第5章　安全和鉴别

随着计算机、互联网和通信的应用范围不断扩大，各种各样的攻击性犯罪现象已经出现，而且有增长的趋势，因此安全和保密性显得日益重要。本章重点介绍智能卡和互联网目前采用的一些安全保证措施，如身份鉴别技术、报文鉴别技术、数字签名技术，以及防火墙和防病毒技术。采用这些安全技术用以保证在开放的网络中数据传输、交换和存储的安全性。

5.1　身份认证

随着不同领域对身份认证安全程度的不同，采用了各种各样的认证方式。例如，在电子商务和金融领域往往采用“凭证＋密码”的方法，来确定客户或持卡人的身份。某些领域已引入生物特征识别技术。

5.1.1　凭证＋密码

1. 证件＋密码

例如，将金融卡插入 ATM 机，持卡人输入密码，若正确，说明持卡人是此卡的主人，允许继续操作，完成取钱、存钱或其他目的。如果输入的密码不正确，可以重新输入 3 次（或其他次数），若每次都不正确，则将卡的功能锁住。通过指定的解锁方法后，此卡才能继续使用。其缺点是经常输入密码，可给不法分子造成偷看、窃取、监听和欺诈的机会。

2. 短信密码

服务方通过互联网接收用户的登录申请，用户方输入用户名、密码、手机号，并满足应用的条件后服务方接受登录。以后当用户提出应用请求时，服务方验证同意后向用户手机发送短信密码（随机码，一般是 6 位数字），用户输入上述随机码后，即可进入应用服务过程。由于互联网与用户手中的手机配合工作，且随机码保留的时间很短，一次有效，从而提高了安全性。

移动互联网已开拓了移动支付的应用功能，可作为网上银行、第三方支付和电子商务交易的凭证，因此在很多场合都由电子凭证替代了纸质凭证。

3. USB Key

USB Key 是可插入计算机 USB 接口的模块。它内置单片机或智能卡芯片，可存储用户的数字证书和密码。并在 USB Key 和服务器中存放证明用户身份的密钥。当需要在网络上验证用户身份时，先由用户向服务器发出一个验证请求，然后服务器生成随机数给 USB Key。双方（服务器和 USB Key）各自通过“单向散列算法”得到运算结果，并在服务器进行比较，如果相等，则认为接到 USB 接口的 USB Key 是一个合法用户，然后可完成相应的服务。

5.1.2 生物特征识别

生物特征识别主要是通过可测量的人体或行为等生物特征进行身份认证。人体特征包含人脸、指纹、静脉、虹膜等，行为特征有签名、语音等。

生物特征识别有以下特点。

(1) 随身性。与人体绑定。

(2) 唯一性。每个人拥有不同的生物特征。

(3) 可采集性。选择的生物特征易于测量，且人们愿意接受。

1. 指纹识别

指纹是指长在人的手指指尖到第一个关节之间的表皮纹线，所有人的每一个手指指纹都不相同，具有唯一性，如果没有意外事件，可终身不变。指纹可分为左旋、右旋、螺旋、双螺旋、拱形、尖拱等类型，通过统计，前面 4 种是常见的。在此基础上再进行精细点的分析，称之为指纹的细节点。指纹的细节点包含多种类型，常用的是指纹脊线的终结点和分叉点，是一些带方向的点的集合。细节点具有稳定的特点和极高的识别率。一幅指纹图像包含约 50 个细节点。图 5.1 所示为右旋型指纹的注册过程；图 5.2 所示为脊线的终结点和分叉点，脊线是有一定密度和走向的黑式纹线，纹线之间的凹陷部分(白色)称为谷线。

