第 3 章

电子商务加密技术及应用

引导案例　网络病毒与网络犯罪

2017 年 5 月 12 日，WannaCry 勒索病毒在全球大肆爆发，该病毒对 99 个国家实施了超过 75 000 次攻击，全球 20 万台计算机文件被加密为.onion 后缀，用户需缴付约 300 比特币的赎金才能解密恢复被感染的文件。我国也成为此次勒索病毒爆发的重灾区，在它的影响下，我国多地的出入境、派出所等公安网疑似遭遇了病毒袭击，不得不一度暂时停办出入境业务；勒索病毒也侵袭到生产网络中，中石油旗下不少加油站也因遭受病毒袭击一度“断网”，使在线支付业务一度中断；彼时正值毕业季，勒索病毒在我国校园网内的肆虐，甚至还导致不少毕业生的毕业设计论文被锁。有关法律专家称，“WannaCry 勒索病毒”的制造者是典型的故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行的行为。

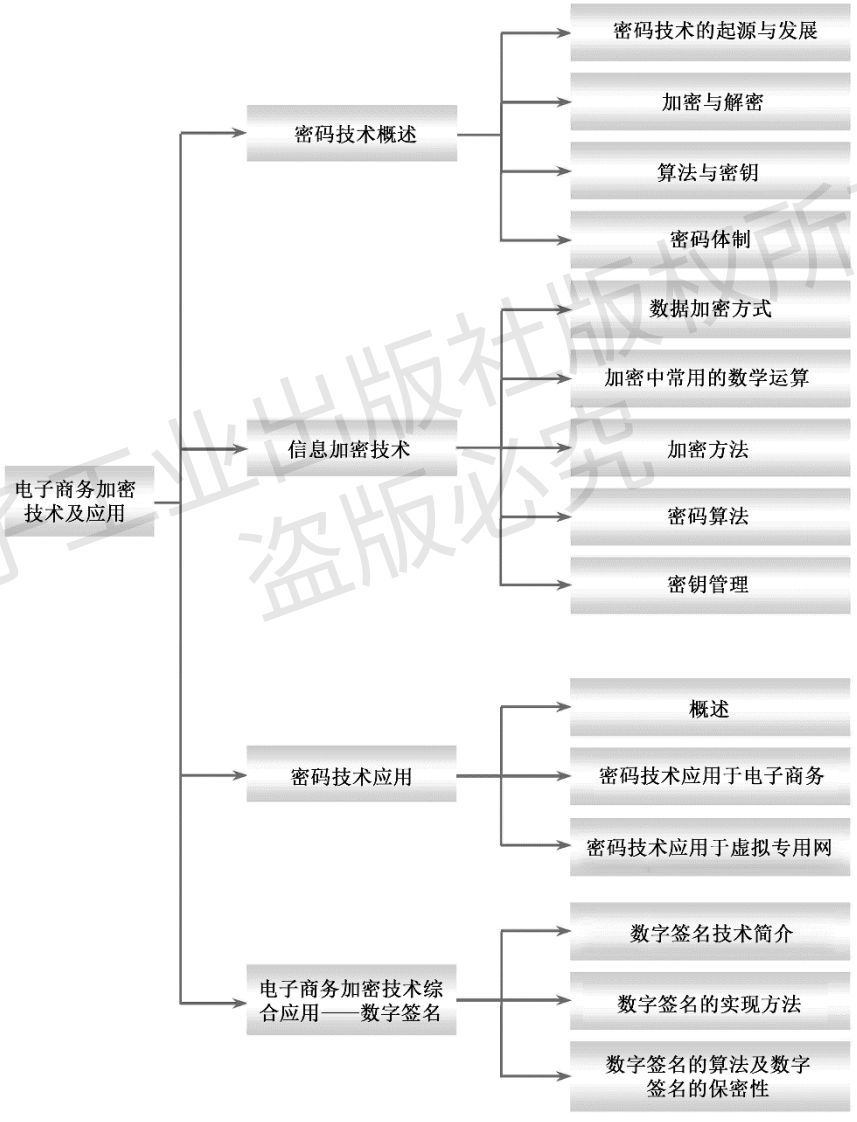
随着互联网和电子商务的快速发展，利用网络犯罪的行为会大量出现，为了保证电子商务的顺利发展，法律保障是必不可少的。2017 年《中华人民共和国网络安全法》实施，是我国网络安全的重要里程碑。在本章中，我们就重点讨论如何使自己的密码不被盗取，如何加密才更安全。

本章学习目标

1. 了解密码技术的发展史；
2. 了解加密与解密的过程；
3. 掌握 DES 算法；

4. 掌握 RSA 算法；
5. 掌握 DES 算法与 RSA 算法的比较；
6. 了解电子商务加密技术综合应用。

学习导航



3.1　密码技术概述

3.1.1　密码技术的起源与发展

作为保障数据安全的一种方式，数据加密起源于公元前 2000 年。埃及人最早使用特别的象形文字作为信息编码来给文字加密。随着时间的推移，巴比伦、美索不达米亚和希腊都开始用密码的方法来保护它们的书面信息不被泄露。

研究消息保密技术的科学叫作密码编码学（Cryptography），而研究在不知道密钥的情况下破译密文、还原明文的科学叫作密码分析学（Cryptanalysis），二者合称密码学（Cryptology）。密码编码学与密码分析学看起来是互相冲突的，事实上两者是相辅相成的，正是密码分析学的发展促进了密码编码学的进步。现代密码学是依赖理论数学而创建和发展的，所以，现代的密码学家通常也是理论数学家。

在密码学中，密码是实现秘密通信的主要手段，是隐蔽语言、文字、图像的特殊符号。凡是用特种符号按照通信双方约定的方法把电文的原型隐蔽起来、不为第三者所识别的通信方式，都称为密码通信。

密码学的发展分为两个阶段：第一个阶段是计算机出现以前，称为传统密码学阶段，基本是靠人工对消息加密、传输和防破译；第二个阶段是计算机密码学阶段，在计算机通信过程中采用密码技术将信息隐蔽起来，再将隐蔽的信息传输出去，信息在传输过程中即使被窃取或被截获也不会泄露信息的内容，从而保证了信息传输的安全。

3.1.2　加密与解密

数据加密是一种限制对网络上传输数据的访问权的技术。它的基本过程就是对原来为明文的文件或数据按某种算法进行处理，使其成为不可读的一段代码（通常被称为“密文”，“密文”只能在输入相应的密钥之后才能显示出本来内容），通过这样的方法来达到保护数据不被非法窃取、阅读的目的。该过程的逆过程为解密，即将该编码信息转化为原来数据的过程。它是加密的反向处理，但解密者必须利用相同类型的加密设备和密钥对密文进行解密。

1．加密的基本功能

（1）防止不速之客查看机密的数据文件。

（2）防止机密数据被泄露或篡改。

（3）防止特权用户（如系统管理员）查看私人数据文件。

（4）使入侵者不能轻易地查找一个系统的文件。

2．对加密信息进行解密的条件

（1）必须知道解密规则或算法。

（2）必须知道解密的密钥。

3．加密与解密的过程

加密与解密的过程如图 3.1 所示。

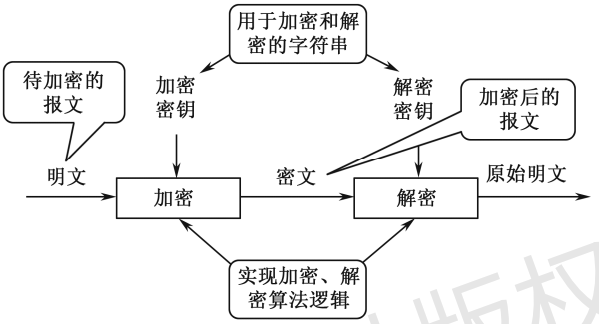


图 3.1　加密与解密的过程

3.1.3　算法与密钥

密码算法是用于加密和解密的数学函数。通常情况下，有两个相关函数，一个用作加密，另一个用作解密。

如果算法的保密性是基于保持算法的秘密，这种算法称为受限制的算法。受限制的算法具有历史意义，但按现在的标准，它的保密性已远远不够。大的或经常变换的用户组织不能使用它们，因为只要有一个用户离开这个组织，其他的用户就必须改换为另外不同的算法。

更糟的是，受限制的密码算法不可能进行质量控制或标准化。在受限制的算法中，每个用户组织必须有他们自己的唯一算法，这样的组织不可能采用流行的硬件或软件产品，但窃听者却可以买到这些流行产品并学习算法，于是用户不得不自己编写算法并予以实现，如果这个组织中没有好的密码学家，那么他们就无法知道他们是否拥有安全的算法。

尽管存在以上缺陷，受限制的算法对低密级的应用来说还是很流行的，使用该算法的用户或者是没有认识到系统中内在的问题，或者是不在乎这些问题。

3.1.4　密码体制

根据密钥类型不同，现代密码技术可分为两类：一类是对称密码体制；另一类是非对称密码体制。

密码算法中的密钥是一种参数，是由使用密码体制的用户随机选取的。密钥成为唯一

能控制明文与密文之间变换的关键。它通常是一个随机的字符串，分为两种：对称密钥与非对称密钥。

1．对称密码体制

对称密码体制也称单钥密码体制或常规密钥密码体制。对称密码已被人们使用了数千年，它有各种形式，从简单的替换密码到复杂的建构方式密码。对称密码系统运行起来通常非常快速，却易受攻击，因为其用于加密的密钥必须与需要对信息进行解密的所有人一起共用，这带来了极大的安全隐患。

