严冬冬 编著

智能卡技术及应用

西安电子科技大学出版社

智能卡技术及应用

智能卡技术及应用

严冬冬　编著

西安电子科技大学出版社
1998

内 容 简 介

智能卡又称集成电路卡(IC 卡)，它继承了磁卡的所有优点，并具有很高的可靠性、安全性。本书对IC 卡的应用体系，包括IC 卡的定义、IC 卡的几种常用芯片、读写设备、片内操作系统，以及IC 卡应用系统的开发和具体应用实例进行了较为全面的论述，较详细地阐明了IC 卡的物理结构、逻辑特性及系统实现技术，讨论了有关安全保密体制，读写系统和片内操作系统，并附有IC 卡的有关国际标准。

本书对从事与IC 卡有关的应用系统的开发人员，以及政府、金融、邮电、医疗等系统从事信息处理工作的人员会有帮助，也可供高等院校相关专业的师生参考。

智能卡技术及应用

严冬冬　编著

责任编辑　马武装

西安电子科技大学出版社出版发行

西安电子科技大学印刷厂印刷

新华书店经销

开本 787×1092　1/16　印张 7 4/16　字数 168 千字

1998 年 3 月第 1 版　1998 年 3 月第 1 次印刷　印数 1 - 6 000

ISBN 7 - 5606 - 0571 - 0/TP • 0285　　定价：9.50 元

前　言

智能卡(IC卡)是继磁卡之后出现的一种新的信息工具，它的大量应用将会开创一个全新的自助服务世界。由于IC卡问世不久，完全成功的应用产品在国内尚未普及，有关IC卡的资料也比较缺乏。本书的目的，就是通过对IC卡的介绍，为国内IC卡应用的研究和开发工作提供借鉴与帮助。

本书共分5章。第1章概述了IC卡的定义，讨论了IC卡与磁卡的不同之处以及IC卡的安全问题，并就我国正在实施的“金卡工程”进行了介绍。第2章重点介绍了几种有代表性的IC卡常用芯片，对其性能参数、内部逻辑等分别进行了详细说明。第3章讨论了IC卡的读写设备，包括卡座、读写器，以及读写器的接口电路和读写技术。第4章介绍了IC卡的片内操作系统，包括基本概念、主要功能、信息结构和实现原则。第5章讨论了IC卡具体应用，包括市场情况、开发原则和几个较成功的应用实例。同时，为了方便读者，本书在附录中附上了IC卡的国际标准ISO 7816。

承蒙西安电子科技大学出版社对本书作者的大力支持，使本书得以出版。作者在此对在本书编写过程中给予帮助的所有人士谨以致谢，感谢陈其昌教授对本书的审阅，感谢责任编辑马武装等人在本书编写中给予的指导。

由于时间仓促，有些资料未能编写在内，如法国Gemplus公司的芯片资料。书中不妥之处难免，望广大读者批评指正。

作　者

1997年7月于深圳

目　　录

第 1 章　智能卡概论 …… 1

1.1　智能卡的定义 …… 1
1.2　IC 卡与磁卡的比较 …… 2
1.3　IC 卡的安全问题 …… 3
1.3.1　信息安全的特性 …… 3
1.3.2　威胁 IC 卡信息安全的因素 …… 3
1.3.3　IC 卡的安全技术 …… 4
1.3.4　密码算法 …… 5
1.4　金卡工程 …… 12
1.4.1　金卡工程总体构想 …… 12
1.4.2　金卡工程规划和布署 …… 13
1.4.3　金卡工程有关标准 …… 14

第 2 章　IC 卡及其专用芯片 …… 15

2.1　美国 ATMEL 公司的 AT24C01/AT88SC102/AT88SC51 芯片 …… 15
2.1.1　简单存储芯片 AT24C01/02/04/08/16 …… 15
2.1.2　加密存储芯片 AT88SC102 …… 21
2.1.3　CPU 芯片 AT88SC51/54C …… 30
2.1.4　射频专用集成电路(RFID ASICs) …… 34
2.2　德国 SIMENS 公司的 SLE4406、SLE4404 芯片 …… 38
2.2.1　电话 IC 卡芯片(SLE4406) …… 38
2.2.2　加密存储芯片(SLE4404) …… 38