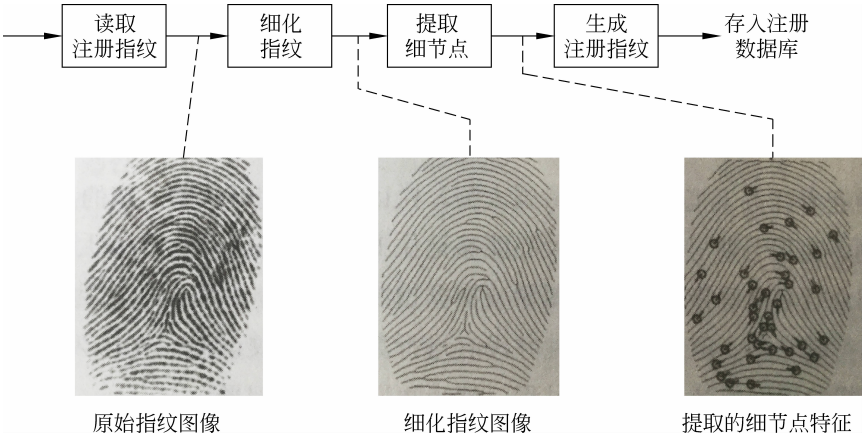


图 5.1 指纹注册过程

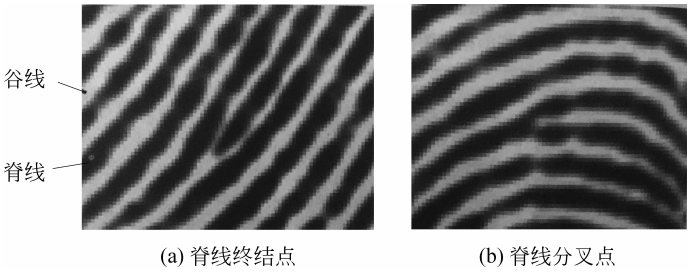


图 5.2 两类指纹细节点特征

1）指纹识别过程

（1）注册阶段。利用指纹采集仪（传感器）采集用户的指纹，转换成计算机可以处理的数字指纹图像，为了安全起见，可采集两个以上手指的指纹图像。通常采集到的指纹图像中有噪声，如果指纹采集仪认为指纹图像质量较差，可以提示用户再次输入指纹。

然后对指纹图像进行处理，得到细化的图像，从中提取细节点，生成注册指纹，存入指纹数据库。

（2）指纹识别认证。识别用户身份，现场采集用户的指纹图像进行处理（处理过程与注册阶段相同），并与注册阶段获得的指纹进行比对。

在采集用户指纹图像时，可能使用了与注册时不同类型的指纹采集仪，而且手指放置的位置有平移、旋转和形变等情况，使得两幅指纹的“细节点”不在同一坐标系中，因此需对图像进行匹配，指纹识别系统可以达到很高的识别率。图 5.3 所示为识别指纹过程。

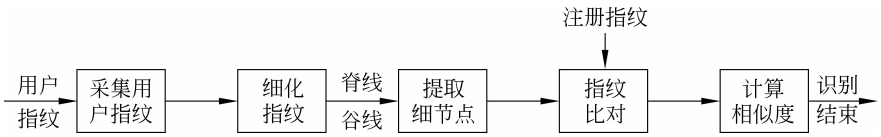


图 5.3　识别指纹过程

2）指纹图像的种类

（1）平板指纹。手指在采集仪上垂直按下再抬起，从而采集到手指中央区域的纹理信息（即纹线）。

（2）滚动指纹。手指按下后再左右滚动手指，从而采集到完整的指纹纹理信息。

（3）识别指纹。用户识别时按下的指纹。

2. 生物识别技术在社保应用

（1）指纹识别。价廉易用，应用较广泛。现场使用时，在指纹识别仪上留下指纹，要防止仿制。

（2）人脸识别。每个人的身份证上都有照片，无须另外采集和存储照片，有互联网的地方可通过计算机＋摄像头或手机终端完成自动认证。对光线和环境要求高，容易受浓妆、眼睛、表情的影响，存在双胞胎的误率、昂贵的设备费用和较慢的识别速度等缺点。

（3）声音识别（说话人识别）。无时间、地点、设备限制，但难以辨别简短的声音，识别时间比其他生物识别长，在生病时采集的声音与标本存在较大差异。

（4）静脉识别。静脉识别包括手掌、手指、手背静脉识别，一两秒即可完成，但设备较贵。

（5）虹膜、视网膜识别。通过近似红外线对眼睛扫描，虹膜是瞳孔周围的环状颜色组织，视网膜是位于眼球后部十分细小的神经。采集设备昂贵，而且需贴近设备进行扫描，

被测人接受度较低，很少使用。

3. 手写签名

手写签名作为一种身份鉴别方法已有较长的历史了。例如，签订合同、签署协议时都需要有相应负责人的签字，因为每个人签名时书写所用力度、笔迹特点等都是不一样的，根据这些特征就能够识别出签名人。手写签名识别的过程如下。