对称密码系统是加密和解密均采用同一个密钥，而且通信双方都必须获得密钥，并保持密钥不被他人所获取。

对称密码系统的安全性依赖于两个因素：第一，加密算法必须是足够强的，仅仅基于密文本身去解密信息在实践上是不可能的；第二，加密方法的安全性依赖于密钥的秘密性，而不是算法的秘密性，因此，我们没有必要确保算法的秘密性，而需要保证密钥的秘密性。对称密码系统的算法实现速度极快，从 AES 候选算法的测试结果看，软件实现的速度都达到了每秒数兆或数十兆比特。对称密码系统的这些特点使其有着广泛的应用。因为算法不需要保密，所以制造商可以开发出低成本的芯片以实现数据加密。这些芯片有着广泛的应用，适合于大规模生产。

对称密码系统最大的问题是密钥的分发和管理非常复杂、价格高昂。例如，对于具有 n 个用户的网络，需要 $n(n-1)/2$ 个密钥，在用户群不是很大的情况下，对称密码系统是有效的。但是对于大型网络，当用户群很大、分布很广时，密钥的分配和保存就成了大问题。对称加密算法的另一个缺点是不能实现数字签名。

2．非对称密码体制

非对称密码体制又称双钥密码体制或公钥密码体制。非对称密码系统使用两个密钥：一个是公开密钥，用来加密纯文字；另一个是私有密钥，只能用来解密。也可以使用私有密钥加密某些信息，然后用公开密钥来解密。公开密钥是大家都可以知道的，这样拿这个公开密钥能够解密的人就知道此信息是来自持有相应私有密钥的人，从而达到认证作用。如有黑客想利用用户的公开密钥找出用户的私有密钥，必须做许多尝试，以现在的计算机技术，要在合理时间内将密码计算出来并不可行。因此，非对称加密技术适合应用在高安全性要求的作业上，它能够确保信息在传输过程中不会被泄露。

非对称密码系统采用的加密钥匙（公钥）和解密钥匙（私钥）是不同的。由于加密钥匙是公开的，密钥的分配和管理就很简单，如对于具有 n 个用户的网络，仅需要 $2n$ 个密钥。非对称密码系统还能够很容易地实现数字签名，因此最适合电子商务应用需要。在实际应用中，非对称密码系统并没有完全取代对称密码系统，这是因为非对称密码系统基于尖端的数学难题，计算非常复杂，它的安全性虽然更高，但它的实现速度却远赶不上对称密码

系统。在实际应用中可利用二者各自的优点，采用对称密码系统加密文件，采用非对称密码系统加密“加密文件”的密钥（会话密钥），这就是混合密码系统，它较好地解决了运算速度问题和密钥分配管理问题。因此，非对称密码体制通常被用来加密关键性的、核心的机密数据，而对称密码体制通常被用来加密大量的数据。

3.2 信息加密技术

3.2.1 数据加密方式

目前主要流行三种数据加密方式：链路加密、节点加密和端到端加密。

1. 链路加密

链路加密是目前最常用的一种加密方法，通常在网络层以下的物理层或数据链路层实现。链路加密只需要把一对密码设备安装在两个节点之间的线路上，即把密码设备安装在节点主机和调制解调器之间，使用相同的密钥即可实现。对于链路加密，所有信息在被传输之前进行加密，每个节点对接收到的信息进行解密，然后使用下一个链路的密钥对信息进行加密，最后进行传输。

由于在每个中间传输节点信息均被解密后重新进行加密，因此包括路由信息在内的链路上的所有数据均以密文形式出现。一条信息可能要经过许多通信链路的传输才能到达目的地。因此，一旦在一条线路上采用链路加密，往往需要在整个网络内部都采用链路加密，如图 3.2 所示。这样，链路加密就掩盖了被传输信息的源点与终点之间的线路。

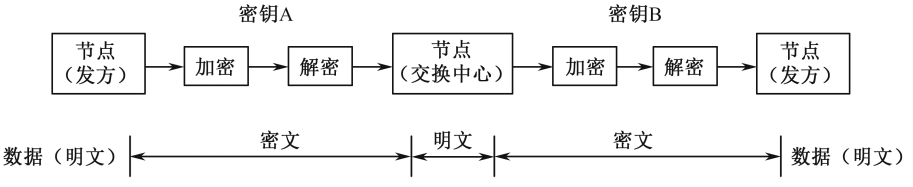


图 3.2 链路加密

尽管链路加密在计算机网络环境中使用相当普遍，但它并非没有问题。链路加密的不足表现为以下三个方面。

（1）通常用在点对点的同步或异步线路上。它要求先对链路两端的加密设备进行同步，这种频繁的同步，带来的后果是数据的丢失或重传。

（2）链路加密仅在通信链路上提供安全性。在一个网络节点上，信息以明文形式存在，因此信息在所有节点上的安全性是薄弱环节。所以，要求在每个中间节点上提供加密硬件设备和一个安全的物理环境，这需要较高的费用。

（3）在传统的加密算法中，用于解密信息的密钥与用于加密的密钥是相同的。该密钥必须被秘密保存，并按一定规则进行变化。这样，密钥分配在链路加密系统中就成了一个问题。因为每个节点都必须存储与其相连接的所有链路的加密密钥，这就需要对密钥进行物理传送或建立专用网络设施，而网络节点地理分布的广阔性使得这一过程变得复杂，同时增加了密钥连续分配时的费用。

2．节点加密

节点加密是链路加密的改进，一般在传输层进行。为了克服在节点中数据以明文显示的缺点，在中间节点里装有用于加密、解密的装置，由这个装置来完成一个密钥向另一个密钥的变换。

尽管节点加密能给网络数据提供较高的安全性，但它在操作方式上与链路加密是类似的。两者均在通信链路上为传输的信息提供安全性，都在中间节点先对信息进行解密，然后进行加密。与链路加密不同的是，节点加密不允许信息在网络节点以明文形式存在。它首先把收到的信息通过节点上的一个安全模块进行解密，然后在同一个安全模块中采用另一个不同的密钥进行加密。节点对节点的加密除了在保护装置里，在节点的其他地方都是以密文的形式出现的。节点加密过程如图 3.3 所示。

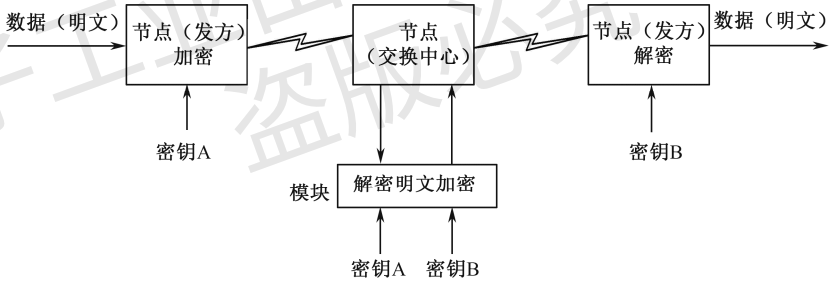


图 3.3　节点加密过程

节点加密要求报头和路由信息以明文形式传输，以便中间节点能得到如何处理节点的信息，因此这种方法给网络攻击者提供了可乘之机。

3．端到端加密

端到端加密也称面向协议加密、脱线加密或包加密，通常在应用层或表示层完成。端到端加密一般由软件来完成，允许数据在从源点到终点的传输过程中始终以密文形式存在。端到端加密过程如图 3.4 所示。采用端到端加密，在信息到达终点之前不进行解密，因为信息在整个传输过程中均受到保护，所以即使有节点被损坏也不会使信息泄露。端到端加密实际上是对整个网络系统采取保护措施。

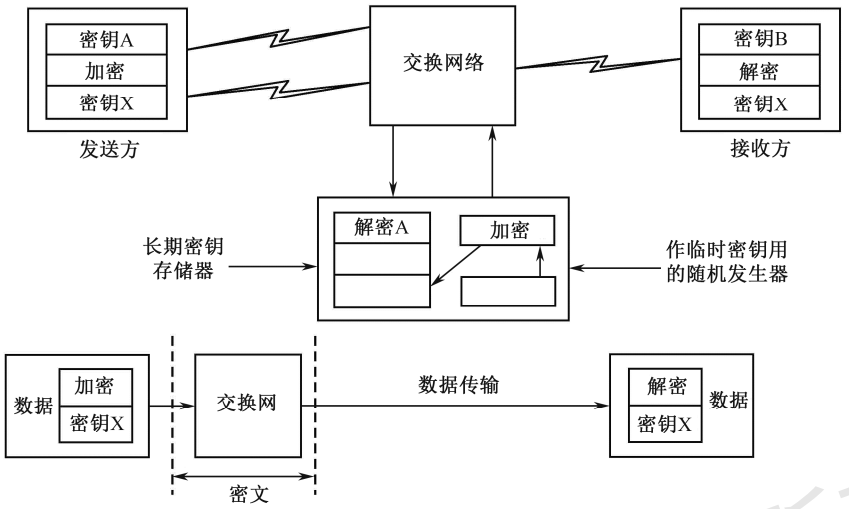


图 3.4　端到端加密过程

由于不需要在中间节点加密和解密，因此端到端加密系统的传输速度更快一些，价格便宜些，并且与链路加密和节点加密相比，更可靠，更容易设计、实现和维护。端到端加密还避免了其他加密系统所固有的同步问题，因为每个报文包均是独立被加密的，所以一个报文包所发生的传输错误不会影响后续的报文包。此方法只需要源和目的节点是保密的即可。

如节点对节点加密一样，端到端加密系统通常只加密报文，不加密报头，这是因为每个信息所经过的节点都要用此地址来确定如何传输信息。由于这种加密方法不能掩盖被传输信息的源点与终点，因此通信业务容易被发现。

端到端加密具有链路加密和节点加密所不具有的优点。

（1）成本低。端到端加密在中间任何节点上都不解密，即数据在到达目的地之前始终用密钥加密保护着，所以仅要求发送节点和最终的目标节点具有加密/解密设备，而链路加密则要求处理加密信息的每条链路均配有分立式密钥装置。