第 3 章　IC 卡接口设备 …… 42

3.1　概述 …… 42
3.2　卡座 …… 43
3.3　IC 卡读卡器 …… 44
3.3.1　IC 卡的接口电路 …… 44
3.3.2　IC 卡读写技术 …… 46

第 4 章　IC 卡操作系统 …… 56

4.1　智能 IC 卡操作系统的基本术语 …… 56
4.2　智能 IC 卡操作系统的主要功能 …… 57
4.2.1　硬件资源管理 …… 57
4.2.2　通讯传输管理功能 …… 61
4.2.3　应用控制管理功能 …… 62

4.2.4 安全控制管理功能 …… 63
4.3 智能IC卡操作系统的信息结构 …… 65
4.3.1 信息结构 …… 66
4.3.2 智能IC卡操作系统命令 …… 67
4.3.3 IC卡操作系统(COS)的实现 …… 68

第5章 IC卡的应用 …… 70

5.1 IC卡的市场态势 …… 70
5.2 IC卡应用系统的一般组成与开发方法 …… 73
5.3 IC卡系统应用举例 …… 74
5.3.1 IC卡加油站系统 …… 74
5.3.2 IC卡电表收费系统 …… 80
5.3.3 IC卡交通违章处罚系统 …… 81
5.3.4 北京市劳动系统通卡工程 …… 83
5.3.5 IC卡组织机构代码证 …… 85
5.3.6 小结 …… 87

附录 IC卡的国际标准ISO 7816 …… 88

附录A 标准ISO 7816/2带触点集成电路卡触点的尺寸及位置 …… 88
附录B 标准ISO/IEC 7816/3带触点集成电路卡电信号和传输协议 …… 90
附录C 标准ISO/IEC7816－3 AMENDENT1 异步
半双工分组传输协议(T＝1) …… 106

参考文献 …… 110

智能卡概论

随着社会的进步和现代化程度的不断提高，人类所拥有的信息种类和数量都在成倍增加，在这样的社会里，我们每天都要处理许多与个人有关的信息，如购物、打电话、到银行存款取款等，需要携带多种票证、现金、单据，给我们带来很多不便和不安全感。

于是，人们寻求一种具有支付、查询、密码查验等多种功能及安全可靠的“卡”。由于磁卡部分具有上述功能，且其结构简单、价格低廉，因而在全世界得到广泛的应用，其应用环境及产业所提供的服务日臻完善和普及。进入本世纪90年代后，磁卡本身存储量小、安全保密性差、易被伪造、多次使用数据易损坏等不足之处逐步暴露，限制了它的进一步应用。这时，一种存储量更大，安全性更好，更耐用的新工具得到了人们的普遍关注，并已开始逐步推广使用。这就是本书将要介绍的智能卡。

1.1 智能卡的定义

智能卡的名称来源于英文“SMART CARD”，又称集成电路卡(Integrated Circuit Card)，即IC卡。它是将集成电路芯片镶嵌于塑料基片之中制成的，并被封装成卡片的形式，其外形与磁卡相似，尺寸大小符合ISO 7816标准(54 mm×86 mm×76 mm)。本书中，我们将这种卡统称为IC卡。

IC卡的概念是70年代提出的。法国BULL公司首创IC卡产品，并将这项技术应用到金融、交通、医疗、身份证明等多个方面。IC卡的核心是集成电路芯片，一般为3 μm以下半导体技术制造。IC卡具有写入数据和存储数据的能力。IC卡存储器中的内容根据需要可以有条件的供外部读取，或供内部信息处理和校验用。

根据卡中的集成电路的不同，IC卡可分为以下三类：

(1) 存储器卡：卡中的集成电路为EEPROM(电可擦除可编程只读存储器)。它仅有数据存储能力，没有数据处理功能。

(2) 逻辑加密卡：卡中的集成电路具有加密逻辑和EEPROM。在对卡中的数据进行操作前，必须验证每个卡的操作密码。密码的验证是由卡中的芯片完成，而不是由读卡终端完成。卡中有一个错误计数器，如果连续三次验证密码失败，则卡中数据被自动锁死，该卡不能再使用。

(3) CPU卡：卡中的集成电路包括CPU(中央处理器)、EEPROM、RAM(随机存储器)以及固化在ROM(只读存储器)中的COS(片内操作系统)。其唯一工作方式为“用户方式”，分为通用型和专用型两种。专用型是指其中的CPU为专用的、保密的，与通用型的主要差别在于其有很好的物理保护措施。智能卡的发展方向是保密的专用型。