预先存储使用者真实签名样本，然后使用者通过触摸屏或手写板等输入签名到计算机，将手写签名的图像、笔顺、速度和压力等信息与真实签名样本进行比对，对所采集签名的数据信息进行预处理。合并和去除独立点和冗余点，进行平滑和倾斜校正等。接着提取特征信息，与真实签名样本进行以下对比。

(1) 签名的整体倾斜角度。

(2) 签名的宽高比。

(3) 签名笔迹长度。

(4) 签名落笔的总时间，签名提笔的总时间。

(5) 笔迹的压力变化。

(6) 笔迹形状的变化。

5.2 智能卡与互联网的通信安全与保密

智能卡必须与别的设备(或者是读写设备，或者是银行主机等)进行通信。同时，也由于智能卡自身已具备了存储及计算的能力，完全可以将它看作是一台袖珍型的计算机，因此它也在卡类系统中提供了端到端的安全控制。

一般而言，在通信方面对信息的篡改和攻击有以下方式。

(1) 对信息内容进行窃取、更改、删除、添加。

(2) 改变信息的源点或目的点，以窃取钱财。

(3) 窃取密码或推导出密码。

(4) 篡改回执。

从安全的角度考虑，就是要针对以上的这些攻击手段采取适当的技术防范措施，以求达到保证智能卡与外部设备进行信息交换过程的有效性与合法性的目的。具体而言，即是要保证该交换过程的完整性(integrity)、真实性(authenticity)、有效性(validity)和保密性(privacy)。这里，完整性是指智能卡及系统必须能检测出在它们之间交换的信息是否已经被修改了，无论这种修改是无意的还是蓄意的；有效性是指卡和系统能把真正合法的信息与一个非法人员所发的欺骗信息正确区分开，既能保证合法交易的进程，又能防止可能的诈骗行为；真实性是指智能卡和系统都必须有一种确证能力，能够确证它们各自所收到的信息都确实是真正由真实对方发出的信息，而且自己所发出的信息也确实是被真正的对方所接收到了；保密性则是指利用密码术对信息进行加密处理，从而防止攻击者窃取所交换的信息。满足这 4 种特性的要求是保证一个信息交换过程安全性的最基本条件，缺一不可。

(1) 完整性的保证。为了保证所交换的信息内容不被非法修改,对之进行鉴别是非常重要的,这种鉴别称为对报文内容的鉴别。一般方法是在所交换的信息报文内加入一个报头或报尾,称其为鉴别码。这个鉴别码是通过对报文进行某种运算而得到的,它与报文的内容密切相关,报文的正确与否可以通过这个鉴别码来检验。鉴别码由报文发送方计算产生,并和报文一起经加密后提供给接收方,接收方在收到报文后,首先对之解密得到明文,然后用约定的算法计算出解密报文(明文)的鉴别码,再与收到报文中的鉴别码相比较,如果相等,则认为报文是正确的;否则就认为该报文在传输过程中已被修改过,接收方可以采取相应的措施,如拒绝接收或报警等。在鉴别过程中,鉴别算法的设计是至关重要的。最简单的算法是计算累加和,即把所传输报文中的所有位全加起来作为该报文的鉴别码。比较理想的鉴别算法一般是与密码学相联系的。鉴别过程的安全性就取决于鉴别算法的密钥管理的安全性。

(2) 信息交换过程的有效性。防止对曾经发送过的或存储过的信息的再利用。例如,在某次交易过程中的一条真实信息(假设是某人从银行账户内提取了一笔钱款),如果这一消息被一个非法截听者记录了下来,他可能一遍遍地重发该消息,如果不能进行报文有效性的验证,那么该人银行账户内的存款将很快就被提光。因此,必须能保证所传送的消息每一条都是唯一的,任何随后产生的重复消息都应当被认为是非法的。实现这种报文时间性鉴别的方法有很多种,常用的方法是每条消息在发送时都附加一个发送当时的日期和时间;或者在报文中加入一个随机数等,从而保证报文的唯一性。