（2）端到端加密比链路加密更安全。

（3）端到端加密可以由用户提供，因此对用户来说该加密方式比较灵活。

3.2.2　加密中常用的数学运算

对称密码中有几种常用的数学运算，这些运算的共同目的就是把被加密的明文尽可能地打乱，从而加大破译的难度。

1．移位和循环移位

移位是指将一段数码按照规定的位数整体性地左移或右移。循环右移是指当右移时，把数码的最后的位移到数码的最前头，循环左移正相反。例如，对十进制数码 12345678 循

环右移 1 位（十进制）的结果为 81234567，而循环左移 1 位的结果则为 23456781。

2．置换

置换是指将数码中的某一位的值根据置换表的规定，用另一位代替。它不像移位操作那样整齐有序，看上去杂乱无章。这正是加密所需要的，经常被应用。

3．扩展

扩展是指将一段数码扩展成比原来位数更长的数码。扩展方法有多种，如可以用置换的方法，以扩展置换表来规定扩展后的数码每位的替代值。

4．压缩

压缩是指将一段数码压缩成比原来位数更短的数码。压缩方法有多种，如可以用置换的方法，来规定压缩后的数码每位的替代值。

5．异或

异或是一种二进制布尔代数运算。异或的数学符号为⊕，它的运算法则如下：

$$1 \oplus 1 = 0$$
$$0 \oplus 0 = 0$$
$$1 \oplus 0 = 1$$
$$0 \oplus 1 = 1$$

也可以简单地理解为，参与异或运算的两数位如相等，则结果为 0，不等则为 1。

6．迭代

迭代是指多次重复相同的运算，这在密码算法中经常使用，以使得形成的密文更加难以破解。

3.2.3　加密方法

1．替换密码法

替换密码法是用一组密文字母代替一组明文字母以隐蔽明文，但保持明文字母的位置不变的方法。在替换法加密体制中，使用了密钥字母表。常见的方法是恺撒密码法。

（1）恺撒密码。恺撒密码是最古老的替换密码。它是公元前 50 年罗马大将恺撒（Gaius Julius Caesar）使用过的密码。其加密方法是，把 A 换成 D，B 换成 E，C 换成 F……Z 换成 C，也称循环移位密码。这样，明文和密文的字母就建立了一对一的映射关系。恺撒密码的映射关系如下：

明文：A B C　D E F　G H I　J K L　M N O　P Q R　S T U　V W X　Y Z

密文：D E F　G H I　J K L　M N O　P Q R　S T U　V W X　Y Z A　B C

用恺撒密码进行加密，如果明文是 CAESAR，则密文是 FDHVDU。恺撒密码加密举例如图 3.5 所示。

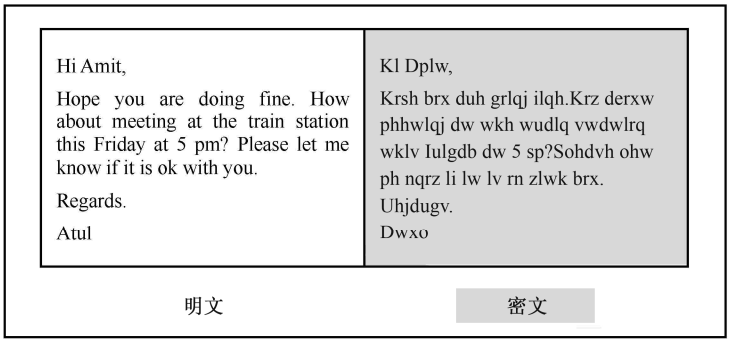


图 3.5　恺撒密码加密举例

（2）恺撒密码的简单改进。用数字 0,1,2,⋯,25 分别和字母 A,B,C,⋯,Z 相对应，则明文字母 P 和密文字母 C 的对应关系是 $C=(P+3) \bmod 26$。这个公式可以推广为 $C=(P+K) \bmod 26$。这里 $K \in S$，$S=\{1,2,\cdots,25\}$，K 是密钥集合，或称密钥空间。

在恺撒密码中，上式中的 K 为 3，因此它的密钥是 3。那么对于明文 P =COM，则密文的第一个字母为(2+3) mod 26=5=F，第二个字母为(14+3) mod 26=17=R，第三个字母为(12+3) mod 26=15=P，所以密文 C =FRP。

2．易位密码法

易位密码法的思想是重新排列明文字母，而排列序列由加密密钥确定。最简单的易位密码是将明文中的字母按顺序颠倒过来重新书写，如 THE CAR 变成 RAC EHT。

假设明文为：密码学的知识对于提高网络数据传输的安全性有着不可估量的作用。

采用易位密码的方法对明文加密，如图 3.6 所示。

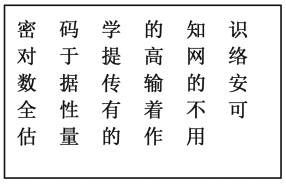


图 3.6　易位加密方法（例）

从左到右，按照列的顺序输出密文为：密对数全估码于据性量学提传有的的高输着作知网的不用识络安可。

上例中的加密方法也就是要介绍的另一种易位密码——列换位密码。该密码的密钥是一个单词或短语，其中不能包括重复字母。

假设，密钥为 HEARTILY，明文为 PLEASETRANSFERDOLLARSTOMYBANKA-

CCOUNTFOUR。

列换位密码方法的思想是首先将密钥转换为列的易位编号，选最小的字母作为第一列，次小的字母为第二列，以此类推。将明文按行水平书写，不全的行可用不常用的字母填满，如表 3.1 所示。

表 3.1　密钥-明文表

密　钥	H	E	A	R	T	I	L	Y
列编号	3	2	1	6	7	4	5	8
明文序列	P	L	E	A	S	E	T	R
	A	N	S	F	E	R	D	O
	L	L	A	R	S	T	O	M
	Y	B	A	N	K	A	C	C
	O	U	N	T	F	O	U	R

对于表中的排列顺序，密文按列的编号顺序由小到大输出，先输出第一列的所有字母（ESAAN），再输出第二列的字母（LNLBU），直到所有列的字母输出完为止，最后得到密文。

明文：PLEASETRANSFERDOLLARSTOMYBANKACCOUNTFOUR

密文：ESAANLNLBUPALYOERTAOTDOCUAFRNTSESKFROMCR

3．一次性加密法

所有密码体制中最值得注意的是一次性加密密码体制。在这种体制中，选择一个随机位串作为密钥，然后把明文信息转换为位串。将明文位串与密钥位串进行异或运算就得到密文位串。所有的密钥（$k_1,k_2,\cdots,k_n$）都是用随机的方法独立产生的，密钥的长度等于明文的长度，每个密钥只使用一次。解密过程为密文与密钥异或，得到明文。

例如，明文为 1101001100110001，密钥为 1110100101011010，进行异或后密文为 0011101001101011。

虽然这种密码看起来非常简单，但迄今为止，这是唯一达到理论不可破译的密码体制。但是，利用这种加密方法，大量的密钥必须通过安全通道在通信双方之间传递。密钥的安全存放及网络状态下密钥的建立和同步都比较困难。

3.2.4　密码算法

1．对称密码算法

对称密码算法又叫传统密码算法，是指加密密钥能够从解密密钥中推算出来，反过来也成立。在大多数对称算法中，加密和解密密钥是相同的。这些算法也叫私有密钥算法或单密钥算法，它要求发送者和接收者在安全通信之前，确定一个密钥。对称算法的安全性

依赖于密钥，泄露密钥就意味着任何人都能对消息进行加密、解密。只要通信需要保密，密钥就必须保密。

对称算法的加密和解密表示为：

$$E_K(M)=C$$

$$D_K(C)=M$$

此公式中，明文用 M 表示，密文用 C 表示，密钥用 K 表示。加密函数 E 使用密钥 K 作用于 M 得到密文 C；相反，解密函数 D 使用密钥 K 作用于 C 产生 M。

对称算法可分为两类：一类是一次只对明文中的单个比特（有时对字节）运算，这种算法称为序列算法或序列密码；另一类是对明文的一组比特进行运算，这些比特组称为分组，相应的算法称为分组算法或分组密码。计算机密码算法的典型分组长度为 64 比特——这个长度大到足以防止分析破译，但又小到足以方便使用（在计算机出现前，算法普遍地每次只对明文的一个字符运算，可认为是序列密码对字符序列的运算）。后来，随着破译能力的发展，分组长度又提高到 128 位或更长。

常用的采用对称密码技术的加密方案有五个组成部分。

（1）明文：原始信息。

（2）加密算法：以密钥为参数，对明文进行多种置换和转换的规则和步骤，变换结果为密文。

（3）密钥：加密与解密算法的参数，直接影响对明文进行变换的结果。

（4）密文：对明文进行变换的结果。

（5）解密算法：加密算法的逆变换，以密文为输入、密钥为参数，变换结果为明文。

图 3.7 是对称密码技术加密、解密的示意图。

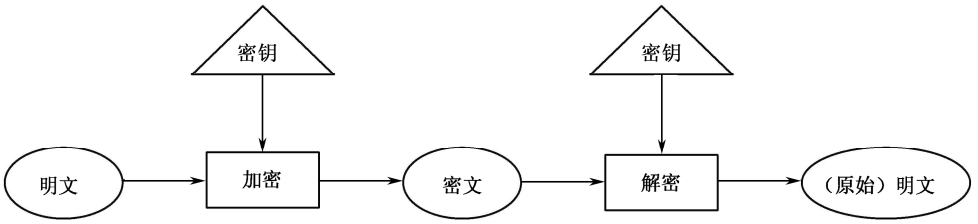


图 3.7　对称密码技术加密、解密示意图

典型的对称加密算法主要包括以下五种。

1）DES 算法

数据加密标准（Data Encryption Standard，DES）是由 IBM 公司研制的一种对称密码算法，美国国家标准局于 1977 年公布，并把它作为非机要部门使用的数据加密标准，四十年来，它一直活跃在国际保密通信的舞台上，扮演了十分重要的角色。

