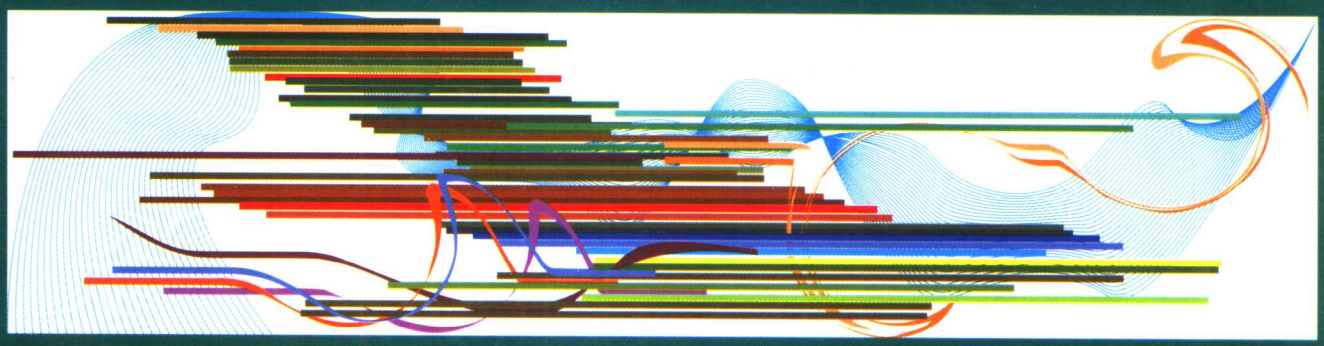
信息安全实验指导



崔宝江　周亚建　杨义先　钮心忻　编著

国防工业出版社
http://www.ndip.cn

信息安全实验指导

崔宝江　周亚建　杨义先　钮心忻　编著

国防工业出版社

·北京·

内 容 简 介

本书以解决和分析具体安全问题为目的，按照由浅入深、由局部到整体的思路，全面介绍了信息安全领域的实用技术和实验设计。全书共分四部分，第一部分和第二部分分别介绍了信息保密技术基础知识和网络基础知识，以使读者建立起信息安全和网络安全的基本概念。在第三部分按照从攻击到防御的思路，从网络和计算机资源的探测以及网络攻防技术入手，过渡到对安全防范技术的介绍，包括系统安全、网络和应用系统安全技术等。第四部分在前面各专项安全技术的基础上进行融合，介绍了网络安全整体解决方案的构建思路，以帮助读者从全方位建立起对网络安全系统整体架构的认识。

本书适合作为信息安全及其相关计算机专业本科高年级及其研究生的专业教材。同时，由于包含了极为丰富的信息及网络安全实用技术，也适合于企事业单位的网络管理人员、安全维护人员、系统管理人员和其它相关技术人员阅读参考。

图书在版编目(CIP)数据

信息安全实验指导 / 崔宝江等编著. —北京：国防工业出版社，2005.5
ISBN 7-118-03898-9

Ⅰ.信… Ⅱ.崔… Ⅲ.计算机网络—安全技术
Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字（2005）第 044573 号

国防工业出版社出版发行
（北京市海淀区紫竹院南路 23 号）
（邮政编码 100044）
北京奥鑫印刷厂印刷
新华书店经售
*
开本 787×1092 1/16 印张 29½ 686 千字
2005 年 5 月第 1 版 2005 年 5 月北京第 1 次印刷
印数：1—4000 册 定价：55.00 元(含光盘)

国防书店：**(010)68428422** 发行邮购：**(010)68414474**
发行传真：**(010)68411535** 发行业务：**(010)68472764**

前　言

随着近年来计算机和网络的迅速普及，给我国经济发展和社会进步带来了前所未有的机遇。但不容乐观的是，来自网络安全的威胁也日趋严重。例如，近年来多次在全球范围内爆发的蠕虫病毒，对社会经济造成了巨大的损失，因而，信息安全问题已经成为制约社会信息化发展的一个瓶颈。面对这一现状，如何提高我国的信息安全建设水平和网络安全的防范意识，已成为全社会共同关注的问题。为适应这一形式，教育部从2000年开始批准在高校中建立信息安全及其相关本科专业，以期为社会培养更多精通安全技术的专业人才。为了加深他们对信息安全知识的了解，进一步培养在信息安全方面的动手能力和感性认识，北京邮电大学信息安全中心组织编写了这本信息安全综合实验的实验指导书。

