电脑技能百练丛书

加密解密技能百练

邱志聪 编著

定价 28 元

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

电脑技能百练丛书

加密解密技能百练

邱志聪　编著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

本书从理论和实际应用两个方面详细地向读者介绍了加密解密技术的理论基础、原理和实现方法。内容包括如下几方面：现代密码算法、常用文件加密系统、信息隐藏技术、系统加密解密、口令破解原理、网络攻击与防护、网络监听与扫描以及安全身份认证。全书涵盖了信息安全技术中的攻击、防御、隐藏、监控、身份认证等多方面的基础理论知识和实施技术。

本书从实用的角度出发，立足于“看得懂、学得会、用得上”，在内容安排上将理论讲解和实际演练相结合，突出其实用性和针对性，旨在学习完一定的理论知识后能够通过练习快速掌握该知识。书中讲解的练习实例均经过作者的实际操作，读者可以依据内容直接进行练习。

本书主要面向入门级的读者，同时也为计算机专业人员、通信专业人员和信息安全领域工作人员提供一定的参考。

图书在版编目（CIP）数据

加密解密技能百练/邱志聪编著. —北京：中国铁道出版社，2004.11

（电脑应用技能百练）

ISBN 7-113-06254-7

Ⅰ.加… Ⅱ.邱… Ⅲ.①电子计算机—密码—加密 ②电子计算机—密码—解密译码 Ⅳ.TP309.7

中国版本图书馆 CIP 数据核字(2004)第 115086 号

书　　名：加密解密技能百练

作　　者：邱志聪

出版发行：中国铁道出版社（100054，北京市宣武区右安门西街 8 号）

策划编辑：严晓舟

责任编辑：苏　茜

封面制作：白　雪

印　　刷：北京鑫正大印刷有限公司

开　　本：787×1092　1/16　　印张：18.5　字数：443 千

版　　本：2005 年 1 月第 1 版　　2005 年 1 月第 1 次印刷

印　　数：1～5000 册

书　　号：ISBN 7-113-06254-7/TP・1349

定　　价：28.00 元

出 版 寄 语

技能百练含意

俗话说：千锤百炼，百炼成钢。不经历风雨，怎能见彩虹？

学电脑的路上，有你，有我，并不孤单。但你我用同样的鼠标，同样的键盘，同样的电脑配置，做出来的效果，却总不一样，这是为什么？

这是因为，一分耕耘，一分收获。

当然，不只这些，因为没有创意，作品就没有灵魂。

所以，聪明应该转变成智慧，智慧激发灵感。

在电脑这个广阔的天地里，我们从来不停步。夜深了，击键声伴着家人的鼾声，时间从光标的箭头下飞逝。我们还不能歇息，电脑时代赋予我们去创造具有生命力的作品。

但这一切，都有赖于我们掌握了非常扎实的基础知识和技能。事实上也的确如此，君不见古埃及大大小小金字塔，因其底座大小不同，高低亦不同，底座越大，金字塔越高。

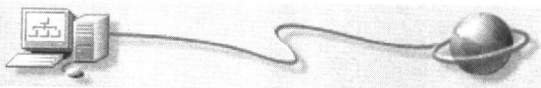
有鉴于此，我们推出《电脑技能百练丛书》，旨在伴您在电脑的旅途上一路同行！

丛书编委

本丛书由第一时间工作室创作完成。愿我们在第一时间共同感受来自电脑时代的最强音。

本丛书编委会成员如下：邱志聪、刘可言、吕梁、王页、薛卫红、金信之、张峥高、喻业、王金秀、康悦辉、韩瑾、李洁、付侃、张占才等。

前言



随着计算机网络技术和电子商务的迅速发展，信息安全已经成为当今社会普遍关注的焦点，各种新闻媒体上不时有某国政府重要网站被攻击、软件出现安全漏洞或者黑客发现操作系统安全漏洞等新闻报道。密码技术已经成为衡量一个国家信息技术发展水平的重要标志，其发展的程度将直接影响国家的安全。