DES 是一个分组加密算法，典型的 DES 以 64 位为分组对数据加密，加密和解密用的

是同一个算法。它的密钥长度是 56 位（因为每个第 8 位都用作奇偶校验），密钥可以是任意的 56 位数，而且可以在任何时候改变。其中有极少数被认为是易破解的弱密钥，但是很容易避开它们不用。DES 算法的保密性依赖于密钥。

DES 加密过程如图 3.8 所示。

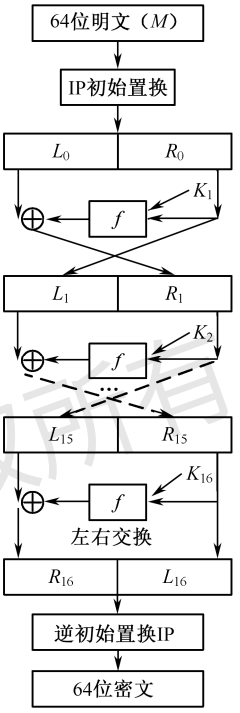


图 3.8　DES 加密过程

（1）要生成一套加密密钥，从用户处取得一个 64 位长的密码口令，然后通过等分、移位、选取和迭代形成一套 16 个加密密钥，分别供每轮运算中使用。

（2）DES 对 64 位（bit）的明文分组 M 进行操作，M 经过一个初始置换 IP，置换成 m_0。将 m_0 明文分成左半部分和右半部分：$m_0 = (L_0, R_0)$，各 32 位长。然后进行 16 轮完全相同的运算（迭代），这些运算被称为函数 f。在每轮运算过程中数据与相应的密钥结合。

（3）在每轮中，密钥位移位，然后从密钥的 56 位中选出 48 位。通过一个扩展置换将数据的右半部分扩展成 48 位，并通过一个异或操作替代成新的 48 位数据，再将其压缩置换成 32 位。这四步运算构成了函数 f。然后，通过另一个异或运算，函数 f 的输出与左半部分结合，其结果成为新的右半部分，原来的右半部分成为新的左半部分。将该操作重复 16 次。

（4）经过 16 轮迭代后，左、右半部分合在一起经过一个末置换（数据整理），这样就完成了加密过程。

图 3.8 中，$L_i = R_{i-1}$，$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$。

DES 的安全性首先取决于密钥的长度。密钥越长，破译者利用穷举法搜索密钥的难度就越大。根据当今计算机的处理速度和能力，56 位长度的密钥已经能够被破解，而 128 位的密钥则被认为是安全的，但随着时间的推移，这个数字也迟早会被突破。

另外，对 DES 算法进行某种变形和改进也是提高 DES 算法安全性的途径。例如，后来演变出的 3-DES 算法使用了三个独立密钥进行三重 DES 加密，这就比 DES 大大提高了安全性。因为如果 56 位 DES 用穷举搜索来破译需要 2∧56 次运算，3-DES 则需要 2∧112 次。又如，独立子密钥 DES 由于每轮都使用不同的子密钥，这意味着其密钥长度在 56 位的基础上扩大到 768 位。另外，DES 还有 DESX、CRYPT、GDES、RDES 等变形。这些变形和改进的目的都是加大破译难度及提高密码运算的效率。

2）IDEA 算法

国际数据加密算法（International Data Encryption Algorithm，IDEA）是由瑞士的 James Massey 和 Xuejia Lai 等人提出的加密算法，在密码学中属于数据块加密算法（Block Cipher）类。IDEA 使用长度为 128 位的密钥，数据块大小为 64 位。从理论上讲，IDEA 属于“强”

加密算法，至今还没有出现对该算法的有效攻击算法。

1990 年，Xuejia Lai 等人在 EuroCrypt'90 年会上提出了分组密码建议 PES（Proposed Encryption Standard）。在 EuroCrypt'91 年会上，Xuejia Lai 等人又提出了 PES 的修正版 IPES（Improved PES）。目前，IPES 已经商品化，并改名为 IDEA。IDEA 已由瑞士的 Ascom 公司注册专利，以商业目的使用 IDEA 算法必须向该公司申请许可。

3）FEAL 算法

FEAL（Fast Data Encipherment Algorithm）密码算法家族是日本 NTT（日本电报电话公司）设计的。密钥组位长度为 64 位，明、密文组位长度为 64 位。FEAL 是一套类似美国 DES 的分组加密算法。FEAL 着眼于当时的 DES 只用硬件去实现，不适用于较小的系统，FEAL 强调其在每轮的安全强度都比 DES 高，所以使用较少的轮数就可达到与 DES 采用 16 轮相同的安全度，如此一来，就比较适合用软件去实现。

从输入与输出的观点来看，FEAL 分组加密法与 DES 是相同的，即 FEAL 的加密或解密分组，以及使用者手中所持有的私有密钥皆如同 DES 一般，都是 64 位。唯一不同的是，FEAL 的密钥没有校验位。

至于 FEAL 加密算法的真正加密结构，则与 DES 有极大的差异。FEAL 完全没有使用置换函数来搅乱加密或解密过程中的数据，更不像 DES 一样具有神秘的 S 盒。FEAL 使用了异或（XOR）、旋转（Rotation）、加法与模（Modulus）运算。

4）LOKI 算法

LOKI 算法作为 DES 的一种潜在替代算法于 1990 年在密码学界首次亮相。 LOKI 同 DES 一样以 64 位二进制分组加密数据，也使用 64 位密钥（只是其中无奇偶校验位），所有 64 位均为密钥，迭代次数为 16。LOKI 密码公布之后，有关专家对其进行了研究破译并证明不大于 14 轮的 LOKI 算法极易受到差分密码分析的攻击。不过，这仍然优于 56 位密钥的 DES。

5）Khufu 和 Khafre 算法

1990 年由默克尔（Merhie）设计的 Khufu 和 Khafre 算法具有较长的密钥，适合于软件实现，比较可靠。Khufu 算法的总体设计同 DES，只是拥有 512 位（64 字节）的密钥。Khafre 算法与前者类似，预定用于不能预先计算的场合。由于 Khufu 算法具有可变的 S 盒，可以抵抗差分密码分析的攻击。

2．非对称密码算法

非对称密码算法（也叫公开密钥算法）是这样设计的：用作加密的密钥不同于用作解密的密钥，而且解密密钥不能根据加密密钥计算出来（至少在合理假定的长时间内）。之所以叫作公开密钥算法，是因为加密密钥能够公开，即陌生者能用加密密钥加密信息，但只有用相应的解密密钥才能解密信息。在这些系统中，加密密钥叫作公开密钥（简称公钥），

解密密钥叫作私有密钥（简称私钥）。私有密钥有时也叫私有密钥。为了避免与对称算法混淆，此处不用私有密钥这个名字。图 3.9 是非对称密码加密、解密的示意图。

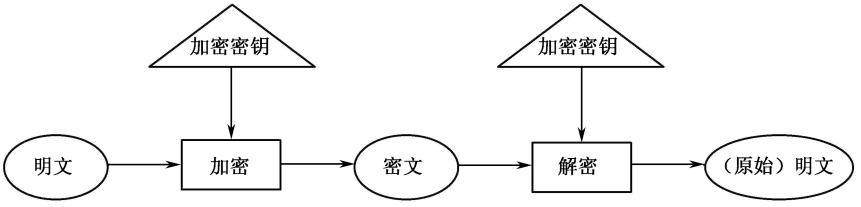


图 3.9　非对称密码加密、解密示意图

用于公钥加密的典型算法有 RSA、背包算法、Rabin 算法、概率加密算法、McEliece 算法等。下面以 RSA 为代表讲述非对称加密体系。

1）RSA 概述

传统的密码体系，需要对每位用户提供密钥，这就需要管理大量的密钥，包括密钥的产生、分发、使用和销毁等过程，并且密钥的传输需要借助于邮件和电话等其他相对不够安全的手段来进行。1976 年，美国学者 Whitfield Diffie 和 Martin Hellman 为解决信息公开传输和密钥管理问题，提出一种新的密钥交换协议，允许通信双方在不安全的媒体上交换信息，这就是“公钥密码体制”。相对于“对称密码算法”，这种方法也称“非对称密码算法”。

RSA 是由它的三个发明者，即 Rivest、Shamir 和 Adelman 的名字命名的。自从其发表以来，一直是众多密码分析员分析研究的对象，但是至今仍未找到任何缺陷。使用此算法的主要难点在于，要实现数百上千的指数运算，这在当时的计算机上是难以实现的。随着微电子技术和计算机技术的迅速发展，现在已生产出能有效实现 1 024 位 RSA 算法的硬件设备。这种密码算法在银行界和当今的电子商务领域得到了广泛应用。

2）RSA 的特点

公钥密码体制给使用者提供配对的两个密钥：一个用于加密；另一个用于解密。也就是说，使用公钥密码体制时，每个用户只需要具备两个相互匹配又相互独立的密钥，一个为公开密钥，另一个为私有密钥。公开密钥是不需要保密的，完全可以公开。需要保密的仅是私有密钥。公钥密码体制的实质，是使用一种安全方法加密，用另一种安全方法解密。例如，用公开密钥加密，而用私有密钥解密。因此，公开密钥的公开属性不会降低系统的安全性。