如按卡与外界的数据传送形式来分，IC卡可分为接触型和非接触型两种。当前广泛使用的是接触型IC卡，在这种卡的左上角有印制版，上面有8个触点可与外部接触。非接触型IC卡的集成电路不向外引出触点，因此它除了有上述IC卡的电路外，还带有射频收发电路及其相关电路 。

由于目前磁卡的使用非常广泛，为了从磁卡平稳过渡到智能卡，考虑到两者的兼容性，所以很多智能卡上也有磁条。因此，IC卡也可同时作为磁卡使用。IC卡的尺寸、触点的位置与用途、磁条的位置及数据格式等均有相应的国际标准给予明确规定。

1.2　IC卡与磁卡的比较

IC卡与磁卡外形差不多，但两者在许多方面存在差异。

(1) 抗破坏性和耐用性：磁卡是靠磁条来存储信息的，在遇到强磁场、静电、扭弯、刮伤等情况下，存储在磁条里面的信息容易丢失；另外，磁条上的信息存放时间较短及读写次数较少，修改不方便。IC卡是由硅片来存储信息的，先进的硅片制作工艺完全可以保证IC卡的抗磁性、抗静电及各种射线的能力；由于硅片的体积很小，里面有环氧树脂的保护，外面有PCB板及基片的保护，因此，其抗机械、抗化学破坏能力也很强。目前，IC卡的信息保存期都在100年以上，而且读写方便，读写次数高达10万次以上。

(2) 存储量和灵活性：磁卡的存储容量最大只有几百个字节，一般磁条只有几十个字节。IC卡的容量可以做到几千个字节，而且其存储区还可以划分，允许有不同的访问级别，为信息处理和一卡多用提供了方便。

(3) 保密性：由于磁卡存储量有限，内部没有对数据内容的安全控制或对读写控制的逻辑电路，读取技术是顺序和机械的。所以，磁卡的保密性较差，容易被复制。IC卡具有很强的保密性，首先体现在芯片的结构和读取方式上。IC卡的容量比较大，而且存储器的读取和写入区域可以任意选择，因此灵活性较大。一般的存储器卡，采用特定的技术，具备较强的保密性。加密存储器卡，其存储区的访问受逻辑电路控制，只有密码正确，才能进行读写，而且密码的核对次数有限，超过规定次数，卡将被锁死。CPU卡的保密性更高，除了密码控制外，还有信息处理功能，可利用各种硬件手段加密，也可利用软件的各种加

密算法加密。

(4) 读写设备成本：磁卡的读写设备中含精密机械和信号转换部件，成本高，一个简单读卡器价格达几百元，复杂点的要到几千元，而且可靠性低、维护量大；另外，由于磁卡容量小，许多信息不能存到卡上，为了保证系统的安全性，对计算机网络的要求高，软件工作量大。IC卡因其本身就能提供数字信号，所以读写只需一个插卡的卡座，简单的卡座价格在十几元，高级的也只要几百元，而且使用寿命长，可靠性高，基本不须维护；由于IC卡的容量大，保密性好，许多信息可以放到卡上，因此对系统网络的要求也不高，系统设计和使用也很方便。

综上所述，IC卡优于磁卡，正在或将要逐步取代磁卡，并将开拓出新的应用领域。

1.3 IC卡的安全问题

IC卡是存储现金、票据、持卡人个人或单位资料等重要信息的媒体。IC卡具有的安全技术必须足以保证信息的安全。

1.3.1 信息安全的特性

一般来讲，信息安全必须具有以下几个方面的特性：

(1) 保密性，防止未经授权的信息获取；

(2) 完整性，防止未经授权的信息更改(修改、删除、增加)；

(3) 可获取性，防止未经授权的信息截取；

(4) 真实性，利用技术手段验证信息的真实性，如数字签名；

(5) 持久性，长时间保存信息的可靠性，准确性。

1.3.2 威胁IC卡信息安全的因素

威胁IC卡信息安全的因素主要来自两个方面：

一、人为因素

人为因素具有主动性，它涉及到信息的保密性、完整性、可获取性、真实性，是对信息安全的主要威胁。具体可表现为以下几种情况：

(1) 截取IC卡和接口设备之间的信息流，分析、复制或插入假信号；

(2) 伪造IC卡，由于流入或流出IC卡及接口设备的信息是可以模拟的，因此，接口设备无法判断信息是来自合法的IC卡还是非法的IC卡；

(3) 在交易中更换IC卡，由于在刷卡交易中，可能存在时间上的迟延，在该迟延时间内，将已授权的IC卡在响应信号写入之前换成另一张卡或一张假卡，将响应信号(即交易数据)写入该卡中；