北京邮电大学信息安全中心是专门从事信息安全教学、科研成果转化的重点实验室。该中心已经培养出我国第一位密码学博士，并在“信息安全”和“密码学”两个专业领域内健全了博士后、博士、硕士和本科培养的教育体系，目前已培养出了数以百计的信息安全专业人才。为了促进和提高全国高校在信息安全领域内的教学科研水平，由北京邮电大学信息安全中心组织发起了“全国信息安全本科专业师资交流与培训互助组”（简称互助组），它将促进各个学校在信息安全及其相关本科专业的教学、实习、实验、科研等方面的交流和学习，积极开展人员与业务的交流和合作。目前，互助组成员单位已近百所，并多次组织了师资交流研讨会。

在互助组的多次交流中，我们在各位代表的建议和支持下，着手组织编写了这本《信息安全实验指导》。全书各章节的编写思路是由浅入深、由局部到整体。首先，在第一部分和第二部分分别介绍了信息保密技术和网络基础知识，以使读者建立起信息安全的基本概念。在第三部分按照从攻击到防御的思路，先从网络和计算机资源的探测以及网络攻防技术入手，再过渡到对安全防范技术的介绍，包括系统安全、网络和应用系统安全技术等。第四部分在前面各专项安全技术的基础上进行融合，介绍了网络安全整体解决方案的构建思路，以帮助读者全方位建立起对信息安全系统整体框架的认识。

在对各个实验的设计上，本书综合考虑了信息安全各个领域的内容，试图从多方位全面囊括信息安全领域的主要知识点。此外，考虑到不同学校千差万别的实验条件，我们的实验内容大部分基于很容易搭建的Windows和Linux操作系统的实验环境，充分降低了信息安全实验开设过程中的成本。同时，考虑部分有条件的高校对较高层次实验的需求，书中同时也设计了对软硬件有较高需求的复杂的大型实验，以期从成本高低和难

易程度等多方面满足不同学校的需求。本书全部讲授建议 51 学时，当然作为教材，授课教师可根据具体的实验室条件、专业情况和课时安排进行取舍。

本书全面介绍了密码学、信息隐藏、网络基础、网络嗅探、网络攻防、系统安全、Web 和 FTP 服务器安全、VPN、IDS、防火墙、CA 系统、AAA 认证等信息安全领域的基础知识。本书从实用技术入手，通过具体实验操作，帮助读者实际掌握和理解信息安全领域各个知识点的精髓。此外，通过设计和构建网络安全企业整体解决方案，从总体设计层面帮助读者把握构建安全网络系统的思路和方法。本书适合作为信息安全及其相关专业本科高年级及其研究生的专业教材，同时，由于包含了极为丰富的信息安全实用技术，也适合于企事业单位的网络管理人员、安全维护人员、系统管理人员和相关技术人员参考和阅读。

本书由北京邮电大学信息安全中心组织编写。其中，第 1、4、5、6、7、8 章由崔宝江编写，第 2、3 章由周亚建编写。全书由杨义先教授和钮心忻教授策划并参与了部分内容的编写。参与本书编写的人员还有牛冠杰、李晨旸、裴心蕊、原毅强、曹明、贾平平、韩坤、李菲菲等。在本书编写过程中得到了冯运波、罗群、徐国爱和周淑萍的鼎力支持，在此对他们表示衷心的感谢。

需要声明的是，编写本书的目的是希望帮助读者全面了解信息安全方面的基本技术，以期建立起安全方面的防范意识，决不是为怀有不良动机的人提供支持，也不承担因为技术被滥用而产生的连带责任。