(3) 真实性。真实性指的是对报文发送方和接收方的鉴别,即对话的双方彼此都要对对方的真实性进行验证,这种验证称为“双向鉴别”。双向鉴别的具体内容将在 5.4 节中(即在密码技术之后)讨论。

(4) 保密性。保密性主要是利用密码技术对信息进行加密处理,以掩盖真实信息,使报文不可理解,达到保密的目的。由于加密、解密是通信安全中最常用的密码技术,也是通信安全的基础之一,其地位极其重要,因此下节专门进行讨论。

5.3 密码技术

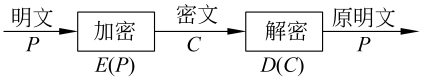
密码技术的出现最初即是以通信的秘密性为目的的,其基本思想就是伪装信息,使局外人不能理解信息的真正含义,而局内人却能理解伪装信息的本来意义。密码技术的实际应用可以追溯到远古时代。公元前 50 年,古罗马的恺撒在高卢战争中就用过一种密码技术来保证其军事命令在传输过程中的保密性,他把从 A 到 W 的每个英文字母均用字母表中它后面的第 3 个位置上的字母来代替,字母 X、Y、Z 分别用 A、B、C 表示。如果分别以数字 0、1、…、25 来对应字母 A、B、…、Z,则他的这种密码变换规则就可以表示成如下形式,即

$$\Phi=\theta+3 \mod 26$$

我们把被伪装的信息称为“明文”,伪装后的信息称为“密文”,而加密时所采用的信息

变换规则称为“密码算法”。在上式中，Φ 为密文字母，θ 为明文字母，3 就是这种密码算法的密钥。如果 Φ 的值超过或等于 26，则减去 26，这就是 mod 26 的意义。显然，这种密码算法是十分简单的。而到了现代，随着计算机在密码学领域的广泛应用，同时也由于现代数学的发展，使现代密码学无论在原理、概念还是工具上都有了巨大的创新与改进。然而，这些新的技术知识也给破译者提供了强有力的工具，从而又给现代密码学提出了新的任务。

所谓加密，就是对机密信息加以伪装的一个过程。被加密的信息称为“明文”，而把密文转变为明文的过程称为“解密”。以下形式表明了这个过程。



明文用 P 表示，在智能卡中，它表现为比特流或二进制数据。

密文用 C 表示，它也是二进制数据，加密函数 E 作用于明文 P 得到密文 C，其表达式为

$$E(P)=C$$

解密函数 D 作用于 C 产生明文 P，其表达式为

$$D(C)=P$$

由于对明文先加密，再解密将恢复出原来的明文，因此下面的等式成立，即

$$D(E(P))=P$$

现代的加密算法都使用密钥，用 k 表示，则下述加密/解密表达式成立，即

$$E_k(P)=C$$

$$D_k(C)=P$$

$$D_k(E_k(P))=P$$

在本书中，算法（algorithm）指的是加密和解密时所用的数学变换，密码体制（cryptosystem）指的是算法和实现它的方法。

一个密码体制一般由两个基本要素构成：密码算法和密钥。这里，密码算法是一些公式、法则或程序，一般与现代数学中的某些理论相联系。考虑到密码算法本身很难做到绝对保密，因此现代密码学总是假定密码算法是公开的，真正需要保密的是密钥，即一切秘密都隐藏在密钥中。所以，现代密码学中密钥管理是极为重要的一个方面。

与加密对应的是密码分析，也称“破译”，是指非授权者通过各种方法窃取密文，并通过各种方法推导出密钥，从而读懂密文的操作过程。而用以衡量一个加密系统的不可破译性的尺度称为“保密强度”。一般而言，一个加密系统的保密强度应该与这个系统的应用目的、保密时效要求及当前的破译水平相适应。能够达到理论上不可破译是最好的（非常难），否则也要求能达到实际的不可破译性，即原则上虽然能够破译，但为了由密文得到明文或密钥必须付出十分巨大的计算代价，而不能在希望的时间内或实际可能的经济条件下求出准确答案。