(4) 对IC卡提供错误的控制信息，如修改余额更新日期，从而可获取最高授权余额；

(5) 销售方或承兑方的作弊；

(6) 接口设备被借用，私自拆卸、改装；

(7) IC 卡的发卡过程，发卡机构的工作人员的安全管理；

(8) 持卡人的非法使用。

任何依赖用户的安全措施都是不可靠的，所以必须对持卡人、IC 卡和接口设备的合法性作相互校验，还需具有授权保护功能、审计跟踪功能、日志功能及设置止付名单(黑名单)。

二、客观因素

客观环境对 IC 卡的干扰、破坏，会影响到信息的持久性和准确性，因此，在封装设计上应考虑保护措施，使芯片免受化学、电气、静电损害。此外，对电触点也须采取措施使之免受玷污。

1.3.3　IC 卡的安全技术

一、IC 卡卡基表面的安全技术

(1) 荧光安全图像印刷技术；

(2) 微线条技术：肉眼看是一段直线条，实际为一系列很小的具有一定安全标识意义的字母、数字序列；

(3) 激光雕刻签名：利用激光将有关图形、字母、数字等签名信息直接“刻入”IC 卡卡基中，而不是仅仅印刷在卡的表面；

(4) 激光雕刻可触摸向量字符；

(5) 激光雕刻图像，利用激光将持卡人照片以不同辉度完全印刷嵌入卡基内；

(6) 安全背景结构，类似于纸币的回纹图案等；

二、硬件安全

芯片保护，包括金属化结构、熔断丝、探测器、随机数产生、存储器逻辑保护和协处理器提供加密运算等措施。芯片安全是 IC 卡安全的基础。其反物理攻击的方法主要有下面几种：

(1) 通过烧断熔丝使测试功能不可再激活；

(2) 高/低电压检测；

(3) 低时钟工作频率的检测；

(4) 通过监控程序防止对地址和数据总线的截听；

(5) 逻辑实施对存储器的保护，设置错误计数器，连续三次口令错误，锁死芯片；

(6) 总线和存储器的物理保护层。

三、软件安全

1. IC 卡存储区的保护

利用软件将 IC 卡的数据存储区划分为若干个区，对每个区都设定各自的访问条件；只有在满足设定条件的情况下，才允许对相应的数据存储区进行访问。通过存储区域的划分，普通数据和重要数据被有效地分离，相应地提高了逻辑安全的强度。

2. IC 卡通信安全与保密

主要是涉及通信过程中的信息完整性、可获取性、真实性和机密性。

(1) 对完整性的保证，即保证所交换报文内容不被非法修改，一般在报文内加入报头

或报尾，即鉴别码。鉴别码由发送方计算产生，和报文一起加密后发送。接收方收到后进行解密，然后用约定的算法算出鉴别码，将其与报文中的鉴别码进行比较。如相等，则报文完整。

对报文可获取性的保证，防止对曾经发送过或存储过的信息的再利用。其实质是对报文时间性的鉴别，即保证所传送的每一条信息都是唯一的，其后产生的重复信息全是非法的。一般在报文中加入一个以时间变量产生的随机数。

(2) 对真实性的保证，即对报文发送方和接收方的鉴别。这一鉴别采用数字签名及身份认证(Authentication)的概念，也就是说IC卡和接口设备之间只有相互认证之后才能进行数据的读、写等具体操作。认证的主要目的在于鉴别伪造的IC卡及应用终端。

认证有以下几种工作方式：

① 内部认证：应用终端阅读IC卡中的固定数据，计算出认证密钥。终端产生随机数并送给IC卡，同时指定下一步应用的密钥。IC卡用指定密钥对该随机数进行加密，然后将加密的随机数送回终端。终端对该随机数进行解密，比较是否一致，若一致则内部认证成功。