本书在编写过程中参考了互联网上公布的一些相关资料，由于互联网上的资料较多，引用复杂，无法一一注明原出处，故在此声明，原文版权属于原作者。

由于作者水平有限，书中难免疏漏和错误之处，希望读者批评指正，以期再版时修订。

作　者

2005 年 3 月

目　录

第一部分　信息保密技术

第 1 章　信息保密技术 …… 2
实验 1-1　古典密码算法 …… 2
实验 1-2　对称密码算法 DES …… 3
实验 1-3　非对称密码算法 RSA …… 9
实验 1-4　Hash 算法 MD5 …… 12
实验 1-5　数字签名算法 DSS …… 17
实验 1-6　信息隐藏技术 …… 18

第二部分　网 络 基 础

第 2 章　网络设备基础 …… 28
实验 2-1　路由器使用入门 …… 28
实验 2-2　二层交换机的配置 …… 42
第 3 章　网络应用基础 …… 56
实验 3-1　在多个路由器之间建立连接 …… 56
实验 3-2　RIP 路由表的配置 …… 60
实验 3-3　NAT 的配置 …… 76
实验 3-4　VLAN 的划分和配置 …… 82

第三部分　网络和系统安全

第 4 章　计算机与网络资源的探测和扫描 …… 104
实验 4-1　使用 Sniffer 工具嗅探 …… 104
实验 4-2　网络端口扫描 …… 115
实验 4-3　综合扫描及安全评估 …… 124
第 5 章　网络攻防技术 …… 144
实验 5-1　账号口令破解 …… 144
实验 5-2　木马攻击与防范 …… 153
实验 5-3　DoS/DDoS 攻击与防范 …… 174

实验 5-4　缓冲区溢出攻击与防范……183
实验 5-5　计算机病毒的防范……189
第 6 章　系统安全……203
实验 6-1　Windows 操作系统安全……203
实验 6-2　Linux 操作系统安全……227
实验 6-3　Windows 中的 Web、FTP 服务器的安全配置……242
实验 6-4　Linux 中 Web、FTP 服务器的安全配置……254
第 7 章　网络和应用系统安全……269
实验 7-1　防火墙……269
实验 7-2　入侵检测系统……296
实验 7-3　虚拟专用网……312
实验 7-4　CA 系统及 SSL 的应用……358
实验 7-5　认证、授权和记账(AAA)服务……395

第四部分　网络安系统整体解决方案

第 8 章　网络安全系统整体解决方案……414
实验 8-1　基于 Window 的网络安全整体解决方案……414
实验 8-2　基于 Linux 系统的网络安全整体解决方案……429
实验 8-3　Cisco 的网络安全硬件集成解决方案……436
实验 8-4　国瑞数码公司的应用安全系统方案……443
参考文献……463

第一部分　信息保密技术

信息的加密变换是目前实现安全信息系统的主要手段，通过利用不同的加密技术可以对信息进行变换，从而实现信息的保密和隐藏。信息保密技术是信息安全的基础内容，本部分从密码算法和信息隐藏两方面对信息保密技术进行介绍，并通过具体实验加深读者对信息保密技术的理解。

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。按照发展进程来看，密码学经历了古典密码、对称密钥密码和非对称密钥密码 3 个阶段。本部分的前 3 个实验分别介绍了古典密码算法的替代加密算法、置换加密算法，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。

Hash 算法和数字签名也是密码学研究的重要内容。Hash 算法将任意长度的输入变换成固定长度的输出。数字签名模拟了传统文件的手写签名，能够实现用户对电子信息的认证。本部分的第 4 个实验和第 5 个实验分别介绍了 Hash 算法中的 MD5 算法及数字签名算法中的 DSA 算法。

信息隐藏技术作为新一代的信息安全技术，在当代保密通信领域起着越来越重要的作用。它将有用的信息隐藏在其它信息中，从而使攻击者无法发现，不仅实现了信息的保密，也隐藏了信息的内容。本部分第 6 个实验介绍了信息隐藏技术的基本原理，并详细介绍了 LSB（最低比特位）信息隐藏算法和 DCT（离散余弦变换）域隐藏算法等两种信息隐藏算法的实现过程。