用公开密钥 K 加密表示为：

$$E_K(M)=C$$

虽然公开密钥和私有密钥是不同的，但用相应的私有密钥解密可表示为：

$$D_K(C)=M$$

有时消息用私有密钥加密而用公开密钥解密，这用于数字签名（后面将详细介绍），尽管可能产生混淆，但这些运算可分别表示为：

$$E_K(M)=C$$

$$D_K(C)=M$$

当前公开密码算法的速度，比起对称密码算法要慢得多，这使得公开密码算法在大数据量的加密中应用有限。

假如某用户的私有密钥为 K_{priv}，其相应的公开密钥为 K_{pub}。他人用其公开密钥对明文 P 进行加密后，将密文消息 E（K_{pub}, P）发给用户，该用户可用其私有密钥进行解密，获得原明文 P，即：

$$P=D[K_{\text{priv}}, E(K_{\text{pub}}, P)]$$

而且，该加密算法还允许该用户用私有密钥加密后的消息，他人只能使用相应的公开密钥才能解密，即：

$$P=D[K_{\text{pub}}, E(K_{\text{priv}}, P)]$$

上述两个性质说明，在公钥体制下，公开密钥及其相应的私有密钥，可以任意次序使用。也就是说，若他人用公开密钥对明文进行加密，则用户需要用相应的私有密钥进行解密；此外，用户也可以先使用私有密钥加密传递，然后他人使用相应的公开密钥对接收的密文进行解密。

在公钥密码体制中，他们将公开密钥提供给所有需要与自己交换消息的人，但必须将私有密钥严格保密。这样，采用公钥密码系统时，通信的双方无须事先交换密钥就可以建立起保密信道。RSA 算法的缺点是，运行速度较慢，效率低。因此，在实际的应用中通常不采用这一算法对信息量大的信息（如大的 EDI 交易）进行加密。对于加密量大的应用，公开密钥加密算法通常用于对称加密方法密钥的加密。

3）RSA 算法原理

RSA 算法基于大数的因子分解，数的位数越多因子分解越困难。大数因子分解问题是数学上的著名问题，RSA 算法自 1978 年公布至今，虽然对之进行了大量的密码分析，但仍然没有有效的方法予以破解，因此可以确保 RSA 算法的安全性。RSA 系统是公钥系统的最具有典型意义的方法，大多数使用公钥密码进行加密和数字签名的产品与标准使用的都是 RSA 算法。

公钥密码体制的思想并不复杂，而实现它的关键问题是如何确定公钥和私钥及加解密的算法，也就是说如何找到“锁和钥匙”的问题。假设在这种体制中，Pk 是公开信息，作为加密密钥，而 Sk 需要由用户自己保密，作为解密密钥，加密算法 E 和解密算法 D 也都是公开的。虽然 Pk 与 Sk 是成对出现的，但却不能根据 Pk 计算 Sk。它们必须满足以下条件：

（1）加密密钥 Pk 对明文 X 加密后，再用解密密钥 Sk 解密，即可恢复出明文，或写作

$D_{Sk}[E_{Pk}(X)]=X$。

（2）加密密钥不能用来解密，即 $D_{Pk}[E_{Sk}(X)]\neq X$。

（3）在计算机上可以容易地产生成对的 Pk 与 Sk。

（4）从已知的 Pk 实际上不可能推导出 Sk。

（5）加密和解密的运算可以对调，即 $E_{Pk}[D_{Sk}(X)]=X$。

从上述条件可以看出，公开密钥密码体制下，加密密钥不等于解密密钥。加密密钥可以对外公开，使任何用户都可将传送给此用户的信息用公开密钥加密发送，而该用户唯一保存的私有密钥是保密的，也只有它能将密文复原、解密。

虽然解密密钥理论上可由加密密钥推算出来，但实际上是不可能的，或者虽然能够推算出，但因为花费很长时间而成为不可行，所以将加密密钥公开也不会危害密钥的安全。从理论上讲，既然 Pk 与 Sk 是一对存在着相互关系的密钥，那么从其中一个推导出另一个就是很有可能的，如何找到一个合适的算法生成合适的 Pk 与 Sk，并且使得从 Pk 不可能推导出 Sk 是需要考虑的重点问题。为了解决这个问题，密码学家们参考了数学上的陷门单向函数。单向函数的加密函数比较容易计算，而计算其逆函数（解密函数）却很困难。为提高保密强度，RSA 密钥至少为 500 位长，一般推荐用 1 024 位。

该算法基于下面两个事实，其保证了 RSA 算法的安全有效性。

（1）已有确定的一个数是不是质数的快速算法。

（2）尚未找到确定一个合数的质因子的快速算法。

4）RSA 算法过程

找两素数 p 和 q；

取 $n=p\times q$；

取 $t=(p-1)\times(q-1)$；

取任何一个数 e，要求满足 e 取（$d*e$）%t==1。

这样最终得到三个数：n,d,e。

设消息为数 M［M 设 $c=(M**d)$ %n］，就得到了加密后的消息 c。

设 $m=(c**e)$%n，则 $m == M$，从而完成对 c 的解密。

注：**表示次方，上面两式中的 d 和 e 可以互换。

在对称加密中：

n,d 两个数构成公钥，可以告诉别人；

n,e 两个数构成私钥，e 自己保留，不让任何人知道。

给别人发送的信息使用 e 加密，只要别人能用 d 解开就证明信息是由你发送的，构成了签名机制。别人给你发送信息时使用 d 加密，这样只有拥有 e 的你能够对其解密。

RSA 的安全性在于对于一个大数 n，没有有效的方法能够将其分解，从而在已知 n,d 的情况下无法获得 e；同样，在已知 n,e 的情况下无法求得 d。

例题：

设两个质数 p=47，q=71，则

$n=p\times q=3\ 337$，

$(p-1)\times(q-1)=46\times70$；

随机选取 e，设 e=79，它与$(p-1)\times(q-1)=3\ 220$ 无公因子，则

$d=79-1\bmod 3\ 220=1\ 019$，

公开 e 和 n，将 d 保密，丢弃 p 和 q。

现在要加密消息 6882326879666683，步骤如下：

首先将其分成小的分组，在此例中，可取分组的长度为 3 位（n 为 4 位数）。

m 将分成以下 6 个分组：

m_1=688，

m_2=232，

m_3=687，

m_4=966，

m_5=668，

m_6=003。

第一分组加密为 $c_1=69979\bmod 3337=1\ 570$。

对随后的分组进行同样的操作后，产生加密后的密文：

c=1570275620912276242 3158。

解密消息时需要用解密密钥 d=1 019 进行相同的指数运算。第一分组解密为：

$m_1=15701019\bmod 3337=688$。

消息的其余部分可用同样的方法解密。

5）RSA 的安全性

RSA 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，因为无法证明破解 RSA 就一定需要做大数分解。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 是最明显的攻击方法。现在，人们已能分解 140 多个十进制位的大素数。因此，数 n 必须选得大一些，视具体适用情况而定。

6）RSA 的速度

由于 RSA 进行的都是大数计算，使得无论是软件实现 RSA 还是硬件实现 RSA，最快的情况也比 DES 慢上 100 倍。速度慢一直是 RSA 算法的缺陷。一般来说，RSA 算法只用于少量数据加密。

7）RSA 的优点

（1）密钥配发十分方便，用户的公用密钥可以像电话本那样公开，使用方便，每个用

户只需持有一对密钥即可实现与网络中任何一个用户的保密通信。

（2）RSA 加密原理基于单向函数，非法接受者利用公用函数不可能在有限时间内推算出私有密钥。

（3）RSA 在用户确认和实现数字签名方面优于现有的其他加密机制。

8）RSA 的缺点

RSA 的缺点主要是产生密钥很麻烦，受到素数产生技术的限制，因而难以做到一次一密。另外，RSA 分组长度太长，为保证安全性，n 至少也要 600 位以上，使运算代价很高，尤其是速度较慢，较 DES 算法慢几个数量级；而且，随着大数分解技术的发展，这个长度还在增加，不利于数字格式的标准化。

目前，SET（Secure Electronic Transaction）协议中要求 CA 认证中心采用 2 048 位长的密钥，其他实体使用 1 024 位的密钥。

3.2.5　密钥管理

1．基本概念

密钥管理是密码系统中的关键技术。密钥管理的任务是管理密钥从产生到销毁的全过程，包括系统初始化，以及密钥的产生、存储、备份、恢复、装入、分配、保护、更新、控制、丢失、吊销和销毁等。从网络应用来看，密钥一般分为以下几类：基本密钥、会话密钥、密钥加密密钥和主机密钥等。

1）基本密钥

基本密钥又称初始密钥，是由用户选定或由系统分配，可在较长时间内由一对用户专门使用的私有密钥，也称用户密钥。基本密钥既要安全，又要便于更换。基本密钥与会话密钥一起用于启动和控制密钥生成器，从而生成用于加密数据的密钥流。

2）会话密钥

会话密钥即两个通信终端用户在一次通话或交换数据时所用的密钥。当用于对传输的数据进行保护时称为数据加密密钥，而用于保护文件时称为文件密钥。会话密钥的作用是使人们不必太频繁地更换基本密钥，有利于密钥的安全和管理。这类密钥可由用户双方预先约定，也可由系统通过密钥建立协议动态地生成并赋予通信双方，它为通信双方专用，所以又称专用密钥。

3）密钥加密密钥

密钥加密密钥是用于对传送的会话或文件密钥进行加密时采用的密钥，也称次主密钥、辅助密钥或密钥传送密钥。每个节点都分配有一个这类密钥。为了安全，各节点的密钥加密密钥应该互不相同。每个节点都必须存储有关到其他各节点和本节点范围内各终端所用的密钥加密密钥，而各终端只需要一个与其节点交换会话密钥时所需要的密钥加密密钥，称为终端主密钥。