编写本书的目的在于通过介绍各种常用的加密和解密技术，使读者对密码技术有进一步的了解，从而更加有效的提高个人信息安全。

本书共分 7 课，每课都安排了练习供读者参考学习。其中第 1 课主要讲解密码学的理论基础，着重讲述现代密码学中的三种密码方式：流式密码、对称密码和非对称密码，同时也讲述了几种常用的密码算法，包括 A5、DES、IDEA 和 RSA 等。第 2 课主要讲解常用的文件加密系统，这些加密系统包括通用文件加密系统、压缩文件的加密方法、多媒体文件的加密方法、PDF 文件的加密方法和 Office 文件的加密方法等。第 3 课主要讲解目前信息安全研究领域中很热门的信息隐藏技术，信息隐藏技术不同于传统的加密技术，其更强调不可检测性。本课内容包括将文件或信息隐藏于其他文件的技术、信息伪装技术和数字签名技术。第 4 课介绍系统的加密，此处讲解的系统的概念是广义的，其包括操作系统、BIOS 系统和防火墙系统等，其中重点讲解了对 Windows 系列操作系统的攻击与防御方法，包括对目前流行的 Windows 2000/NT/XP 系统 SAM 数据的攻击、缓冲区攻击、碎片文件攻击等，同时针对 Windows 98 系统 PWL 文件、屏幕保护密码和网上邻居保护密码等讲述了其对应的攻击与防护方法。此外，本课对 BIOS 系统和防火墙系统也作出了一定的阐述。第 5 课讲解口令破解的原理与方法，首先从密码学上的攻击原理开始，一步步地过渡到实际口令攻击中常用的缺省口令攻击、字典攻击、暴力攻击和混合攻击。除此之外，本课末还讲述了密码的强度以及如何通过工具软件和编程产生随机秘密。第 6 课主要讲解网络的攻击与防护方法，包括 Email 系统的攻击与防护、对流行的聊天软件 QQ 和 ICQ 的攻击与防护、对 IE 浏览器的攻击与防护以及木马程序的攻击与防范等。第 7 课主要讲解在网络优化和攻击中经常用到的两个技术：网络监听和网络扫描，前者用于监听网络上传输的数据包并截获敏感信息，后者用于对网络中主机的漏洞进行扫描。

书中源代码与部分软件下载地址链接可到 http://www.tqbooks.net/download.asp 上免费下载。

由于时间仓促，水平有限，书中错误和不当之处敬请读者批评指正，欢迎与我们联系：（电子邮件）：wg100@vip.sina.com。我们也会在适当时间进行修订和补充，并发布在天勤网站：http://www.tqbooks.net“图书修订”栏目中。

编　者

2004 年 10 月

目 录

第 1 课　加密解密基础——现代密码算法

▼ 本章学习的主要内容有哪些？

加密算法作为加密解密系统的基础，在数据安全保护系统中起着举足轻重的作用。加密和认证是保护系统安全的两种基本技术。加密主要的目的是使截获者在不知道密钥的条件下不能解读密文内容。仙农（Shannon）提出的将明文隐蔽在消息中的基本技术：混乱与扩散。现代密码算法中的序列密码算法依赖于混乱，而分组密码算法则综合运用了混乱和扩散技术，使得其强度有所提高。公开密钥算法作为现代密码算法中的一个重要分支，使用一对相异的密钥来分别进行加密和解密处理，并且这一对密钥不能相互推算。

本章将分别讲解现代密码算法和认证系统的基本原理，同时给出几个著名算法的源代码并详细讲解其应用及编程。

▼ 通过本章的学习要达到什么目标和要求？

通过本章的学习，读者应该掌握密码学的基本概念和知识，对各种密码算法有一定的了解，能够认识三种密码系统各自的特点和优缺点，能够根据算法的强度和速度等性能以选择合适的加密算法，并能够利用本章提供的算法的源代码实际开发工作中加以应用。