第 1 章　信息保密技术

实验 1-1　古典密码算法

一、实验目的

通过编程实现替代密码算法和置换密码算法，加深对古典密码体制的了解，为深入学习密码学奠定基础。

二、实验原理

古典密码算法曾被广泛应用，大都比较简单，使用手工和机械操作来实现加密和解密。它的主要应用对象是文字信息，利用密码算法实现文字信息的加密和解密。下面介绍两种常见的具有代表性的古典密码算法，以帮助读者对密码算法建立一个初步的印象。

1. 替代密码

替代密码算法的原理是使用替代法进行加密，就是将明文中的字符用其它字符替代后形成密文。例如，明文字母 a、b、c、d，用 D、E、F、G 做对应替换后形成密文。

替代密码包括多种类型，如单表替代密码、多明码替代密码、多字母替代密码、多表替代密码等。下面我们介绍一种典型的单表替代密码——恺撒(Caesar)密码，又叫循环移位密码。它的加密方法就是将明文中的每个字母用此字符在字母表中后面第 k 个字母替代。它的加密过程可以表示为下面的函数：

$$E(m)=(m+k) \bmod n$$

其中，m 为明文字母在字母表中的位置数；n 为字母表中的字母个数；k 为密钥；E(m)为密文字母在字母表中对应的位置数。

例如，对于明文字母 H，其在字母表中的位置数为 8，设 k=4，则按照上式计算出来的密文为 L，计算过程如下：

$$E(8) = (m+k) \bmod n = (8+4) \bmod 26 = 12 = L$$

2. 置换密码

置换密码算法的原理是不改变明文字符，只将字符在明文中的排列顺序改变，从而实现明文信息的加密。置换密码有时又称为换位密码。

矩阵换位法是实现置换密码的一种常用方法。它将明文中的字母按照给定的顺序安排在一个矩阵中，然后用根据密钥提供的顺序重新组合矩阵中的字母，从而形成密文。例如，明文为 attack begins at five，密钥为 cipher，将明文按照每行 6 个字母的形式排在矩阵中，形成如下形式：

a	t	t	a	c	k
b	e	g	i	n	s
a	t	f	i	v	e

根据密钥 cipher 中各字母在字母表中出现的先后顺序，给定一个置换：

$$f=\begin{bmatrix}1&2&3&4&5&6\\1&4&5&3&2&6\end{bmatrix}$$

根据上面的置换，将原有矩阵中的字母按照第 1 列、第 4 列、第 5 列、第 3 列、第 2 列、第 6 列的顺序排列、则有下面的形式：

a	a	c	t	t	k
b	i	n	g	e	s
a	i	v	f	t	e

从而得到密文：abatgftetcnvaiikse

其解密的过程是根据密钥的字母数作为列数，将密文按照列、行的顺序写出，再根据由密钥给出的矩阵置换产生新的矩阵，从而恢复明文。

三、实验环境

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

四、实验内容和步骤

(1) 根据实验原理部分对替代密码算法的介绍，自己创建明文信息，并选择一个密钥，编写替代密码算法的实现程序，实现加密和解密操作。

(2) 根据实验原理部分对置换密码算法的介绍，自己创建明文信息，并选择一个密钥，编写置换密码算法的实现程序，实现加密和解密操作。

五、实验报告要求

要求上述密码算法最后的实现程序提供加密和解密两个接口：int encrypt ( )和 int decrypt ()。当加密或者解密成功时返回 CRYPT_OK，失败时返回 CRYPT_ERROR。

实验 1-2　对称密码算法 DES

一、实验目的

通过用 DES 算法对实际的数据进行加密和解密来深刻了解 DES 的运行原理。

二、实验原理

信息加密根据采用的密钥类型可以划分为对称密码算法和非对称密码算法。对称密码算法是指加密系统的加密密钥和解密密钥相同，或者虽然不同，但是可以从其中任意一个推导出另一个，更形象的说就是用同一把钥匙开锁和解锁。在对称密码算法的发展历史中曾出现过多种优秀的算法，包括 DES、3DES、AES 等。下面我们以 DES 算法为例介绍对称密码算法的实现机制。