4）主机密钥

主机密钥是指对密钥加密密钥进行加密的密钥，存于主机处理器中。

几类密钥之间的关系如图 3.10 所示。

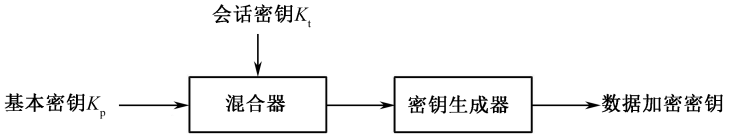


图 3.10　几类密钥之间的关系

密钥安全保密是密码系统安全的重要保证。保证密钥安全的基本原则是除了在有安全保证环境下进行密钥的产生、分配、装入及存入保密柜内备用外，密钥绝不能以明文的形式出现。密钥一般采用分级的保护管理办法，如图 3.11 所示。

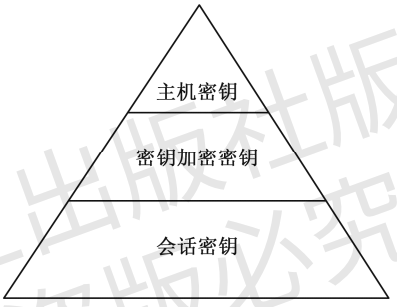


图 3.11　密钥的分级保护

2．基于对称算法的密钥管理

与公开密钥算法相比，对称算法具有运算速度快、占用资源少的优点，因此在很多计算或通信能力受限的系统中得到了广泛的应用。对称算法要求通信双方共享一个秘密作为加密密钥，因此对密钥的管理与交换更加困难。对称算法还经常应用于身份鉴别协议，在此过程中密钥管理也基于对称算法。

在传统的口令鉴别协议中，每个用户有一个与系统主机共享的身份标识和对应的口令。如果一个用户要登录系统，必须将他的身份标识及对应的口令发送给主机。主机搜索口令表，检验该身份标识与口令是否存在。如果存在，请求被接收，否则拒绝这个请求。这种方案不能抵抗重发攻击，显然是不安全的。一些改进的协议将主机上的口令表加密，但是仍然不能抵抗重发攻击。

对称密钥管理通过共同保守秘密来实现。通信双方必须使用相同的密钥，密钥的交换必须是安全可靠的，同时还要设定防止密钥被泄露或更改的程序。这样，对称密钥的管理和分发工作就变成了一个潜在的和烦琐的过程。密钥在通信各方分发和存储时都存在泄露的危险，一旦密钥泄露，其安全性便不再有保障。

通常对称密钥分发和存储的安全管理可借助于公开密钥密码体制。在分发时，首先用收方公开密钥加密该对称密钥，然后再传送给收方，因为只有收方才拥有用以解密的私有密钥，从而才能解密并安全地获得共享的对称密钥。对称密钥的存储可采用类似的方法，用户使用自己的公开密钥加密对称密钥，并进行存储，由于只有用户本身可以对该加密后的对称密钥解密，从而保证了对称密钥的安全。

3．公钥密钥管理

公钥密码体制密钥管理主要解决两个问题：一是私有密钥的保护；二是公开密钥及其所有者身份的确认。私有密钥由用户内部所采取的安全策略加以保护，一般用口令或存取权限等访问控制策略进行保护。公开密钥及其所有者身份的确认，目前一般根据 X.509 协议，由命名为身份认证机构（CA）的脱机可信实体来完成。CA 为每个用户颁发其签发的证书，证书中有该用户的公开密钥和该用户的身份信息，从而不同用户就可以通过交换证书来确认其公开密钥和身份。

在这种方式中，每个用户必须选定一个可信的 CA。与用户一样，每个 CA 也必须有一对公开密钥和私钥。用户与 CA 以下列方式交换公开密钥：彼此都相信收到的密钥的有效性和对方身份，然后 CA 用其私钥对包括 CA 名、用户名、用户的公开密钥及其有效期的数据集等进行数字签名，并将该签名附在上述数据集的后面，构成用户的证书。当用户分别使用不同的 CA 服务时，不同的 CA 要为其所属的每个用户建立一个证书，且各个 CA 之间要能够相互验证，只要保证每个 CA 都是可信赖的，用户之间公开密钥和身份的确认就可以得到保证。

公开密钥算法在身份认证、密钥协商及数字签名等方面有着天然的优势，基于这些特性已经提出了大量的协议用于解决安全问题，公开密钥算法无论是在理论上还是在实际应用中都得到了广泛的认可。在应用中，公开密钥算法所需要解决的一个关键问题是用户的公开密钥有效性的认证。因为这些信息是公开的，任何人都可以访问，所以有可能遭到恶意的替换、篡改等。要使得公开密钥算法得到应用，必须解决这些问题，公钥基础设施正是基于此而出现的一种技术。

当 A 要与 B 通信时，A 产生一对公钥、私钥对，并向 B 发送产生的公钥和 A 的身份。B 收到 A 的消息后，产生会话密钥 Ks，用 A 发送来的公钥加密后发送给 A。A 用私钥解密得到会话密钥 Ks。此时，A 和 B 可以用会话密钥 Ks 进行保密通信。A 销毁此次产生的公钥、私钥对，B 销毁从 A 那里得到的公钥。

公钥的分配方法有以下几种。

1）公开发布

用户将自己的公钥发给所有其他用户或向某一团体广播。例如，将自己的公钥附加在消息上，发送到公开的区域，如互联网的邮件列表。这种方法简单但有一个非常大的缺陷，

别人能很容易地伪造这种公开的发布信息。

2）公钥动态目录表

建立一个公用的公钥动态目录表，表的建立和维护及公钥的分布由某个公钥管理机构承担，每个用户都能可靠地知道管理机构的公钥。

4．密钥托管

密码技术可以用来保护合法的机密信息，也可能被非法用户用来逃避法律的打击，因此有必要为国家相关职能部门提供依法获得个人加密信息的渠道。密钥托管密码系统是具有备份解密能力的密码系统。它允许授权者在特定的条件下，借助于一个以上持有专用数据恢复密钥的、可信赖的委托方所提供的信息来解密密文。数据恢复密钥不同于通常的加解密密钥，但由它们可以恢复加解密密钥。

3.3 密码技术应用

3.3.1 概述

密码学的起源可能要追溯到人类刚刚出现，并且尝试去学习如何通信的时候，他们不得不去寻找方法确保他们通信的机密。但是最先有意识地使用一些技术方法来加密信息的可能是公元六年前的古希腊人，他们使用的是一根叫 scytale 的棍子，送信人先绕棍子卷一张纸条，然后把要加密的信息写在上面，接着打开纸送给收信人。如果不知道棍子的宽度（密匙）是不可能解密里面的内容的。后来，罗马的军队用恺撒密码进行通信。在随后的 19 个世纪里，主要是发明一些更加高明的加密技术，这些技术的安全性通常依赖于用户赋予它们多大的信任程度。

然而，密码学文献发展是一个很奇妙的过程。由于战争和各个国家之间的利益，密码学重要的进展很少在公开文献中出现。一直到 1918 年，20 世纪最有影响的密码分析文章之一——William F．Friedman 的专题论文 *The Index of Coincidence and it Application in Cryptography*（重合指数及其在密码学中的应用）问世。

第一次世界大战以后，情况开始变化，完全处于秘密工作状态的美国陆军和海军的机要部门在密码学方面取得了根本性的进展。但是由于战争的原因，公开的文件几乎没有。

从 1949 年到 1967 年，密码学文献几乎空白。在 1967 年，一部与众不同的著作——David Kahn 的 *The Code Breakers*（《破译者》）出现了，它并没有任何新的技术思想，但却对密码学的历史进行了相当完整的记述。这部著作的意义不仅在于它涉及了相当广泛的领域，而且也使成千上万的人了解了密码学。从此新的密码学文章开始源源不断地被发表。

在 20 世纪 70 年代后期和 80 年代初期，当公众在密码学方面的兴趣显示出来时，美国国家安全局（NSA），即美国官方密码机构曾多次试图平息它，但是结果与 NSA 的愿望大

相径庭，相反却为密码学的公开实践和专题研讨会做了许多意想不到的宣传。

历史车轮滚滚向前，密码学紧跟科学技术前进的步伐，经历了如下发展历程：密码学的初级形式——手工阶段；中间形式——机械阶段；高级形式——电子与计算机阶段。密码分析特别依赖数学方面的知识，现代密码学离开数学是不可想象的，密码学涉及数学的各个分支，如代数、数论、概率论、信息论、几何、组合学等。不仅如此，密码学的研究还需要具有其他学科的专业知识，如物理、电机工程、量子力学、计算机科学、电子学、系统工程、语言学等。反过来，密码学的研究也促进了上述各学科的发展。

计算机的出现大大促进了密码学的变革。由于商业应用和大量计算机网络通信的需要，民间对数据保护、数据传输的安全性、防止工业谍报活动等课题越来越重视，密码学的发展从此进入了一个崭新的阶段，与此同时，密码学的研究开始大规模地扩展到民用。

随着计算机网络不断渗透到各个领域，密码学的应用也随之扩大。其主要的应用集中在网络安全领域中，这是密码学应用的最主要的方面，也是密码学研究成为热点的主要原因之一。众所周知，互联网具有固有的安全弱点，因此网络安全面临诸多威胁，熟知的有计算机病毒、黑客入侵、机密文件泄露、DoS（拒绝服务攻击）、DDoS（分布式拒绝服务攻击）等。信息化和网络化是当今世界经济和社会发展的大趋势，但是在世界范围内，对计算机网络的攻击手段层出不穷，网络犯罪日益严重，而密码学的应用是进一步保护公民隐私和国家安全的需要，因此可以预见，随着信息化的发展，密码学的发展和应用将会越来越广泛和深入。