密码体制的分类很多。例如，可以按照密码算法对明文信息的加密方式，分为序列密

码体制和分组密码体制；按照加密过程中是否注入了客观随机因素，分为确定型密码体制和概率型密码体制；按照是否能进行可逆的加密变换，分为单向函数密码体制和双向函数密码体制。卡内常用的是按照密码算法所使用的加密密钥和解密密钥是否相同，能不能由加密过程推导出解密过程（或者反之，由解密过程推导出加密过程），而将密码体制分为对称密码体制和非对称密码体制，在下面将予以讨论，并简述属于单向密码体制的 Hash 算法。在某些卡内还使用了其他算法，如手机的 SIM 卡采用 A3、A5 和 A8 加密算法，Philips 公司支持 CRYPTO 1 流密码加密算法。

5.3.1 对称密码体制

对称密码体制又称为单钥密码体制、对称密钥密码体制、秘密密钥密码体制。在这种密码体制中，加密密钥和解密密钥是相同的，即使二者不同，也能够由其中的一个很容易地推导出另一个。因此它的密钥必须极为安全地传递和保护，从而使密钥管理成为影响系统安全的关键性因素。

目前，在智能卡中应用较多的是对称密码体制，其中较典型的加密算法是 DES 算法。该算法是一种分组密码算法，分组密码算法的基本设计技巧是 Shannon 所建议的扩散（diffusion）和混乱（confusion）。扩散就是要将每一位明文尽可能迅速地作用到较多的输出密文位中，以隐蔽明文的统计特性。扩散同时也是指把每一位密钥的影响尽可能地扩散到较多的输出密文位中。混乱是指密文和明文之间的关系应该尽可能的复杂化，要避免出现很有规律的、线性的相关关系。同时不能让多个明文对应同一密文状态，使解密出现困难。

DES 是 IBM 公司于 1975 年研发成功并公开发表的，这也开创了公开全部算法的先例。

1. DES 算法的加密过程

DES 算法是把 64 位的明文输入块变换为 64 位的密文输出块，它所使用的密钥也是 64 位，其中 8 位为奇偶校验位。整个算法的流程如图 5.4 所示。要加密的一组数据先经过初始置换 IP 的处理，然后通过一系列迭代运算，最后经过 IP 的逆置换 IP^{-1} 给出加密的结果。图 5.4 中，$k_i(i=1\sim16)$ 是初始密钥 K 经分解、移位后产生的 16 个 48 位长的子密钥。从图中可见，与密钥有关的算法包括子密钥的生成和密码函数 f。

1）初始置换 IP

首先讨论初始置换 IP。IP 的功能是将输入的 64 位数据块按位重新组合，并把输出分为 L_0 和 R_0 两部分，每部分各长 32 位。重新组合的规则如表 5.1 所示。