② 外部认证：终端设备从IC卡中读取卡数据并算出认证密钥。因为IC卡本身不能发送此数据，所以由终端设备控制。终端设备从IC卡中取得一随机数(通常为8字节)，用认证密钥对之进行加密并发送到IC卡。IC卡对此加密值进行对比。

③ 相互认证：终端设备从IC卡中读取卡数据并从中算出认证密钥。终端设备从IC卡中取得一随机数(通常为8字节)并产生其自己的一随机数(通常为8字节)。这两个随机数和卡数据由认证密钥一起加密。终端设备将此加密值送到IC卡。IC卡用终端设备指定的认证密钥对此加密值进行解密、比较。若正确，IC卡用认证密钥加密终端设备的随机数和自己的随机数，并将此加密值发送回终端设备。终端设备解密此加密值再与自己的随机数进行对比。

从以上三种认证工作方式可以看出，加密解密密钥只存在于IC卡和有关应用终端的内部，一旦形成决不外露。因此，密钥十分安全。每次认证以随机数为媒介，且每次认证数据均不相同(相同概率很小)，因而破译难度大(几乎不可能)。所以这种工作方式具有很高的安全性。其中加密解密算法一般均采用国际通用的DES或RSA算法。这两种算法均具有很高的安全性。

(3) 对机密性的保证，利用密码技术对报文进行加密处理。

1.3.4 密码算法

通常用的有两种密码算法：第一种为对称密钥密码算法或秘密密钥算法(DES)；第二种为非对称密钥密码算法或公共密钥算法(RSA)。

(1) 对称密钥密码算法或秘密密钥算法(DES)：

对称密码体制，就是加密密钥和解密密钥是相同的，即使不同，也容易由其中一个导出另一个。也就是说，在这种密码体制中，能加密也就能解密，所以密钥的管理成为影响系统安全的关键。目前，这种特点已难以适应现在计算机系统开放性的要求。

DES密码是1977年由美国国家标准局公布的一个分组密码算法。

分组密码是将明文按一定的位长度分组，明文组和密钥组全部经过加密运算得到密文组。解密时密文组和密钥组经过解密运算(加密运算的逆运算)，还原为明文组。

分组密码的优点是：密钥可以在一定时间内固定，不必每次变换，因此给密钥配发带来了方便。但是，由于分组密码存在着密文传输错误在明文中扩散的问题，因此在信道质量较差的情况下无法使用。

(2) 非对称密钥密码算法或公共密钥算法(RSA)：

1976 年有人提出了公共密钥密码体制，其原理是：加密密钥和解密密钥分离。这样一个具体用户就可以将自己设计的加密密钥和算法公诸于众，而只保密解密密钥。任何人利用此加密密钥和算法向该用户发送的加密信息，该用户均可以将之还原。因此，人们通常也将这种密码体制称为双密钥密码体制或非对称密码体制。

公共密钥密码的优点是：不需要经安全渠道传递密钥，大大简化了密钥管理。所以，又可称为公开密钥算法或简称为公钥算法。

1978 年有人提出了公共密钥密码的具体实施方案，即 RSA 方案。

1991 年提出的 DSA 算法也是一种公共密钥算法，在数字签名方面有较大的应用优势。

目前，国际上在智能 IC 卡上应用得较多的加密解密算法是 DES 算法、RSA 算法及 DSA 算法。下面重点介绍这三种算法。

一、数据加密标准 DES

1973 年，美国国家标准局开始研究除国防部外的其它部门的计算机系统的数据加密标准，加密算法要达到的目的(通常称为 DES 密码算法要求)主要有以下几点：

- 提供高质量的数据保护，防止数据未经授权的泄露和未被察觉的修改；
- 具有相当高的复杂性，使得破译的开销超过可能获得的利益，同时又要便于理解和掌握；
- DES 密码体制的安全性应该不依赖于算法的保密，其安全性仅以加密密钥的保密为基础；
- 实现经济、运行有效，并且适用于多种完全不同的应用。