▼ 本章知识对掌握加密技术有何重要性？

加密算法是实现加密技术的核心内容，掌握本章讲述的内容对于在实际工作中选择一种合适的加密算法或者是开发一种加密算法有重要的参考性，同时，通过学习本章讲授的知识，读者可以掌握如何在实现几种常用的加密算法并对其进行编程，以便在实际编程工作中提供参考。

▼ 本章难以理解的知识有哪些？掌握这些难点知识有什么方法和窍门？

如何编程实现并利用算法的源代码是本章难以掌握的知识点，由于各个算法的源代码的接口不一致，在使用这些源代码的时候可能会给用户造成一定的困扰。用户应该仔细阅读算法源代码的注释，尤其是对函数的注释，同时要仔细分析算法的流程，必要时建立一个试验项目来进行验证，通过不断的摸索来掌握算法代码的正确使用方法。

课堂讲解

一、密码学的基本概念

采用密码技术可以屏蔽和保护需要保密的消息，使未授权者不能提取消息。被屏蔽的消息称作明文（plaintext），屏蔽后的消息称作密文（ciphertext）。将明文变换成密文的过程称作加密（encryption），其逆过程称作解密（decryption）。对明文进行加密时所采用的一组规则称为加密算法（encryption algorithm），对密文进行解密时所采用的一组规则称作解密算法（decryption algorithm）。加密和解密算法的操作通常都是在一组密钥（key）控制下进行的，分别称为加密密钥和解密密钥。

一个密码通信系统可以用图 1-1 表示，它由以下几个部分组成：信源、加密器、解密器、接收者、加密密钥源、解密密钥源，此外，通常假设系统在遭受攻击者（非法入侵者和密码分析者）攻击的情况下进行通信以检验系统的安全性。

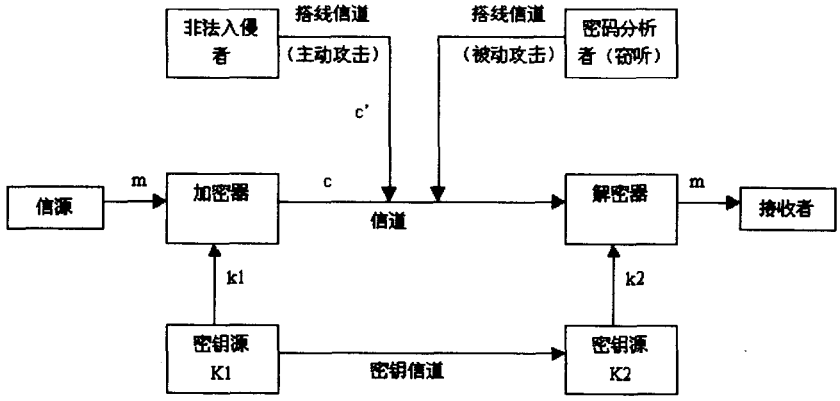


图 1-1　密码系统模型

为了保护信息的机密性，抵抗密码分析，保密系统应当满足以下要求：

（1）系统即使达不到理论上是不可破的，也应当是实际上不可破的。也就是说，从截获的密文或者某些明文－密文对，要确定密钥或者任意明文在计算上是不可行的。

（2）系统的保密性不依赖于对加密体制或算法的保密（Kerckhoff 假设），而依赖于密钥的保密性。

（3）加密和解密算法适用于所有密钥空间中的元素。

（4）系统既易于实现又便于使用。

防止消息被窜改、删除、重传和伪造的一种有效方法是使发送的消息具有被验证的能力，使接收者或第三者能够识别和确认消息的真伪，实现这类功能的密码系统称为认证系统（authentication sysem）。消息的认证性和保密性不同，保密性是使截获者在不知道密钥的条件下无法解读密文的内容，而认证性是使任何不知道密钥的人无法构造一个密报，使指