表 5.1 初始置换 IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

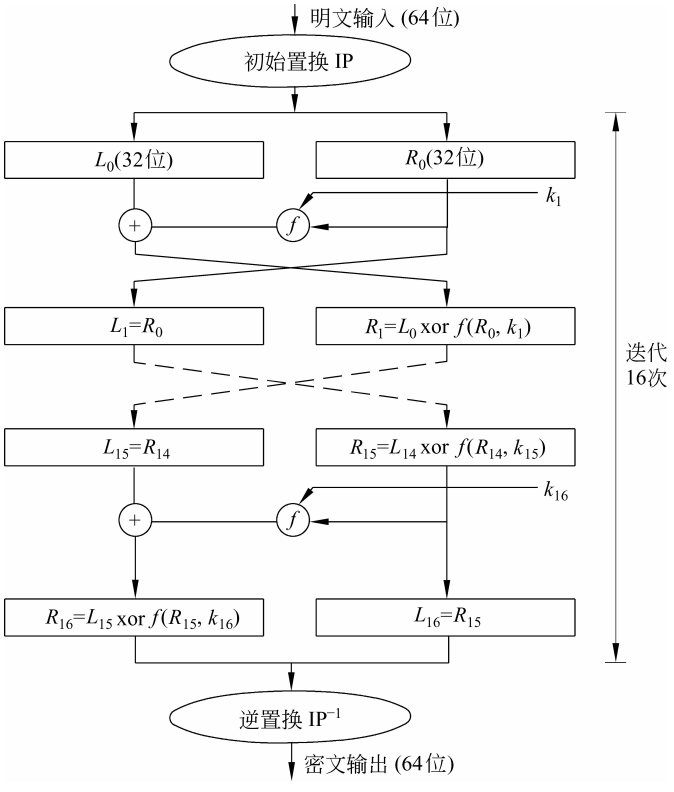


图 5.4　DES 算法

即将输入的第 58 位换至第 1 位，第 50 位换至第 2 位，第 1 位换到第 40 位，依次类推，最后一位是原来的第 7 位。L_0 和 R_0 则是换位输出后划分的两部分，L_0 是输出结果的左边 32 位，R_0 就是右边的 32 位。即如果令置换前的输入值为 $b_1 b_2 \cdots b_{64}$，则经过初始置换后的结果为

$$L_0 = b_{58} b_{50} \cdots b_8 \quad R_0 = b_{57} b_{49} \cdots b_7$$

2）16 次迭代

接下来就是迭代过程，将 R_0 进行扩展，并与子密钥 k_1 进行运算得到 $f(R_0, k_1)$，再与 L_0 按位模 2 加得到 R_1，将 R_0 作为 L_1，就完成了第一次迭代，依次类推，第 i 次的迭代可以表示为

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \text{ xor } f(R_{i-1}, k_i)$$

式中，xor（异或）为按位作模 2 加。

在迭代过程中，f 的操作过程是：首先将 32 位的 R_{i-1} 扩展至 48 位，与子密钥 k_i 按位模 2 加后，再进行两次置换，得到 32 位输出 $f(R_{i-1}, R_i)$。

3）逆置换 IP^{-1}

经过 16 次迭代运算后，得到 $R_{16} L_{16}$，将之作为输入，进行逆置换 IP^{-1}，即得到密文。

IP^{-1}完成的功能正好是 IP 的逆过程。

上述的各次置换都可从 DES 算法的列表中查到，但无法用公式表示，达到扩散和混乱的目的。

4）子密钥 $k_1 \cdots k_{16}$ 的生成

下面介绍子密钥的生成。子密钥 k_i 的生成过程如图 5.5 所示。

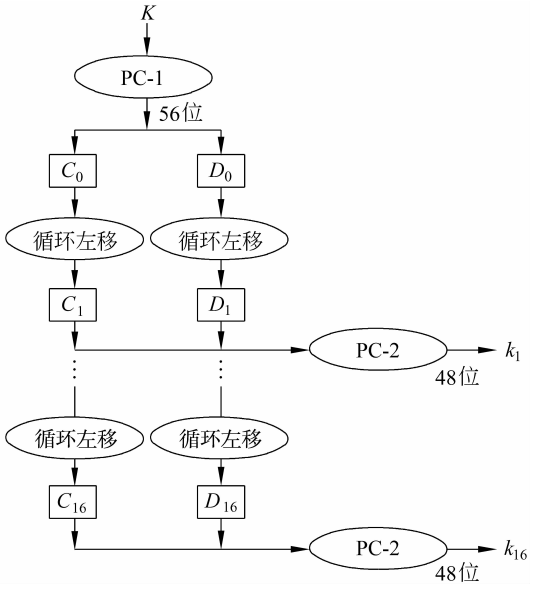


图 5.5　子密钥的生成

密钥 K 本身为 64 位，但其中第 8、16、24、…、64 位是奇偶校验位，所以 K 实际只有 56 位。将这 56 位的数据经过选择换位 PC-1 后产生的结果分为两部分：C_0 和 D_0 分别是左、右各 28 位，然后分别经过循环左移位，得到 C_1、D_1，合并后，再经缩小换位 PC-2，即得到 48 位的子密钥 k_1。同样，将 C_1、D_1 经过循环左移，合并后，再经缩小换位 PC-2，得到子密钥 k_2，依次类推，可以产生 k_3，k_4，…，k_{16}。