1977 年 1 月，美国政府颁布：采纳 IBM 公司设计的方案作为非机密数据的正式数据加密标准 (DES—Data Encryption Standard)。

1. DES 密码算法

DES 密码实际上是 Lucifer 密码的进一步发展。它是一种采用传统加密方法的分组密码。它的算法是对称的，既可用于加密又可用于解密。

图 1.1 中 k_i(i=1～16)是初始密钥 K 经分解、移位后生成的 48 位长的子密钥；f 为密码函数。子密钥 k_i 的生成如图 1.2 所示。初始密钥 K 为 64 位，其中 8、16、24、…、64 (8 * N)位是奇偶校验位，所以 K 的有效位只有 56 位。对有效位的数据(56 位)按换位规则 P(见表 1.1)进行换位，再将得到的结果分为左右两部分 C_0、D_0，各 28 位。C_0、D_0 分别经循环左移得到 C_1、D_1，左右合并，按换位规则 CP(见表 1.2)进行缩小换位，得到 48 位子密钥 k_1。同样 C_1、D_1 分别经循环左移得到 C_2、D_2，左右合并，按换位规则 CP 进行缩小换位，得到 48 位子密钥 k_2。同理可得 k_3，…，k_{16}。这里循环左移的位数按表 1.3 进行。

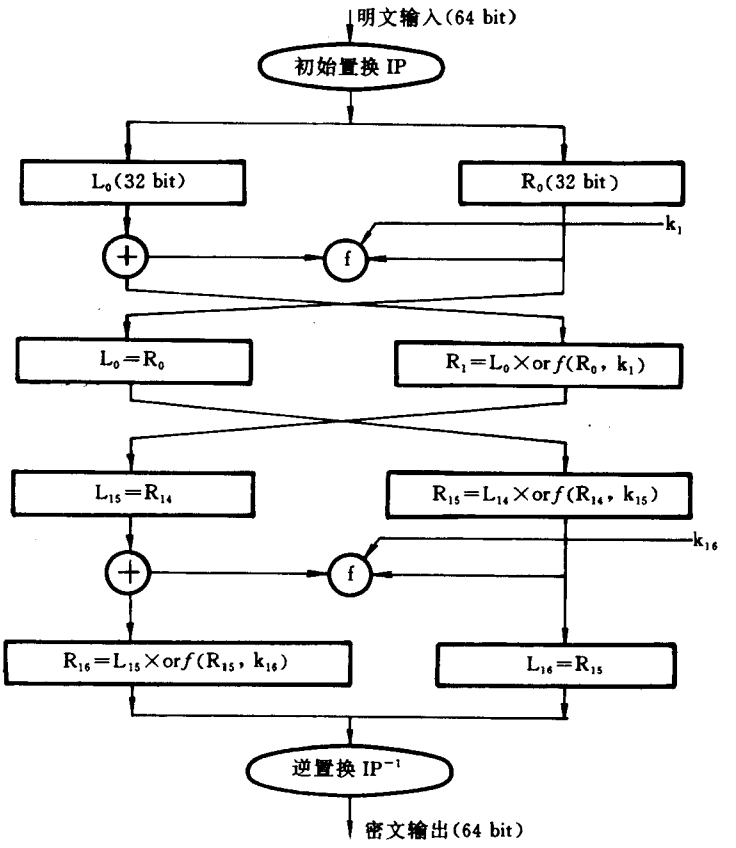

图 1.1　DES 密码算法粗框图

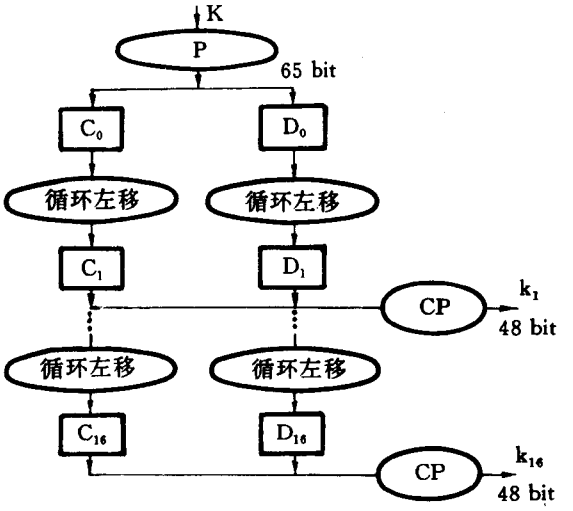

图 1.2　子密钥 k_i 的生成

表 1.1　换位规则 P

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

表 1.2　换位规则 CP

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	22

表 1.3　循环左移的位数

迭代次数	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
左移位	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

