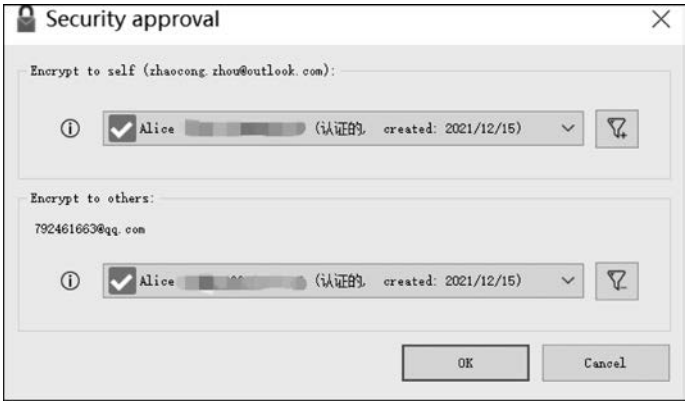

图 3.26　选择加密公钥

(2) 如图 3.27 所示，查看收到的邮件时发现文件内容被隐藏，取而代之的是两个加密的附件。将附件下载到本地，进到本地保存的路径下，如图 3.28 所示，右击.asc 文件(这个文件为 GPG 加密后的加密文件，所需要解密的也是该文件)，在弹出的快捷菜单中选择 More GpgEX options→Decrypt 选项进行解密(详细解密步骤可参考 3.5.5 解密文件)。

提示：如果在解密时已经将密钥对或者私钥导入软件 Kleopatra 中，系统会默认直接使用该密钥对文件进行解密。

图 3.27　加密后的邮件

图 3.28　解密文件操作

(3) 在执行完上一步的解密过程后,在选择存放的路径中会多出一个文件,双击该文件,即可查看解密后邮件的内容,如图 3.29 所示。

图 3.29　解密后文件内容

练习题

1. 单项选择题

(1) 就目前计算机设备的计算能力而言,数据加密标准 DES 不能抵抗对密钥的穷举搜索攻击,其原因是(　　)