DES 算法是由美国 IBM 公司在 20 世纪 70 年代提出，并被美国政府、美国国家标准局和美国国家标准协会采纳和承认的一种标准加密算法。它属于分组加密算法，即在

明文加密和密文解密过程中，信息都是按照固定长度分组后进行处理的。混淆和扩散是它采用的两个最重要的安全特性。混淆是指通过密码算法使明文和密文以及密钥的关系非常复杂，无法从数学上描述或者统计。扩散是指明文和密钥中每一位信息的变动，都会影响到密文中许多位信息的变动，从而隐藏统计上的特性，增加密码的安全。

DES 算法将明文分成 64 位大小的众多数据块，即分组长度为 64 位。同时用 56 位密钥对 64 位明文信息加密，最终形成 64 位的密文。如果明文长度不足 64 位，则将其扩展为 64 位(如补零等方法)。具体加密过程首先是将输入的数据进行初始换位(IP)，即将明文 M 中数据的排列顺序按一定的规则重新排列，生成新的数据序列，以打乱原来的次序。然后将变换后的数据平分成左右两部分，左边记为 L_0，右边记为 R_0，然后对 R_0 实行在子密钥(由加密密钥产生)控制下的变换 f，结果记为 $f(R_0, K_1)$，再与 L_0 做逐位异或运算，其结果记为 R_1，R_0 则作为下一轮的 L_1。如此循环 16 轮，最后得到 L_{16}、R_{16}，再对 L_{16}、R_{16} 实行逆初始置换 IP^{-1}，即可得到加密数据。解密过程与此类似，不同之处仅在于子密钥的使用顺序正好相反。

DES 全部 16 轮的加密过程如图 1-1 所示。

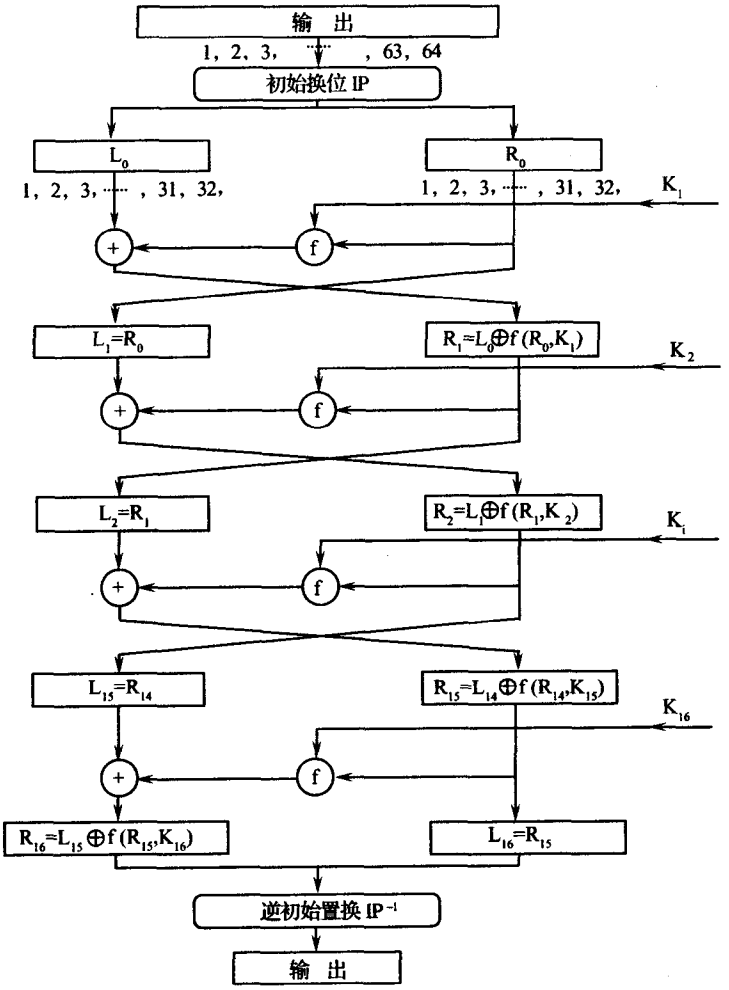


图 1-1 DES 加密/解密流程

DES 的加密算法包括 3 个基本函数。

1. 初始换位(IP)

