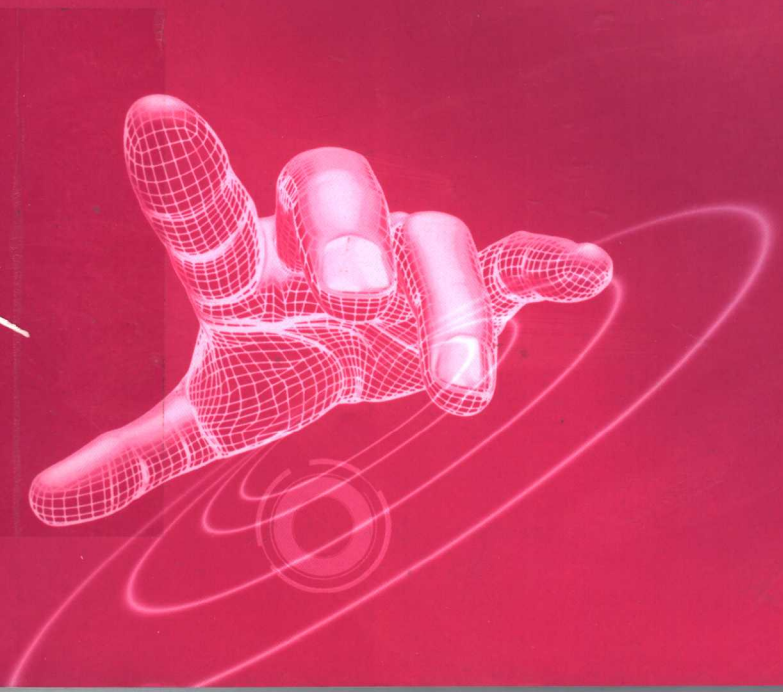
高等院校信息技术应用型特色教材

信息安全技术实验

王新昌　刘育楠　王鲁　编著



清华大学出版社

高等院校信息技术应用型特色教材

信息安全技术实验

王新昌　刘育楠　王鲁　编著

清华大学出版社
北京

内 容 简 介

本书以解决具体信息安全问题为目的，以信息安全保障体系为内容框架，由浅入深，由基础到综合，全面介绍了信息安全领域的实用技术及实验。全书共分7个单元。第1～3单元介绍信息保密、信息认证和访问控制等信息安全基本技术的相关实验，涵盖了信息加密、安全传输、口令和证书认证以及个人防火墙等内容。第4单元为系统平台安全实验，介绍Windows和Linux操作系统平台的安全配置和增强。第5单元介绍电子邮件、Web和FTP等典型的信息应用安全实验。第6单元介绍信息网络安全实验，主要包括网络侦查与扫描、网络攻击与防范以及入侵检测等实验。第7单元为信息安全综合保障实验，通过对VPN和防火墙产品进行部署、配置和使用，使读者从全方位建立起对信息安全保障体系的认识。

本书是掌握、实践和运用信息安全技术的一本实用指导书籍，能够帮助读者了解信息安全技术体系，掌握信息安全技术，掌握维护和强化信息系统安全的常用技术和手段，解决实际信息系统的安全问题。

本书既可作为高等院校信息安全及计算机相关专业本科及大专(高职)的专业教材，也可作为安全管理人员、网络管理人员、系统管理人员和其他相关技术人员的参考书。

图书在版编目(CIP)数据

信息安全技术实验/王新昌，刘育楠，王鲁编著. —北京：清华大学出版社，2007.9
高等院校信息技术应用型特色教材
ISBN 978-7-302-15648-2

Ⅰ. 信… Ⅱ. ①王… ②刘… ③王… Ⅲ. 信息系统－安全技术－高等学校－教材
Ⅳ. TP309

中国版本图书馆CIP数据核字(2007)第103377号

责任编辑：孟毅新
责任校对：袁　芳
责任印制：何　芊

出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦A座
http://www.tup.com.cn　　**邮　　编**：100084
c-service@tup.tsinghua.edu.cn
社 总 机：010-62770175　　**邮购热线**：010-62786544
投稿咨询：010-62772015　　**客户服务**：010-62776969