A. DES 算法是公开的

B. DES 的密钥较短

C. DES 除了其中 S 盒是非线性变换外,其余变换均为线性变换

D. DES 算法简单

(2) 数字签名可以做到(　　)。

A. 防止窃听

B. 防止接收方的抵赖和发送方的伪造

C. 防止发送方的抵赖和接收方的伪造

D. 防止窃听者攻击

(3) 下列关于 PGP(Pretty Good Privacy)的说法不正确的是(　　)。

A. PGP 可用于电子邮件,也可用于文件存储

B. PGP 可选用 MD5 和 SHA 两种散列算法

C. PGP 采用了 ZIP 数据压缩算法

D. PGP 不可使用 IDEA 加密算法

(4) 为了保障数据的存储和传输安全,需要对一些重要数据进行加密。由于对称密码算法(①),因此特别适合对大量的数据进行加密。DES 实际的密钥长度是(②)位。

① A. 比非对称密码算法更安全

B. 比非对称密码算法密钥长度更长

C. 比非对称密码算法效率更高

D. 还能同时用于身份认证

② A. 56　　B. 64　　C. 128　　D. 256

(5) 使用 Telnet 协议进行远程管理时,(　　)。

A. 包括用户名和口令在内,所有传输的数据都不会被自动加密

B. 包括用户名和口令在内,所有传输的数据都会被自动加密

C. 用户名和口令是加密传输的,而其他数据则是以文明方式传输的

D. 用户名和口令是不加密传输的,其他数据则是以加密传输的

(6) 以下不属于对称密码算法的是(　　)。

A. IDEA　　B. RC　　C. DES　　D. RSA

(7) 以下算法中属于非对称算法的是(　　)。

A. 散列算法　　B. RSA 算法　　C. IDEA　　D. 3 DES

(8) 以下不属于公钥管理方法的是(　　)。

A. 公开发布　　B. 公用目录表　　C. 公钥管理机构　　D. 数据加密

(9) 以下不属于非对称密码算法特点的是(　　)。

A. 计算量大　　B. 处理速度慢

C. 使用两个密码　　D. 适合加密长数据

(10) 假设使用一种加密算法,它的加密方法很简单:将每一个字母加5,即a加密成f。这种算法的密钥就是5,那么它属于(　　)。

A. 对称加密技术　　B. 分组密码技术

C. 公钥加密技术　　D. 单向散列函数密码技术

(11) DES属于(　　)。

A. 对称密码体制　　B. 恺撒密码体制

C. 非对称密码体制　　D. 公钥密码体制

(12) 第一个实用的、迄今为止应用最广的公钥密码体制是(　　)。

A. RSA　　B. Elgamal

C. ECC　　D. NTRU

2. 填空题

(1) (　　)的重要性在于赋予消息M唯一的"指纹",其主要作用于验证消息M的完整性。

(2) 非对称加密算法有两把密钥:一把称为私钥;另一把称为(　　)。

(3) IDEA是目前公开的最好和最安全的分组密码算法之一,它采用(　　)位密钥对数据进行加密。

(4) RSA算法的安全是基于(　　)分解的难度。

(5) (　　)技术是指一种将内部网络与外部网络隔离的技术,以防止外部用户对内部用户进行攻击。

(6) MD5把可变长度的消息散列成(　　)位固定长度的值。

(7) DES算法加密过程中输入的明文长度是(　　)位,整个加密过程需经过(　　)轮的子变换。

(8) 在密码学中通常将源消息称为(　　),将加密后的消息称为(　　)。这个变换处理过程称为(　　)过程,它的逆过程称为(　　)过程。

3. 简答题

(1) 对称加密算法与非对称加密算法有哪些优缺点?

(2) 如何验证数据完整性?

(3) 散列算法有何特点?

(4) 简要说明DES加密算法的关键步骤。

(5) 什么情况下需要数字签名?简述数字签名的算法。

(6) 什么是身份认证?用哪些方法可以实现?

(7) RSA算法的基本原理和主要步骤是什么?

4. 综合应用题

(1) WYL 公司的业务员甲与客户乙通过 Internet 交换商业电子邮件。为保障邮件内容的安全，采用安全电子邮件技术对邮件内容进行加密和数字签名。安全电子邮件技术的实现原理如图 3.30 所示。根据要求，回答问题 1～问题 4，并把答案填入下面对应的位置。

(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)

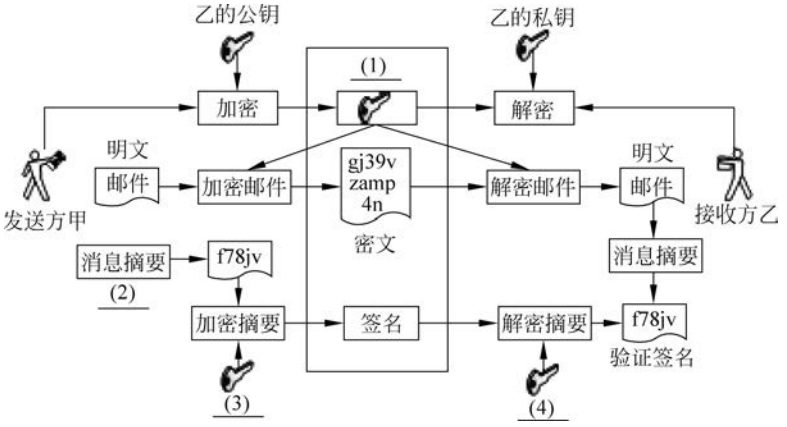

图 3.30　安全电子邮件技术的实现原理

【问题 1】

给图 3.30 中(1)～(4)处选择合适的答案。(1)～(4)的备选答案如下：

A. DES 算法　　B. MD5 算法　　C. 会话密钥　　D. 数字证书

E. 甲的共钥　　F. 甲的私钥　　G. 乙的共钥　　H. 乙的私钥

【问题 2】

以下关于报文摘要的说法中正确的有(5)、(6)。(5)和(6)的备选答案如下：

A. 不同的邮件很可能生成相同的摘要

B. 由邮件计算出其摘要的时间非常短

C. 由邮件计算出其摘要的时间非常长

D. 摘要的长度比输入邮件的长度长

E. 不同输入邮件计算出的摘要长度相同

F. 仅根据摘要很容易还原出原邮件

【问题 3】

甲使用 Outlook Express 撰写发送给乙的邮件，他应该使用(7)的数字证书来添加数字签名，而使用(8)的数字证书来对邮件加密。(7)和(8)的备选答案如下：

A. 甲　　B. 乙　　C. 第三方　　D. CA 认证中心

【问题 4】

乙收到了地址为甲的含数字签名的邮件，他可以通过验证数字签名来确认的信息有

(9)、(10)。(9)和(10)的备选答案如下：

A. 邮件在传送过程中是否加密　　B. 邮件中是否含病毒

C. 邮件是否被篡改　　D. 邮件的发送者是否是甲

(2) 恺撒密码明文字母表为 ABCDEFGHIJKLMNOPQRSTUVWXYZ。它的密文密码表是什么？

(3) 利用列置换密码算法，密钥用对换表示为 o=(245)，加密 xiandaimimaxue，写出解密过程。