3.3.2　密码技术应用于电子商务

密码技术应用于电子商务的最大特点就是顾客可以在网上进行支付，而不必担心自己的信用卡被人盗用。在过去，用户的信用卡号码和终止日期可能会被窃贼得到，随后窃贼就可以通过电话订货，而且使用用户的信用卡进行付款，这种高风险性长期阻碍了电子商务的发展，于是人们开始用 RSA 技术提高信用卡交易的安全性，从而促进了电子商务的发展。

互联网、电子商务的发展，促进了金融服务形式的创新，网上银行就是这种创新的具体应用之一。如今人们只需通过一台联网的计算机，便可享受到许多理财服务，如查询、代收费、转账、挂失、咨询、投诉等。然而，网络的开放性与共享性也导致了网络的安全性受到严重影响，如何保证网上数据的安全和交易对方的身份确认无误是网上银行能否得以推广的关键。可以说，网上银行最关键的问题就是安全问题。密码技术的发展和应用，有助于解决网上银行安全问题，对保证交易信息安全是必不可少的。下面主要讲解安全电子商务交易中的密码技术应用。

1．每个用户只有一对密钥对——签名密钥对的情形

假定用户 A 和用户 B 进行交易，用户 A 拥有一对签名密钥对 Kva（公钥）、Ksa（私

钥）。用户 B 拥有一对签名密钥对 Kvb（公钥）、Ksb（私钥）。当用户 A 欲将秘密信息（如支付信息）传送给用户 B 时，用户 B 收到信息后的操作过程如下。

（1）用自己的私钥 Ksb 解密本次通信的数据加密密钥（对称密钥）。

（2）用对称密钥解开本次通信的数据信息。

（3）验证用户 A 的证书合法性。

（4）将本次通信的数据信息内容按照规定的 Hash 算法做杂凑处理。

（5）用用户 A 证书中的公钥，对用户 A 的 Hash 私钥签名做解密运算。

（6）将（4）与（5）的结果进行比对，若相等，则本次通信成功。

2．每个用户拥有两对密钥对的情形

这种情况会与上面略有不同：用户 A 除了拥有一对签名密钥对 Kva（公钥）、Ksa（私钥）以外，还有一对加密密钥对 Kea（公钥）、Kda（私钥）；用户 B 除有一对签名密钥对 Kvb（公钥）、Ksb（私钥）外，还拥有一对加密密钥对 Keb（公钥）、Kdb（私钥）。当用户 A 欲将秘密信息（如资金信息）传送给用户 B 时，用户 A 将信息流发给用户 B。此时用户 B 收到信息后的操作过程与上一种情形的不同之处在于：用户 B 须先用自己的加密私钥 Kdb 解开此次通信的数据加密密钥。后续步骤与上面的（2）～（6）相同。

一般的电子商务应用软件在通信会话时都采用分组密码算法（可选用不同的工作模式），如 DES、三重 DES、RC2、RC4、IDEA 等。密钥长度在标准的 SET 系统中为 56 位，其他非标准系统中根据信息的安全等级不同可选多种长度。密钥的产生和使用为一次一密。非对称密码算法多见于 RSA、DSA 等，其模长一般在 1 024 位或以上。

3.3.3 密码技术应用于虚拟专用网

虚拟专用网被定义为通过一个公用网络（通常是互联网）建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全、稳定的隧道。虚拟专用网是对企业内部网的扩展。

虚拟专用网可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的内部网建立可信的安全连接，并保证数据的安全传输。通过将数据流转移到低成本的网络上，一个企业的虚拟专用网解决方案将大幅度地减少用户花费在城域网和远程网络连接上的费用。同时，这将简化网络的设计和管理，加速连接新的用户和网站。另外，虚拟专用网还可以保护现有的网络投资。随着用户的商业服务不断发展，企业的虚拟专用网解决方案可以使用户将精力集中到自己的生意上，而不是网络上。虚拟专用网可用于不断增长的移动用户的全球互联网接入，以实现安全连接；可用于实现企业网站之间安全通信的虚拟专用线路，以经济有效地连接到商业伙伴和用户的安全网络。

虚拟专用网的结构如图 3.12 所示。

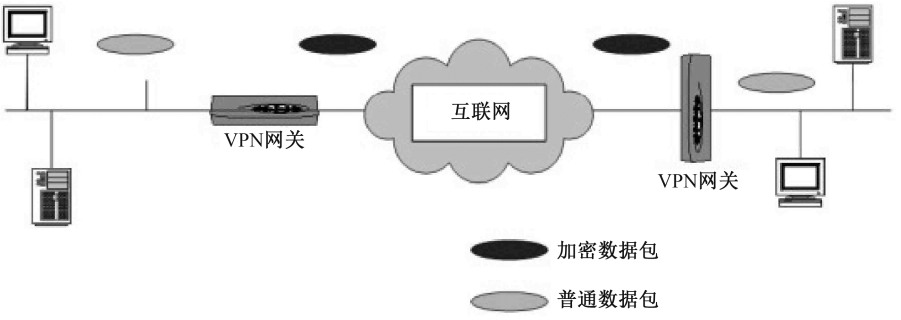


图 3.12　虚拟专用网的结构

要通过互联网建立虚拟专用网，不仅只是对两端传送的数据进行加密，以保证通过公网传输的信息即使被他人截获也不会泄露，还需要对用户的身份进行认证，来保证信息的完整性、合法性，并鉴别用户的身份。虚拟专用网还需要建立访问控制能力，只有合法用户才能访问内部网，不同用户的访问权限也会不一样。

3.4　电子商务加密技术综合应用——数字签名

3.4.1　数字签名技术简介

目前，电子支付、网上银行等电子商务服务在银行业务中所占比重加大，越来越多的客户借助计算机网络交换资金信息。因此保证网络上传递资金信息的安全，防止非法窃取和篡改，成为银行网络信息化建设的重要基础。计算机加密技术的使用为银行业务发展提供了安全保障。

传统的银行业务是通过票据上的印章或签名来辨别真伪的，电子数据是通过数字签名技术来解决这一问题的。签名和验证过程是这样的：发送方首先用公开的单向散列函数对信息进行一次变换，得到散列值，然后用私有密钥对散列值加密，得到一个数字标签，即数字签名，附于信息之后一同发出；接收方用发送方的公开密钥对数字签名进行解密，得到散列值的明文，再将得到的信息通过同一单向散列函数进行计算，同样得到一个散列值。比较两个散列值，如果相同，则证明签名有效，否则无效。其中发送方的公钥是由一个可信赖的技术管理机构即身份认证机构（CA）发布的。

为了鉴别文件的真伪，传统的做法是相关人员在文件上亲笔签名或盖印章。签名起到认证、核实、生效的作用。在计算机应用中，结合 Hash 函数和非对称加密算法，可以实现数字签名（Digital Signature）。数字签名是对信息发送者的身份进行辨识的重要手段，同时也是保证信息在传输过程中的完整性的必要手段。数字签名技术普遍用于银行、电子贸

易等。它主要应对以下安全问题。

（1）否认：事后发送者不承认文件是他发送的。

（2）伪造：有人自己伪造了一份，却声称是某人发送给自己的。

（3）冒充：冒充别人的身份在网上发送文件。

（4）篡改：接收者私自篡改文件的内容。

数字签名机制具有可证实性、不可抵赖性、不可伪造性、不可重用性和不可改变性。

数字签名满足了以下要求。

（1）签名是可信的。接收方用发送方的公开密钥验证时，他知道是由发送方签名的。

（2）签名是不可伪造的。只有发送方知道他的私有密钥。

（3）签名是不可重用的。签名是信息的一一对应函数。

（4）被签名的信息是不可改变的。如果信息有任何改变，信息就不可能用发送方的公开密钥进行验证。

（5）签名是不可抵赖的。接收方不用发送方的帮助就能验证发送方的签名。

数字签名算法包括签名算法和验证算法两种算法。各种密码算法都可用于数字签名，因此可有大量的数字签名算法，如 DES 数字签名算法、RSA 数字签名算法。

3.4.2 数字签名的实现方法

实现数字签名有很多方法，目前数字签名采用较多的是公钥加密技术，如基于 RSA Date Security 公司的 PKCS（Public Key Cryptography Standards）、Digital Signature Algorithm、X.509 等。1994 年，美国标准与技术协会公布了数字签名标准（DSS），使公钥加密技术得到了广泛应用。公钥加密系统采用的是非对称加密算法。

1．用非对称加密算法进行数字签名

1）算法的含义

此算法使用公开密钥和私有密钥，分别用于对数据的加密和解密，即如果用公开密钥对数据进行加密，只有用对应的私有密钥才能进行解密；如果用私有密钥对数据进行加密，则只有用对应的公开密钥才能解密。

2）签名和验证过程

（1）发送方首先用公开的单向函数对报文进行一次变换，得到数字签名，然后利用私有密钥对数字签名进行加密后附在报文之后一同发出。

（2）接收方用发送方的公开密钥对数字签名进行解密变换，得到一个数字签名的明文。发送方的公钥是由一个可信赖的技术管理机构即认证机构（CA）发布的。

（3）接收方将得到的明文通过单向函数进行计算，同样得到一个数字签名，再将两个数字签名进行对比，如果相同，则证明签名有效，否则无效。

这种方法使任何拥有发送方公开密钥的人都可以验证数字签名的正确性。由于发送方私有密钥的保密性，使得接收方既可以根据验证结果来拒收该报文，也能使他人无法伪造报文签名或对报文进行修改，原因是数字签名是对整个报文进行的，是一组代表报文特征的定长代码，同一个人对不同的报文将产生不同的数字签名。这就解决了银行通过网络传送一张支票，而接收方可能对支票数额进行改动的问题，也避免了发送方逃避责任的可能性。