印 刷 者：北京鑫丰华彩印有限公司
装 订 者：三河市金元印装有限公司
经　　销：全国新华书店
开　　本：185×260　　**印　　张**：19.75　　**字　　数**：435千字
版　　次：2007年9月第1版　　**印　　次**：2007年9月第1次印刷
印　　数：1～4000
定　　价：27.00元

前 言

信息化是当今世界经济和社会发展的大趋势。信息化的发展已经、正在并且将进一步改变世界的政治、经济、军事、社会结构以及人们的生活方式，但随之而来的信息安全问题也越来越突出。信息安全威胁、信息安全和网络安全事件，大大降低了信息系统的安全性、可信性、可用性，严重干扰和影响了信息化建设的健康发展。面对这一现状，《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27号)中指出，加强信息安全技术研究开发，推进信息安全产业发展，加强信息安全法制建设和标准化建设，加快信息安全人才培养，增强全民信息安全意识是我国信息安全保障工作的主要任务。

信息工程大学电子技术学院是最早从事信息安全领域研究和教学的军事院校，在信息安全学科专业领域拥有一支学术水平高的专家队伍；承担了信息安全领域大量科研课题，取得了一系列科研成果；荣获了国家科技进步一等奖、军队科技进步一等奖等多项奖励；培养了大批合格人才，能够从事本科至博士研究生的多层次人才培养。为了适应当前信息安全人才培养的需要，更好地培养具有全面素质和能力的信息安全人才，根据多年的教学与科研积累，着手组织编写了这本《信息安全技术实验》。

本书以解决具体信息安全问题为目的，以信息安全保障体系为内容框架，以信息安全基本技术、系统平台安全技术、信息应用安全、信息网络安全及信息安全综合保障为主线，由浅入深，由基础到综合，全面介绍了信息安全领域的实用技术及实验。

本书主要有以下特点。

1. 系统性

信息安全技术涉及信息安全系统建设的各个方面。本书注重内容的系统性，以信息安全保障体系为内容框架，内容涵盖了信息保密技术、信息认证技术、访问控制技术、操作系统平台安全技术、邮件安全技术、防火墙技术、虚拟专用网 VPN 技术、网络侦查与扫描技术、网络攻击与防范技术以及入侵检测技术等，内容全面，体系完整。

2. 新颖性

为适应信息安全理论和技术发展迅速、知识更新快的特点，本书紧跟学科发展前沿，及时将信息安全领域的新技术、新手段和新工具融入内容体系，及时对信息安全体系进行扩充和完善。

3. 逻辑性

本书注重内容结构的逻辑性，围绕解决具体信息安全问题这一目的，由信息安全基本

实验引入，通过信息安全基本技术实验、信息平台安全实验、信息应用安全实验以及信息网络安全实验层层深入，最后以信息安全综合保障实验为结束，由浅入深，层次分明，有利于读者对信息安全技术的掌握和实践。

本书由解放军信息工程大学电子技术学院信息安全技术教研室组织编写。其中，第1、2、5、7、14章由刘育楠编写，第3、4、8章由王鲁编写，第6、9、10、11、12、13、15章由王新昌编写。全书由王新昌负责统稿，张红旗教授负责审稿。参与本书编写的人员还有张斌、汪永伟、代向东、杨智、包义保、杨艳、杜学绘、任志宇、王超、曹利峰等。

需要声明的是，编写本书的目的是帮助读者掌握信息安全技术，掌握维护和强化信息系统安全的常用技术和手段，解决实际信息系统的安全问题。但从另一个角度讲，本书中介绍的技术和工具可能含有攻击性或有害性。对于因技术或工具滥用所引起的安全问题，本书作者概不负责。