定的接收者可以确认消息的合法性和有效性。

一个安全的认证系统应满足下述的基本要求：

（1）指定的接收者可以检验和证实消息的合法性和真实性。

（2）消息的发送者对所发送的消息不能抵赖。

（3）除合法的消息发送者外，其他人不能伪造合法的消息。

（4）当通信双发发生争执时，可由仲裁者（arbitrator）解决争执。

1. 密码体制的分类

根据密钥的特点，可以将密码体制分为对称和非对称密码体制两种。对称密码体制又称私钥（private key）密码体制，非对称密码体制又称公钥（public key）密码体制。在私钥密码体制中，加密密钥和解密密钥是一样的或彼此之间容易相互确定，按加密方式不同又可以将私钥密码体制分为流密码（stream cipher）和分组密码（block cipher）两种。在流密码中，将明文消息按字符逐位地加密。在分组密码中，将明文消息分组（每组含有多个字符），逐组地进行加密。在公钥密码体制中，加密密钥和解密密钥不同，而且从一个难以推出另一个，可将加密能力和解密能力分开。

2. 密码算法

密码算法是信息安全的重要基础之一，没有安全的密码算法，就不会有信息安全。针对不同的应用，有不同的安全协议，例如在 Internet 上进行安全的信用卡交易使用了 SET 协议；为了确保数据在网络上传输时不被窃取，定义了 SSL 协议，这些安全协议都必须使用安全的密码算法来对数据作相对应的安全处理，以确保信息在网络上传输时的安全性。使用合适的算法和协议，可以使系统达到以下四项功能：

（1）机密性

数据不会被未授权的攻击者窃取。

（2）可认证性

能够确认数据的来源，确实是传送者本人，而不是其他人伪造的。

（3）完整性

能够确认数据未受到无意或者是恶意的窜改。

（4）不可否认性

发送方在送出消息后，不可否认他曾经送出该消息。

2. 对密码系统的攻击

对一个密码系统的攻击主要有两种：被动攻击和主动攻击。非授权用户通过各种办法（如搭线窃听、电磁窃听、声音窃听等）来窃取机密信息并从截获的密文中推断出原来的明文，这类攻击称为被动攻击。另一类攻击称作主动攻击，非法入侵者主动向系统窜扰，采用删除、更改、填增、重放、伪造等手段向系统注入假信息以达到攻击系统的目的。在密码学中有一个 Kerckhoff 假设，即假设攻击者知道所使用的密码系统。在设计密码系统的时候，应在 Kerckhoff 假设下达到安全性，即不应该把密码系统的安全性建立在敌手不知道所使用的密码系统的前提下。

根据密码分析者破译时已具备的前提条件，通常将攻击类型分为以下四种：

（1）唯密文攻击：密码分析者有一个或更多的用同一密钥加密的密文，通过对这些截获的密文进行分析得出明文或密钥。

（2）已知明文攻击：除待解的密文外，密码分析者有一些明文和用同一密钥加密这些明文所对应的密文。

（3）选择明文攻击：密码分析者可得到所需要的任何明文所对应的密文，这些密文与待解的密文时用同一密钥加密。

（4）选择密文攻击：密码分析者可得到所需要的任何密文所对应的明文，解密这些密文所使用的密钥与解密待解密文的密钥是一致的。

3. 现代密码系统

现代密码系统是相对古典密码系统而言的，通常是指 Shannon 在 1949 年发表了“保密系统的信息理论”，将信息论的理论引入到密码系统中以后发展起来的密码系统。现代密码系统涵盖了流密码系统、分组密码系统和公钥密码系统，这三种密码系统各有特点，在不同的条件下应选择使用适当的密码系统。下面将分别讲述这三种密码系统以及其对应的一些算法。

二、流密码系统

前面已经指出，在私钥密码体制中根据对明文和加密方式的不同可以分为流密码和分组密码。在分组密码中，明文被分为 m 个符号的大数组 $x = (x_1, x_2, \cdots, x_m)$，每一组明文在密钥 $k = (k_1, k_2, \cdots, k_t)$ 的控制下变换成 n 个符号的密文组 $y = (y_1, y_2, \cdots, y_n)$。流密码则是将明文的位串（bit stream）与伪随机数产生器经过适当的运算得到密文。在流密码中，消息被分成连续的符号 $x = x_1, x_2, \cdots$，用密钥流 $k = k_1, k_2, \cdots$的第 i 个元素 k_i 对 x_i 加密，如果密钥流是重复的，则称该流密码是周期的，否则称之为非周期的。分组密码与流密码之间的主要区别在于其记忆性。