它的作用是把输入的 64 位数据块的排列顺序打乱，每位数据按照下面换位规则重新组合，即将第 58 位换到第 1 位，第 50 位换到第 2 位，……，依次类推。重组后的 64 位输出分为 L_0、R_0(左、右)两部分，每部分分别为 32 位。

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

R_0 和 K_1 经过 $f(R_0, K_1)$变换后的输出结果，再和 L_0 进行异或运算，输出结果做为 R_1，R_0 则赋给 L_1。L_1 和 R_1 同样再做类似运算生成 L_2 和 R_2,……，经过 16 次运算后生成 L_{16} 和 R_{16}。

2. f 函数

f 函数是多个置换函数和替代函数的组合函数，它将 32 位比特的输入变换为 32 位的输出，如图 1-2 所示。R_i 经过扩展运算 E 变换后扩展为 48 位的 $E(R_i)$，与 K_{i+1} 进行异或运算后输出的结果分成 8 组，每组 6 比特的并联 B，$B=B_1B_2B_3B_4B_5B_6B_7B_8$，再经过 8 个 S 盒的选择压缩运算转换为 4 位，8 个 4 位合并为 32 位后再经过 P 变换输出为 32 位的 $f(R_i, K_{i+1})$。其中，扩展运算 E 与置换 P 主要作用是增加算法的扩散效果。