本书编写过程中，参考了因特网上信息安全相关的一些资料，从中得到了一些帮助。由于因特网资料繁多，引用复杂，无法一一注明，故在此声明，并表示衷心感谢。

信息安全学科内容广泛、发展迅速。由于作者水平有限，书中难免存在不足之处，敬请读者批评指正。

作　者

2007年9月

目 录

第 1 单元 信息保密技术实验

第 2 单元 信息认证技术实验

第 3 单元 访问控制技术实验

第 4 单元 系统平台安全实验

第 5 单元 信息应用安全实验

第 6 单元 信息网络安全实验

第 7 单元 信息安全综合保障实验

第1单元

信息保密技术实验

信息的加密变换是目前实现信息安全的基本手段之一，采用信息保密技术对信息进行保密处理是最常用、最有效的安全保护手段。信息保密技术是信息安全的基础内容，也被认为是信息安全的核心技术。在信息系统中采用信息保密技术的目的是保护信息的保密性、完整性和可用性。

研究信息加密和解密变换的学科称为密码学，密码学是信息保密技术的核心，它是一门古老而深奥的学科。从密码学的发展进程来看，它经历了古典密码、对称密钥密码和非对称密钥密码3个阶段。本单元中，第1章分别从密码算法和加解密工具两方面对信息保密技术进行实践，介绍了对称加密算法中的DES算法以及非对称加密算法中的RSA算法。通过实验使读者进一步理解信息保密技术的功能、作用、基本原理和实现机制。

除了使用传统加密技术实现信息的存储与传输安全外，随着Internet应用的增长，如何利用Internet这样的公共网络实现快捷安全的信息传输，成为各类用户，尤其是企业用户普遍关心的问题。虚拟专用网络(Virtual Private Network，VPN)就是解决这一问题的有效途径。VPN通过公共网络(如Internet)建立一个临时的安全连接，构建一条穿过公共网络的安全、稳定的隧道，为远程用户、企业分支机构、商业伙伴等建立可信的安全连接，确保数据的安全传输。本单元中，第2章分别对Windows和Linux下VPN的简单构建方法进行了介绍。

第 1 章

密 码 算 法

实验 1-1　对称密码算法 DES

一、实验目的

通过对 DES 算法进行分析，并使用 DES 算法对数据进行加密和解密，进一步理解 DES 的实现和加解密原理。

二、实验环境

运行 Windows 或 Linux 操作系统的计算机，具有 VC(Windows)、gcc(Linux)等 C 语言编译环境。

三、预备知识

1. 对称密码算法

根据采用的密钥类型，可将现有的加密算法分为两种：对称(单钥)密码算法和非对称(双钥或公钥)密码算法，前者如 DES，后者如 RSA。

对称密码算法的加解密使用的加密密钥和解密密钥相同，或者虽然不同，但可以从其中任意一个推导出另一个。对称密码的关键问题是将密钥安全地传送给参与保密通信的双方。对称加密算法要求通信双方在建立安全信道之前，约定好所使用的密钥。对于好的对称加密算法，其安全性完全决定于密钥的安全，算法本身是可以公开的，因此一旦密钥泄漏就等于泄漏了被加密的信息。对称算法是传统常用的算法，它最广泛使用的是 DES 算法。

2. DES 算法

DES(Data Encryption Standard，数据加密标准)算法原是 IBM 公司为保护产品的机密于 1971—1972 年研制成功的，后被美国国家标准局和国家安全局选为联邦信息加密标准，并于 1977 年颁布使用。ISO 也已将 DES 作为数据加密标准。DES 是世界上最早被公认的实用密码算法标准，多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，数据分组长度为 64 位(8 字节)，密文分组长度也是 64 位，没有数据扩展；密钥长度为 64 位，其中有 8 位为奇偶校验位，有效密钥长度为