1. 分类及工作模式

在流密码中，加密器中存储器的状态随时间而变化，这一变化可以用一个状态转移函数来描述。根据状态转移函数是否依赖于输入的明文符号，可将流密码分为两类，即同步流密码和自同步流密码。

（1）同步流密码

在同步流密码中，状态转移函数与输入的明文符号无关，此时密钥流也与明文符号无关，所以某时刻输出的密文与该时刻之前的明文也无关。因而可将同步流密码的加密器分为密钥流生成器（或称伪随机序列生成器）和加密变换器两部分，如图 1-2 所示。

同步流密码的一个优点是无错误传播，一个传输错误只影响一个符号，不会影响后续数据。

（2）自同步流密码

在自同步流密码中，状态转移函数与输入的明文符号有关，此时密钥流也与明文符号有关，某时刻输出的密文不仅依赖于明文符号。

密码反馈模式是自同步流密码的一种最常用的工作模式，如图 1-3 所示。每个密文产生后都会立刻送到移位寄存器的一端，在每次跌代运算中，移位寄存器的值都作为加密算法 E_B 的输入，而输出的最低位符号用作下一个密文符号。

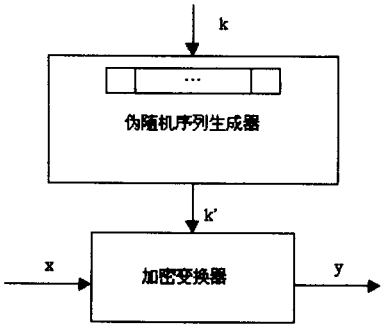


图 1-2　同步流密码系统

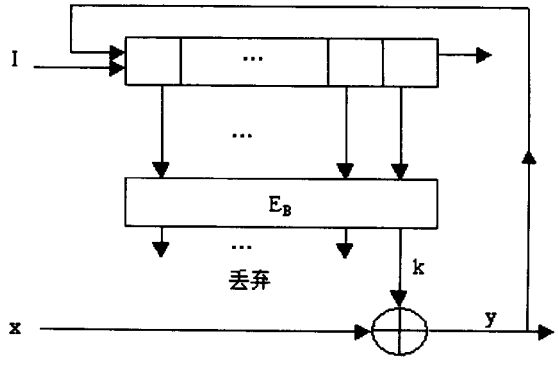


图 1-3　自同步流密码系统

对于密码反馈模式，传输错误影响反馈圈。如果一个密文符号在传输中出错或丢失，则该错误将一直影响输出结果直至该错误移出寄存器。

2. 安全性分析

目前绝大多数有关流密码的研究成果都是同步流密码方面的。但自同步流密码具有抵抗密文搜索攻击和认证功能等优点，非常值得深入研究。同步流密码系统的密码强度主要取决于密钥流生成器的设计，在设计同步流密码系统时一定要注意密钥流生成器的性能。

3. A5 算法

A5 是用于 GSM 加密的序列密码，被用于加密从移动终端到基站的连接，如图 1-4 所示。A5 由三个 LFSR 组成，寄存器的长度分别是 19、22 和 33。所有的反馈多项式系数都较少，三个 LFSR 的异或值作为输出。A5 用不同的时钟控制，每一个寄存器由它自身中间位的时钟控制，并且三个寄存器的中间位的反向门限函数异或。