以上介绍了 DES 的加密过程。文中提到的换位、置换都有表可查，在本书中基本上都省略了。

DES 的解密算法是一样的，只是采取逆向处理。例如，在第一次迭代时使用 k_{16}，第二次使用 k_{15}……最后一次使用 k_1。

2. DES 算法的安全性

DES 算法的优点是加密/解密的速度快（运算简单），适用于对大量数据进行加密的场合。

DES 算法的安全性在于攻击者破译的方法除了穷举搜索外还没有更有效的手段，而搜索 56 位长的密钥的穷举空间是 2^{56}，在早期，如果用一台计算机搜索，就需要若干年的时间。随着科学技术的发展，更高速计算机、分布式计算机和网络的出现，会使 DES 的安全性受到威胁，某些部门已明确表示不再使用 DES 算法，但目前 DES 算法还是广泛应用于智能卡系统中。例如，在国际和国内流行的金融卡中主要采用 DES 算法，但为了安全

起见，采用双长度密钥的 3-DES 算法。

3. 三重 DES(3DES)

三重 DES 用 3 个密钥对明文加密/解密 3 次。发送者先用第 1 个密钥对明文加密，然后用第 2 个密钥解密，最后用第 3 个密钥加密；接收者用第 3 个密钥解密，用第 2 个密钥加密，最后用第 1 个密钥解密。

$$C=E_{k3}(D_{k2}(E_{k1}(P)))$$

$$P=D_{k1}(E_{k2}(D_{k3}(C)))$$

图 5.6 所示为三重 DES 算法的加密/解密过程，密钥的长度为 168 位(3×56 位)。如果 $k_3=k_1$，则用两个密钥，密钥的长度为 112 位。一般使用的密钥长度为 112 位。

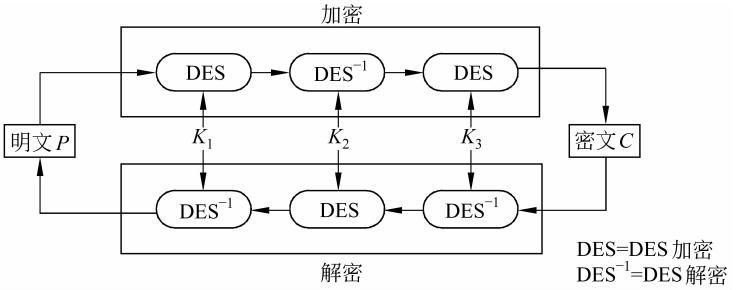


图 5.6　三重 DES

其后发展的高级加密标准 AES(Advance Encryption Standard)是美国国家标准技术研究所 NIST 旨在 21 世纪取代 3DES 的加密标准，加密数据块分组长度为 128 位，密钥长度为 128 位、192 位或 256 位。

对称密码体制的密钥使用了一段时间以后就需要更换，加密方需通过某种秘密渠道把新密钥传送给解密方。在传递过程中，密钥容易泄露。

由于对称密码体制的加密密钥和解密密钥是相同的，在智能卡中采用 DES 算法，当信息的收发方对信息内容及确定有错方产生争执时，DES 算法就显得无能为力了。典型的例子是发送方可能是不诚实的，由于他发送的信息可能对他不利而抵赖，接收方又无法证明该消息确实是由发送方发过来的。在这一争执中，作为仲裁的第三方也无法区分哪一方有错，而使用非对称密码体制可以消除这种争执。

5.3.2　非对称密码体制

非对称密码体制又称为双钥密码体制或公开密码密钥体制。在这种密码体制中，加密和解密分别通过两个不同的密钥实现，并且由其中的一个密钥推导出另一个密钥是很困难的。采用非对称密码体制的每个用户都有一对由认证机构(Certification Authority，CA)发放的数字证书和一对密钥，其中一个可以公开，称为公开密钥，简称为公钥；另一个发给用户秘密保存，称为私钥。有关 CA 的概念和作用参见 5.3.4 节。

非对称密码体制具有如下的一些优点。

(1) 密钥分发简单。由于加密和解密密钥不同，而且不能从加密密钥推导出解密密钥，因而加密密钥表可以像电话号码本一样分发。