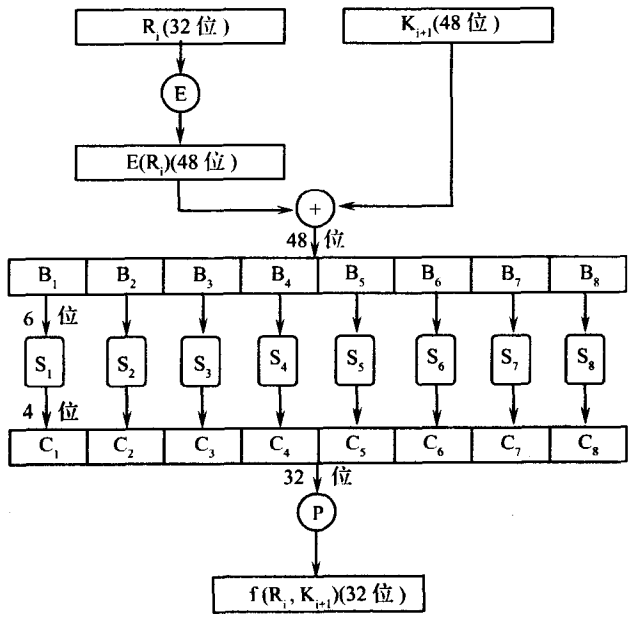


图 1-2　DES 算法中 f 函数的处理流程

3. 逆初始置换函数 IP^{-1}

它将 L_{16} 和 R_{16} 作为输入，进行逆初始换位得到密文输出。逆初始换位是初始换位的逆运算，换位规则如下所列：

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

DES 的加密算法中除了上面介绍的 3 个基本函数，还有一个非常重要的功能模块，即子密钥的生成模块，具体子密钥的产生流程如图 1-3 所示。

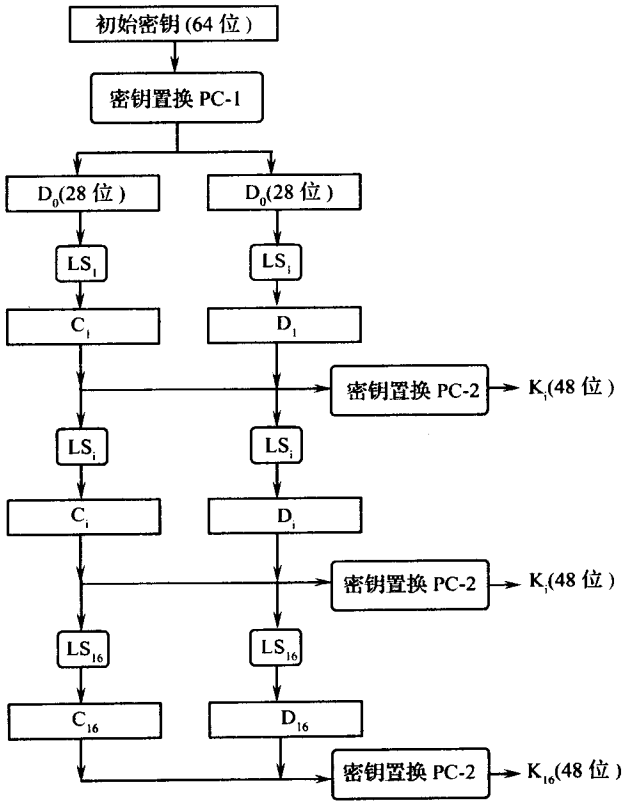


图 1-3　子密钥的产生流程

输入的初始密钥值为 64 位，但 DES 算法规定，其中第 8、16、……、64 位是奇偶校验位，不参与 DES 运算。所以，实际可用位数只有 56 位，经过缩小选择换位表 1(表 1-2)即密钥置换 PC-1 的变换后，初始密钥的位数由 64 位变成了 56 位，将其平分为两部分 C_0、D_0，然后分别进行第 1 次循环左移，得到 C_1、D_1，将 C_1(28 位)、D_1(28 位)合并后得到 56 位的输出结果，再经过缩小选择换位表 2(表 1-3)即密钥置换 PC-2，从而得到了密钥 K_1(48 位)。依次类推，便可得到 K_2、……、K_{16}。需要注意的是，16 次循环左移对应的左移位数要依据表 1-1 的规则进行。

表 1-1　左移位数规则

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
LS_i	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

表 1-2　缩小选择换位表 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

表 1-3　缩小选择换位表 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

三、实验环境

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

四、实验内容和步骤

1. 算法分析

在光盘中附加了有关 DES 算法的程序，根据所提供的程序分析 DES 算法的实现过程。DES 程序包括一个头文件和一个实现 DES 算法的 C 文件。头文件里主要是一些宏定义和函数声明，其中还包括保证可移植性的一些定义。DES 程序通过宏定义可选择小代码模式(#define small_code)或者选择大代码模式。在大代码模式下，程序定义了多个表，从而使 DES 算法中的很多运算都可以通过查表实现，速度较快，但要求有较多的存储空间；在小代码模式运行时，可以不查表，从而节省了存储空间，但是速度较慢。读者可以根据自己的需求来选择不同的运行模式。

加密解密时主要用到下面 5 个函数。

(1) int des_setup(const unsigned char *key, int keylen, int num_rounds, des_key *skey)

函数名称：密钥生成函数。

参数说明：

key 是一个指针，指向用户输入的初始密钥。

keylen 是输入密钥的长度，以字节为单位。

num_rounds 是加密轮数，当输入 0 时，使用算法默认的轮数。

skey 是一个指向结构体变量的指针，变量里面存储加密和解密时每轮使用的子密钥。

当密钥生成时，返回值为 CRYPT_OK(0)，结果保留在 skey 指向的结构体。

des_key 的定义如下：

typedef struct des_key{

ulong32 ek[32], dk[32];

}des_key;

结构体里的 ek 存储加密时用的子密钥，dk 存储解密时用的子密钥。

结构体中用 2 个 32 位的整数来存储一轮的 48 位密钥，每一个 32 位整数被分成 4 个 8 位，每个 8 位的第 6 位存储密钥。如果把 48 位密钥分成 8 组，则这 8 组按存储的顺序从高到低分别为 1、3、5、7、2、4、6、8。这样做是为了加密时可以把扩展和查表运算结合进行。