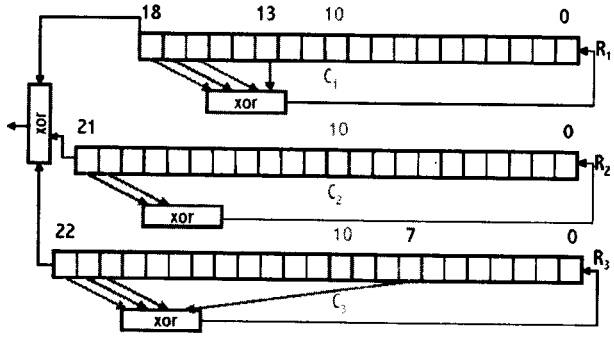


图 1-4　A5 结构图

A5 的基本思路是好的，其效率非常高，并且已经通过所有已知的统计测试。

三、分组密码系统

分组密码是将明文划分为长 m 的数组 $x = (x_1, x_2, \cdots, x_m)$，各组明文分别在密钥 $k = (k_1, k_2, \cdots, k_t)$ 的控制下变换成等长的输出数字序列 $y = (y_1, y_2, \cdots, y_n)$。分组密码的模型，如图 1-5 所示。它与流密码的不同之处在于输出的每一位数字不只与相应时刻输入明文数字有关，而是与一组长为 m 的明文数字有关。

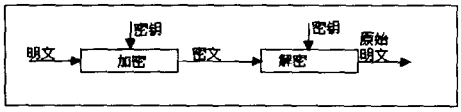


图 1-5　分组密码系统

分组密码系统的优点在于其容易实现同步，因为一个密文组的传输错误不会影响其他组，丢失一个明密文组不会对其后的组的解密正确性带来影响。

目前著名的对称分组密码系统算法有 DES、IDEA、Blowfish、RC4、RC5、FEAL 等。下面将分别讲述 DES、IDEA 等几种著名的分组密码系统算法的原理。

1. DES 算法

DES（Data Encryption Standard）算法是最广为使用的对称分组密码算法。它是 1970 年由美国 IBM 公司提出，被美国国家标准局公布为数据加密标准的一种分组加密法。20 多年来，尽管计算机硬件及破解密码技术的发展非常迅速，但直至今日，在已知的攻击方法，如差分攻击和线性攻击中，还是无法完全攻破 DES，换而言之，DES 仍被公认是安全的。

（1）DES 的描述

DES 是一个分组加密算法，它以 64 位为分组对数据加密。64 位一组的明文从算法的一端输入，另外一端输出 64 位的密文。DES 是对称算法：加密和解密使用同一算法。

密钥通常表示为 64 位，但每个第 8 位都用作奇偶校验，因此有效的密钥长度为 54 位。在所有的密钥空间中有极少量的弱密钥，如全 0 和全 F 的密钥等，在选择密钥时应尽量避免。DES 算法的保密性依赖于密钥的秘密性。

简单地说，算法只不过是加密地两个基本技术——混乱和扩散的组合。DES 的基本组建分组是这些技术的一个组合（先代替后置换），它基于密钥作用于明文。DES 有 16 轮运算，需要在明文分组上实施 16 次相同的组合技术。

（2）DES 算法概要

DES 对 64 位明文进行分组操作。通过一个初始置换，将明文分组分成左半部分和右半部分，各 32 位长。然后进行 16 轮完全相同的运算，这些运算被称为函数 f，在运算过程中数据与密钥解密。经过 16 轮后，左、右半部分合在一起经过一个末置换（初始置换的逆置换），这样算法就完成了，如图 1-6 所示。

DES 的每一轮运算，如图 1-7 所示，在每一轮运算中，密钥移位，然后再从密钥的 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与 48 位密钥结合，通过 8 个 S 盒将 48 位替代成新的 32 位数据，再将其置换一次。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，其结果即