要加密的明文经过初始置换 IP(见表 1.4)的处理，然后再经一系列迭代运算，所得结果由 IP 的逆置换 IP^{-1}(见表 1.5)给出加密结果。IP 的功能是将输入的 64 位数据按位重新组合，分为 L_0、R_0 两部分，位长皆为 32 位。表 1.4 为初始置换 IP 的换位规则，表 1.5 为逆置换 IP^{-1}的换位规则。f 为密码函数，其结构如图 1.3 所示。它的功能是利用放大换位 EP(见表 1.6)将 32 位的 R_{i-1}扩展到 48 位。在与子密钥 k_i 按位作模 2 加后，将所得结果分为 8 个 6 位长的数据块，分别经替代函数 S_1，S_2，…，S_8(即所谓的 S 盒)变换产生 8 个 4 位长的数据块，合并为 32 位，再经简单换位 SP(见表 1.7)得到 $f(R_{i-1}, k_i)$。表 1.8 为替代函数 S_i。

表 1.4　初始置换 IP 的换位规则

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

表 1.5　逆置换 IP^{-1}的换位规则

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

表 1.6　放大换位 EP

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

表 1.7　简单换位 SP

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

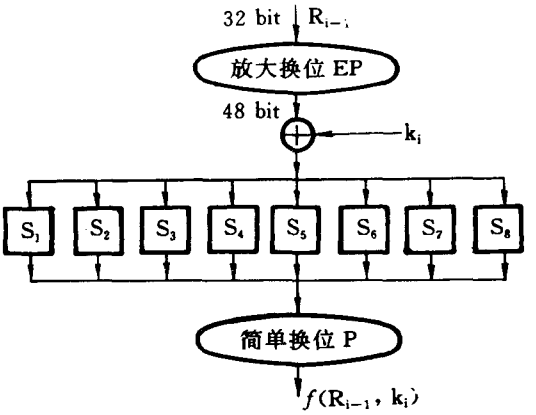

图 1.3　密码函数 f 结构图

表 1.8　替代函数 S_i(S 盒)

R/h	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	S_1
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0	
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	S_2
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	S_3
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12	
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15	S_4
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9	
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4	
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14	
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9	S_5
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6	
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14	
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3	
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11	S_6
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8	
2	9	14	15	5	2	8	12	3	7	0	4	10	1	3	11	6	
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13	

续表

R/h	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1	S_7
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6	
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2	
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12	
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7	S_8
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2	
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8	
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11	

说明：假设输入 6 位二进制数 $D=d_1d_2d_3d_4d_5d_6$，则表中 $h=d_2d_3d_4d_5$，$R=d_1d_6$，根据 R、h 可得 $S=s_1s_2s_3s_4$(4 位二进制数)，完成将 6 bit 的输入变换为 4 bit 的输出。

DES 算法可以使用四种操作模式，这四种操作模式是：电子密文、密码分组链接、输出反馈及密文反馈。其中，电子密文是最简单的模式，安全性也最差；密码分组链接经常以软件方法实现；输出反馈和密文反馈往往在硬件实现的算法中实现。

DES 公布之后，制造有关 DES 设备的厂商已达几十家。随着 DES 应用的日益扩大，各种 DES 专用芯片也应运而生，这种 DES 芯片价格便宜，加密解密速度快，在有关产品中使用十分广泛。

2. DES 密码的破译

首先考虑用穷举法破译 DES 密码的问题。设已知一段密码文 C 及与它对应的明码文 M，用一切可能的密钥 K 加密 M，直到得到 E(M)=C，这时所用的密钥 K 即为要破译的密码的密钥。穷举法的时间复杂性是 T=O(n)，空间复杂性是 S=O(1)。对于 DES 密码，$n=2^{56}\approx 7\times 10^{16}$即使使用每秒钟可以计算 100 万个密钥的大型计算机，也需要算 10^6 天才能求得所使用的密钥，因此看来是很安全的。

3. DES 密码反破译的策略

自 DES 算法公诸于世以来，人们一直对 DES 的安全性持怀疑态度，对密钥的长度、迭代次数及 S 盒的设计众说纷纭。从技术上说，对 DES 的批评主要集中在以下几个方面：

(1) 作为分组密码，DES 的加密单位仅有 64 位(二进制)，这对于数据传输来说太小，因为每个分组仅含 8 个字符，而且其中某些位还要用于奇偶校验或其他通讯用途；