56 位。DES 的整个体制是公开的，系统的安全性全靠密钥的保密。

1）DES 加密

（1）DES 加密流程

DES 算法处理的数据对象是一组 64 位的明文分组。设该明文分组为 $M=m_1m_2\cdots m_{64}$（$m_i=0$ 或 1）。明文分组经过 64 位的密钥 K 来加密，最后生成长度为 64 位的密文 E。其加密过程如图 1-1 所示。

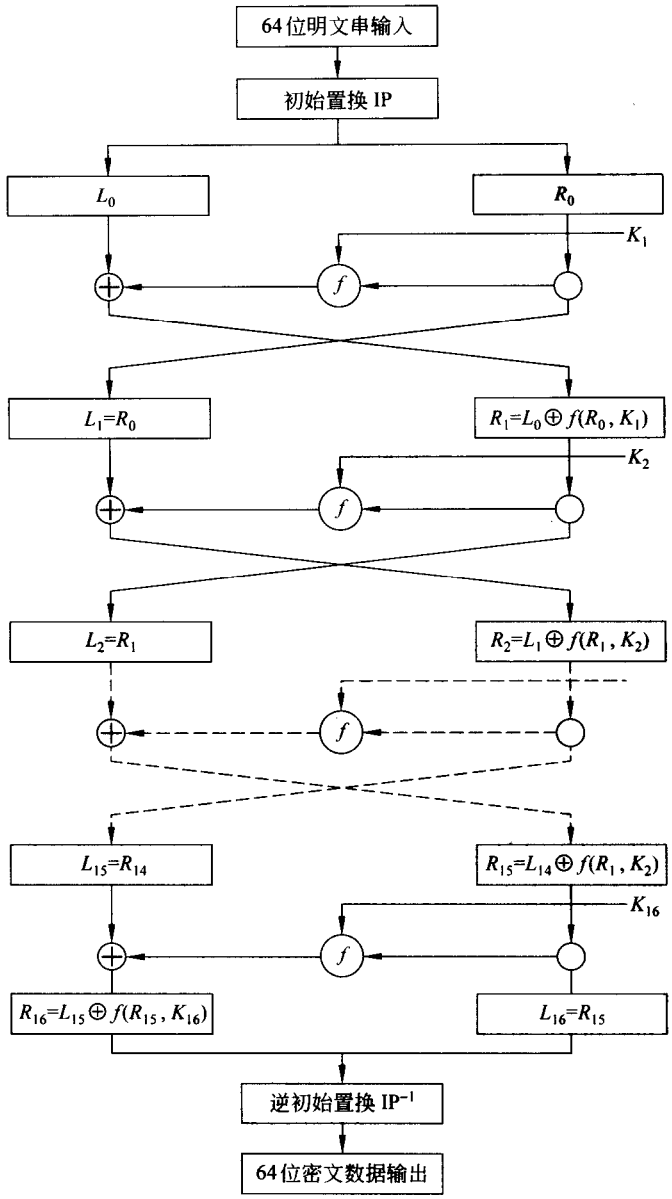


图 1-1　DES 加密流程

待加密的 64 位明文串 M，经过 IP 置换后，得到的比特串的下标列表如表 1-1 所示。

表 1-1　初始置换 IP

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

该分组被分为 32 位的 L_0 和 32 位的 R_0 两部分。R_0 与子密钥 K_1 经过变换 $f(R_0, K_1)$ 输出 32 位的位串 f_1，f_1 与 L_0 做不进位的二进制加法运算。运算规则为：

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

f_1 与 L_0 做不进位的二进制加法运算后的结果赋给 R_1，R_0 则原封不动地赋给 L_1。L_1 与 R_0 又做与以上完全相同的运算，生成 L_2，R_2。以此类推，一共经过 16 次运算，最后生成 R_{16} 和 L_{16}。其中 R_{16} 为 L_{15} 与 $f(R_{15}, K_{16})$ 做不进位二进制加法运算的结果，L_{16} 是 R_{15} 的直接赋值。