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 次便实现了 DES 的 16 轮运算。

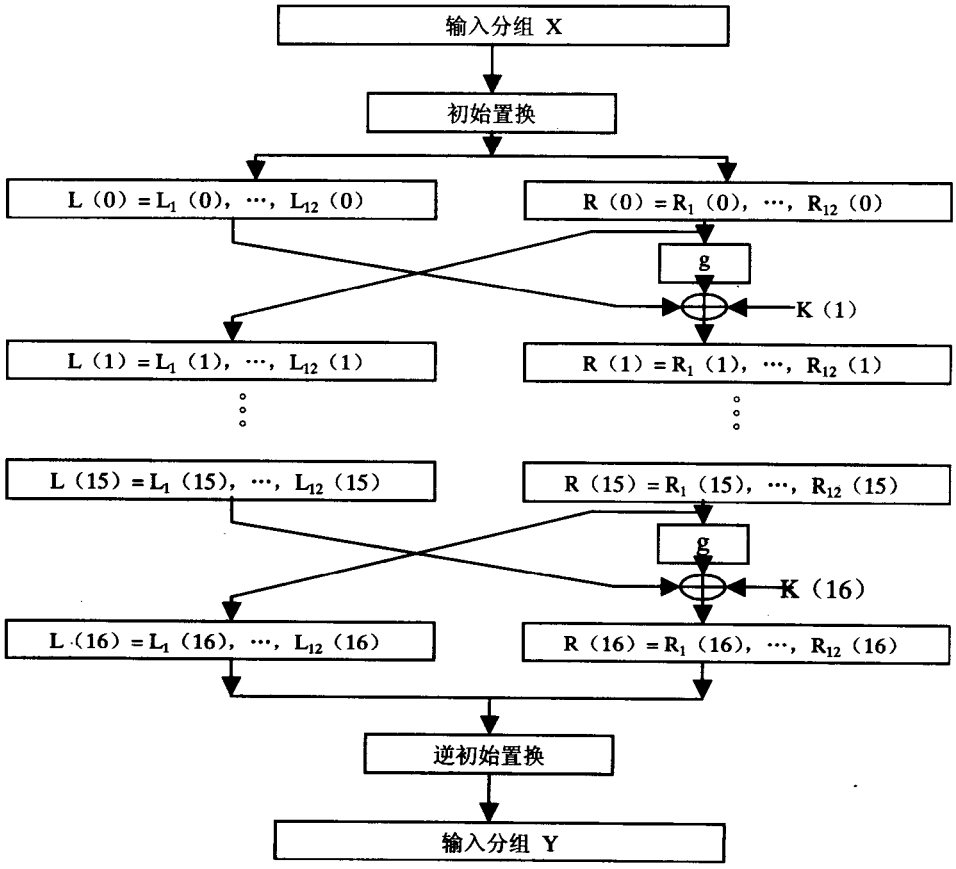


图 1-6 DES 算法概要

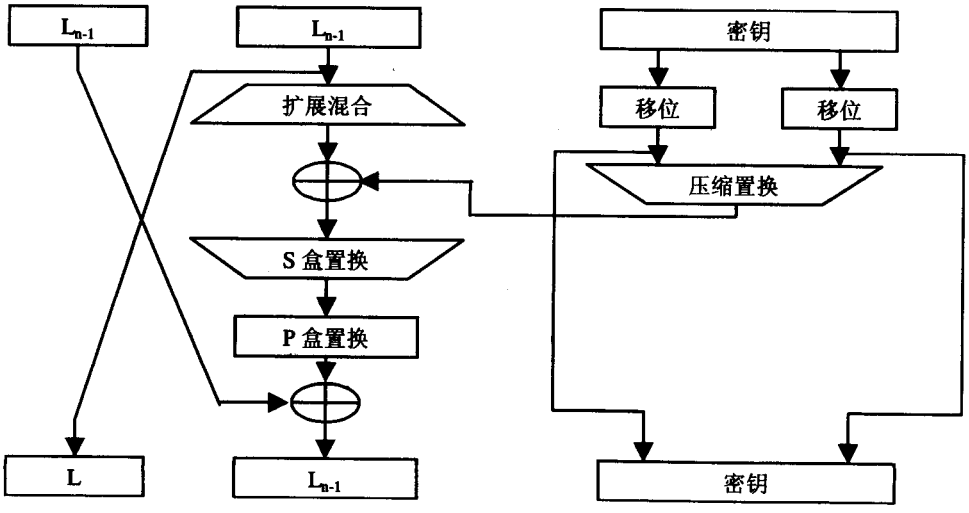


图 1-7 DES 每轮运算过程