(2) 密钥仅有 56 个二进制位未免太短，各次迭代中使用的密钥 K(i)是递推产生的，这种相关性降低了密码体制的安全性。目前，有人认为：在现有的技术条件下用穷举法寻找正确密钥已趋于可行，若要安全保护 10 年以上的数据最好不用 DES 算法；

(3) 实现替代函数 S_i 所用的 S 盒的设计原理尚未公开，其中可能留有隐患。更有人担心 DES 算法中有“陷阱”，知道秘密的人很容易进行密文解密。

针对以上 DES 的缺陷，人们提出了几种增强 DES 安全性的方法，主要有以下几种：

• 三重 DES 算法：此方法为密码专家 Merkle 及 Hellman 推荐。

• 具有独立子密钥的 DES 算法：每一轮迭代都使用一个不同的子密钥，而不是由一个 56 个二进制位的密钥产生。由于 16 轮迭代的每一轮使用一个 48 个二进制位的密钥，所以这一方法可以增强 DES 的加密强度。

·带用交换S盒的DES算法：Biham和Shamir证明，通过优化S盒的设计，甚至S盒本身的顺序，可以抵抗差分密码分析，以达到进一步增强DES算法的加密强度的目的。

二、RSA(Rivest－Shamir－Adleman)算法

1976年，Diffie和Hellman在斯坦福大学发表了在密码学史上有深远意义的论文《密码学的新方向》。他们指出，可以适当选择加密算法E和解密算法D，使得即使知晓加密算法E也无法推出解密算法D。他们的论文使密码工作者耳目一新，开辟了密码学研究的一个新方向。他们提出的密码体制要满足以下三个要求：

(1) D(E(M))＝M；

(2) 从E推出D在计算上是不可能的；

(3) 用选择明码文破译E在计算上是不可能的。

第一条要求说明，如果把D运用于加密后的消息E(M)，将恢复明码文消息M。第二条要求是公共密钥密码体制的关键，否则就不能将E公开。第三条要求也是完全必要的，因为在已知E的情况下，密码分析员肯定会选择一些明码文，用E对它加密，并千方百计地破译它。

满足这些要求后，就没有理由再不把E公布于众。在利用公共密钥密码体制时，需要进行秘密通讯的用户首先设计出满足以上三个要求的E和D。然后把E公布于众，比如刊印在文件中或登记在手册上。任何想与他通讯的用户都可以用他的公开变换加密消息M生成E(M)，他收到E(M)后，再用他的秘密变换D解密E(M)，得到明码文消息M＝D(E(M))。

在传统密码体制中，由于加密密钥和解密密钥可以简单的互导，因此密钥必须首先经由安全通道分发给通讯双方，随后才能利用公共通道建立起安全通讯，因而密钥分配问题是传统密码体制的薄弱环节。公共密钥密码体制不存在这个问题，因此特别适合于在计算机网络中建立分散于各地的用户之间的秘密通讯联系。

公共密钥密码体制的上述优点，使得设计者的论文问世之后立即受到密码学界的普遍关注。许多研究人员进行了认真的研究，目前已发表了一些实用的算法。RSA方法就是其中一种。

RSA算法于1978年首次推出，以三位发明者Rivest、Shamir及Adelman的名字命名，并在以后经受住了多年广泛的密码分析破译。

RSA算法的安全性来自于分解大数因子的困难。大数分解(将一个大合数分解成其素数因子的乘积)和素性检测(判定一个给定的正整数是否为素数)是著名的数论难题之一，高斯曾称之为“算术中最重要最有用的问题之一”。古往今来，曾吸引不少的中外学者以浓厚的兴趣为此付出了艰辛的努力，然而由于其本身所固有的难度及指数阶的计算复杂度，一直困扰着人们进行更深入的探索。本世纪50年代以来，随着计算机技术的飞速发展以及有关理论方法的不断提出，对这个古老的难题研究又重新兴起，许多研究成果被直接应用于密码学中，导致了密码学研究的第二大成就的代表——RSA公共密钥密码体制的出现，并广泛应用于金融、商业等领域。

在RSA算法中，解密密钥(专用)和加密密钥(公用)是一对非常大(100～200位十进制数或更大)的素数的函数，该算法由素数计算出两个密钥，而且猜想由一个密钥确定另一个密钥相当于分解两个素数乘积的因子。目前，为实现RSA算法，需要寻找大质数，这个