R_{16} 与 L_{16} 合并成 64 位的比特串。值得注意的是，R_{16} 一定要排在 L_{16} 前面。R_{16} 与 L_{16} 合并后生成的比特串，经过置换 IP^{-1} 后所得比特串的下标列表如表 1-2 所示。

表 1-2　逆初始置换 IP^{-1}

IP^{-1}	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
	33	1	41	9	49	17	57	25

经过置换 IP^{-1} 后生成的比特串即密文 E。

(2) f 变换

f 变换，即 $f(R_{i-1}, K_i)$ 函数，其功能是将 32 位的输入再转化为 32 位的输出。其过程如图 1-2 所示。

输入 R_{i-1}(32 位)，经过变换 E 后，扩展为 48 位。扩展后的位串的下标列表如表 1-3

所示。

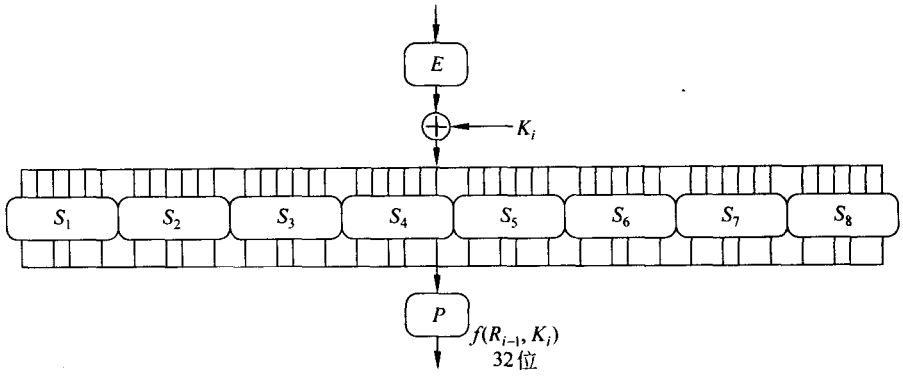


图 1-2　DES 算法中 f 变换流程

表 1-3　扩展后的位串下标

E	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	31

扩展后的位串分为 8 组，每组 6 位。各组经过各自的 S 盒后，又变为 4 位，合并后又成为 32 位。该 32 位经过 P 变换后，其下标列表如表 1-4 所示。

表 1-4　经过 *P* 变换后的位串下标

P	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

经过 P 变换后输出的位串即是 32 位的 $f(R_{i-1}, K_i)$。

(3) S 盒

下面讲解 S 盒的变换过程。任取一 S 盒，如图 1-3 所示。

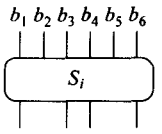


图 1-3　DES 中的 S 盒示意

在其输入 b_1、b_2、b_3、b_4、b_5 和 b_6 中，计算出 $x=b_1\times2+b_6$，$y=b_5+b_4\times2+b_3\times4+b_2\times8$，再从 S_i 表中查出 x 行、y 列的值 S_{xy}。将 S_{xy} 转换为二进制，即得 S_i 盒的输出。DES 中 8 个 S 盒如图 1-4 所示。

		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_1	0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	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
S_2	0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	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
S_3	0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	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
S_4	0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	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
S_5	0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	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
S_6	0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	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	13	11	6
	3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7	0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	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
S_8	0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	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