2．用对称加密算法进行数字签名

1）算法的含义

对称加密算法所用的加密密钥和解密密钥通常是相同的，即使不同也可以很容易地由其中的任意一个推导出另一个。在此算法中，加、解密双方所用的密钥都要保守秘密。由于该类算法计算速度快而被广泛应用于对大量数据如文件的加密过程中，如 RD4 和 DES。

2）签名和验证过程

Lamport 发明了称为 Lamport-Diffie 的对称加密算法：利用一组长度是报文的比特数（n）两倍的密钥 A 来产生对签名的验证信息，即随机选择 $2n$ 个数 B，由签名密钥对这 $2n$ 个数 B 进行一次加密变换，得到另一组 $2n$ 个数 C。

（1）发送方从报文分组 M 的第一位开始，依次检查 M 的第 i 位，若为 0 则取密钥 A 的第 i 位，若为 1 则取密钥 A 的第 i+1 位；直至报文全部检查完毕。所选取的 n 个密钥位形成了最后的签名。

（2）接收方对签名进行验证时，也是首先从第一位开始依次检查报文 M。如果 M 的第 i 位为 0，就认为签名中的第Ⅰ组信息是密钥 A 的第 i 位，若为 1 则为密钥 A 的第 i+1 位；直至报文全部验证完毕后就得到了 n 个密钥。由于接收方具有发送方的验证信息 C，所以可以利用得到的 n 个密钥检验验证信息，从而确认报文是否是由发送方所发送。

由于这种方法是逐位进行签名的，只要有一位被改动过，接收方就得不到正确的数字签名，因此其安全性较好，其缺点是签名太长，签名密钥及相应的验证信息不能重复使用，否则极不安全。

3．认证产品

认证产品可分为两大类：一是用户认证，主要是通过单独签名访问网络资源；二是对象认证，即判定传递信息和文件的认证及其真实性。数字签名技术主要用于信息、文件及其他存储在网上的传输对象的认证。AT&T Government Market 的 Secret Agent 便通过将数字签发的文档作为 E-mail 消息的文件附件的形式，将现有客户机运行环境中 E-mail 系统、Web 浏览器等应用密切地结合在一起；Regnoc Software 的 Signature 使用 OLE 2.0 可对 Windows 下的任何文本做数字签名；ViaCrypt 的 ViaCrypt PGP 可从传递信息的应用中切割文本至 Windows 或 Macintosh 裁剪板，在那里对它进行数字签名后将它粘贴到传递信息中。其对于电子商务的一个功能是：能破译雇员发送或接收的所有密文，可设置成在公司密钥下

自动破译所有外发信息，且要求雇员须使用职权范围允许的解密密钥。

3.4.3 数字签名的算法及数字签名的保密性

数字签名的算法很多，应用最为广泛的是 Hash 签名、DES 签名、DSS 签名和 RSA 签名。

1．Hash 签名

Hash 签名不属于强计算密集型算法，应用较广泛。很多少量现金付款系统，如 DEC 的 Millicent 和 CyberCash 的 CyberCoin 等都使用 Hash 签名。使用较快的 Hash 算法，可以降低服务器资源的消耗，减轻中央服务器的负荷。Hash 的主要局限是接收方必须持有用户密钥的副本以检验签名，因为双方都知道生成签名的密钥，较容易攻破，存在伪造签名的可能。如果中央或用户计算机中有一个被攻破，那么其安全性就受到了威胁。

2．DES 签名

DES 用于数字签名就像 DES 算法一样，加密和解密使用同一密钥，密钥必须是严格保密的。使用这种密码系统时，密钥的保密性不仅能保证消息的保密性，还能保证消息的真实性。

例如，信息的发送方和信息的接收方共享一个共同的密钥［如客户（S）和银行（R）是通信双方］，S 就可将其转账请求信息经过加密后发送给 R。由于除 S 外无其他人知道 S 的密钥，因此，R 可以确认此信息的真实性。但是，对称密钥不能防止伪造信息。由于 R 也知道该密钥，银行就有可能创建同 S 发出的相同的转账信息。为避免这种情况，采用对称密钥时，就需要一个仲裁方（A）来防止伪造信息。

假设：发送方 S 和仲裁方 A 有相同的密钥 Ks，而接收方 R 和仲裁方 A 有相同的密钥 Kr。S 和 R 已事先约好了统一的数字签名的格式，S 要发送信息给 R，要求消息具有不可伪造性和真实性两个特点。

在电子银行的环境里，这里的仲裁方实际上就是各级交换中心。交换中心作为仲裁方，必须是通信各方可信赖的、公正的第三方。因此，这种数字签名可用于银行专用网内的数字通信，以保证网络中传输消息的安全性。

3．DSS 和 RSA 签名

DSS 和 RSA 都采用了公钥算法，不存在 Hash 的局限性。DSS 是由美国国家标准化研究院和国家安全局共同开发的。由于它是由美国政府颁布实施的，主要用于与美国政府做生意的公司，其他公司则较少使用，它只是一个签名系统。RSA 是最流行的一种加密标准，许多产品的内核中都有 RSA 的软件和类库，早在 Web 飞速发展之前，RSA 数据安全公司就负责数字签名软件与 Macintosh 操作系统的集成，在 Apple 的协作软件 PowerTalk 上还增

加了签名拖放功能，用户只要把需要加密的数据拖到相应的图标上，就可完成电子形式的数字签名。RSA 与微软、IBM、Sun 和 Digital 都签订了许可协议，在几大公司的生产线上都加入了类似的签名特性。与 DSS 不同，RSA 既可以用来加密数据，也可以用于身份认证。和 Hash 签名相比，在公钥系统中，由于生成签名的密钥只存储于用户的计算机中，安全系数也更大一些。

数字签名的保密性在很大程度上依赖于公开密钥。数字认证是基于安全标准、协议和密码技术的电子证书，用以确立一个人或服务器的身份，它把一对用于信息加密和签名的电子密钥捆绑在一起，保证了这对密钥真正属于指定的个人和机构。数字认证由验证机构 CA 进行电子化发布或撤销公钥验证，信息接收方可以从 CA 的 Web 站点上下载发送方的验证信息。VeriSign 是第一家 X.509 公开密钥的商业化发布机构，在它的 Digital ID 下可以生成、管理应用于其他厂商的数字签名的公开密钥验证。

在实际应用中，为了防止把签名和签名信息一起重用，数字签名经常包括时间标记。把日期和时间的签名附在信息中，并和信息中的其他部分一起签名。

案例分析题

杭州的李先生反映，2018 年 7 月自己的银行卡五分钟之内被人盗刷了三十多万元，令人好奇的是银行卡就在李先生自己的身上。据李先生说，事发时，自己在公司的沙发上坐着，突然手机收到了两条银行的消费短信，一笔是二十多万元，一笔是十多万元，李先生经过查询得知这两笔钱是在泰国消费的，李先生以为是自己的卡丢了，于是立马就打开钱包查看，发现卡还在自己的包里，现在自己的卡里只剩下 20 多元钱。

实际上，这绝非个案。在北京、广东、江苏等经济发达地区，同类受害者数量达到上万人。在网上支付带给人们便利，并逐渐“飞进寻常百姓家”的同时，它的种种隐患同样暴露得十分彻底。

问题：

本案例是关于支付过程的安全问题，用户可以采取哪些措施来保证自己的支付安全呢？

自测题

一、判断题

1．对称密码体制也称双钥密码体制或公钥密码体制。（　　）

2．端到端加密具有链路加密和节点加密所不具有的优点：成本低，更安全、灵活。（　　）

3．DES 是数据加密标准的缩写，它是由惠普公司研制的一种对称加密算法。（　　）

4．公开密钥算法的设计是：加密的密钥和解密的密钥都是公开可以得到的。（　　）

5．虚拟专用网（VPN）就是互联网。（　　）

二、单选题

1．目前主要流行三种数据加密方式：链路加密、（　　）和端到端加密。

A．多码加密　　B．换位加密

C．节点加密　　D．仿射加密

2．（　　）是最古老的替换密码。

A．恺撒密码　　B．维热纳尔密码

C．维吉尼亚密码　　D．四方密码

3．IDEA 算法的中文名是（　　）。

A．公开密钥算法　　B．国际数据加密算法

C．数据加密标准　　D．对称算法

4．下列不属于数字签名的算法是（　　）。

A．Hash　　B．DES

C．AKO　　D．DSS 和 RSA

三、简答题

1．简述双向认证协议的实现过程。

2．简述链路加密、节点加密和端到端加密三种加密方式的特点。

3．已知明文是 1101001101110001，密码是 0101111110100110，试用一次性密码加密方法写出加密和解密过程。

4．密钥管理的目的是什么？密钥管理通常涉及的有关问题有哪些？

实训题

在淘宝网（www.taobao.com）申请自己的账号，并保管好自己的密码，尝试利用这个账号进行一次网上购物。

步骤一：登录淘宝网，在网页的左上角单击“免费注册”按钮。

步骤二：注册后会出现一个注册协议，接受就单击“同意协议”按钮，如图 3.13 所示。

步骤三：填写手机号，完成验证后单击“下一步”按钮，如图 3.14 所示。

图 3.13　同意协议

图 3.14　手机号注册

步骤四：填写手机短信接收到的校验码，单击“确认”按钮，如图 3.15 所示。

图 3.15　输入手机校验码

步骤五：设置登录名和密码，密码两次输入需要一致，登录名必须和别人不一样才能提交成功，如图 3.16 所示。

图 3.16　设置登录名和密码

步骤六：设置支付方式，也可以单击“跳过，到下一步”按钮，如图 3.17 所示。

图 3.17　设置支付方式

步骤七：注册完成，如图 3.18 所示。

图 3.18　注册完成

思考：如何开设淘宝店铺？