图 1-4　DES 中的 8 个 S 盒

2）DES 子密钥的生成

DES 算法中，由 64 位的密钥生成 16 个 48 位的子密钥。其生成过程如图 1-5 所示。

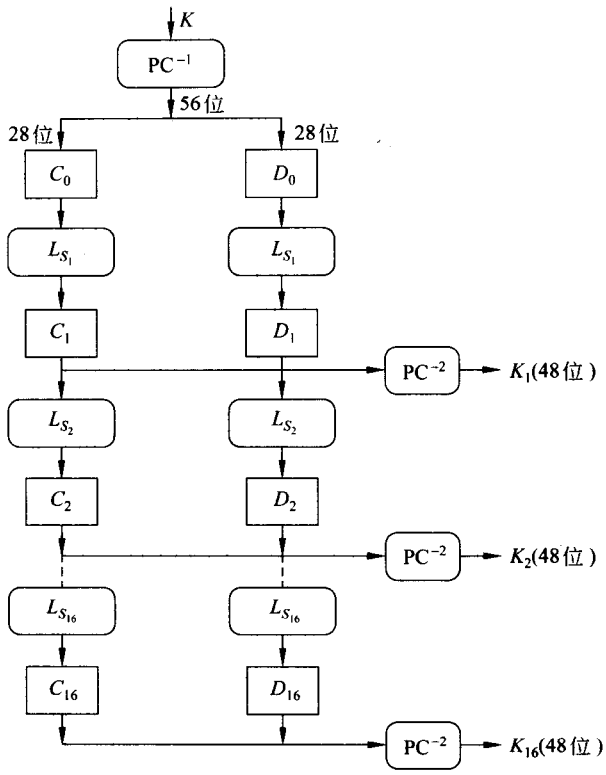


图 1-5　DES 算法子密钥的生成过程

子密钥生成过程具体解释如下：64 位的密钥 K，经过 PC^{-1} 后，生成 56 位的串。其下标如表 1-5 所示。

表 1-5　密钥 K 经 PC^{-1} 后的位串下标

PC^{-1}	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

该位串分为长度相等的位串 C_0 和 D_0。然后将 C_0 和 D_0 分别循环左移 1 位，得到 C_1 和

D_1。C_1和D_1合并起来生成C_1D_1，C_1D_1经过PC^{-2}变换后即生成 48 位的K_1。K_1的下标列表如表 1-6 所示。

表 1-6　密钥 K_1 的下标列表

PC^{-2}	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	32

C_1、D_1分别循环左移L_{S_2}位，再合并，经过PC^{-2}，生成子密钥K_2。以此类推，直至生成子密钥K_{16}。

注意：$L_{S_i}(i=1,2,\cdots,16)$的值是不同的，具体如表 1-7 所示。

表 1-7　$L_{S_i}(i=1,2,\cdots,16)$的值

迭代顺序	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
左移位数	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

3）DES 解密流程

DES 的解密过程和 DES 的加密过程完全类似，只不过将 16 圈的子密钥序列K_1，K_2，…，K_{16}的顺序倒过来。即第一圈用第 16 个子密钥K_{16}，第二圈用K_{15}，其余类推。DES 解密流程的第一圈运算如图 1-6 所示。

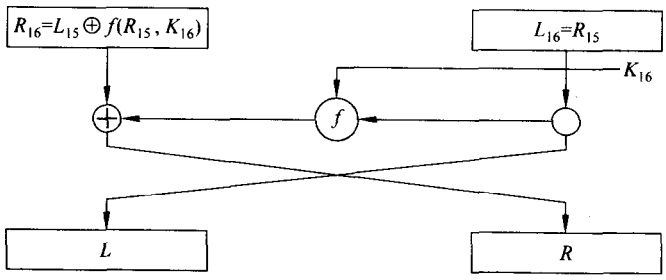


图 1-6　DES 解密流程的第一圈运算

DES 的实际密钥长度为 56 位。对 DES 最尖锐的批评之一是密钥太短。就目前计算机的计算机能力而言，DES 不能抵抗对密钥的穷举搜索攻击。

目前人们仍然不知道 DES 中是否存在陷门。所谓陷门，通俗地讲，就是设计者在算法的设计中留了一个后门，知道这一秘密的人可以进入这一后门获得使用该算法的用户