(2) void des_ecb_encrypt(const unsigned char *pt, unsigned char *ct, des_key *key)

函数名称：加密函数。

参数说明：

pt 是指向待加密的明文数组的指针。

ct 是指向存储加密结果的指针。

key 是调用密钥生成函数后存储每一轮子密钥的结构体变量。

加密成功时，返回 CRYPT_OK。

(3) void des_ecb_decrypt(const unsigned char *ct, unsigned char *pt, des_key *key)

函数名称：解密函数。

参数说明：

ct 是指向待解密的密文数组的指针。

pt 是指向存储解密结果的指针。

key 是调用密钥生成函数后存储每一轮子密钥的结构体变量。

解密成功时，返回 CRYPT_OK。

加密和解密时，pt 和 ct 可以指向同一块内存。

(4) int des_test(void)

函数名称：测试函数。

这个函数用来对加密算法进行测试。函数体内部定义了对应的明文和密文数组，并且进行了多轮加密和解密。这个函数还可以用来测试函数的运行时间。

(5) int des_keysize(int *desired_keysize)

函数名称：密钥长度检验函数。

参数说明：

desired_keysize 是使用者所想要的密钥长度。

当密钥长度小于所需密钥长度时，返回值为 CRYPT_INVALID_KEYSIZE，否则，desired_keysize 指向的变量被置为 8。

2. 使用实例分析

```
#include"des.h"

int main(int argc, char *argv[])
{
  unsigned char pt[9]="abcdefgh",ct[9],key[8]={'a','b','c','d','a','b','c','d'};
des_key skey;
  pt[9]=ct[9]='\0';
```

```
  des_setup(key,8,0,&skey);
  des_ecb_encrypt(pt,ct,&skey);
  des_ecb_decrypt(ct,pt,&skey);
  printf("%s\n",pt);
  printf("%s\n",ct);

  system("PAUSE");
  return 0;
}
```

说明：这个程序演示了对一组 8Byte 的数据进行加密和解密的过程。pt 指向明文数组，ct 指向密文数组，skey 是密钥数组。pt 和 ct 数组长度设为 9，是为了方便控制台字符串输出。对文件加密时，可以指定读取和写入的字符数，这两个数组长度应该定义为 8。

五、实验报告要求

(1) 使用光盘附录提供的程序对一个文件进行加密和解密，提交程序代码和执行结果。

(2) 使用光盘附录提供的程序对输入的十六进制数加密(把输入的字符转化成整数。例如，输入两个字符 1F，转化成二进制数 00011111)，比较输入和输出。当把输入的数改变一个位时(如把 1F 变为 1E)，比较输出的变化，并说明原因。

实验 1-3　非对称密码算法 RSA

一、实验目的

通过实际编程了解非对称密码算法 RSA 的加密和解密过程，加深对非对称密码算法的认识。

二、实验原理

前面讲的对称密码算法要求通信双方通过交换密钥实现使用同一个密钥，这在密钥的管理、发布和安全性方面存在很多问题，而非对称密码算法解决了这个问题。

非对称密码算法是指一个加密系统的加密密钥和解密密钥是不同的，或者说不能用其中一个推导出另一个。在非对称密码算法的两个密钥中，一个是用于加密的密钥，它是可以公开的，称为公钥；另一个是用于解密的密钥，是保密的，称为私钥。非对称密码算法解决了对称密码体制中密钥管理的难题，并提供了对信息发送人的身份进行验证的手段，是现代密码学最重要的发明。

RSA 密码体制是目前为止最成功的非对称密码算法，它是在 1977 年由 Rivest、Shamir 和 Adleman 提出的第一个比较完善的非对称密码算法。它的安全性是建立在“大数分解和素性检测”这个数论难题的基础上，即将两个大素数相乘在计算上容易实现，而将该乘积分解为两个大素数因子的计算量相当大。虽然它的安全性还未能得到理论证明，但

经过 20 多年的密码分析和攻击，迄今仍然被实践证明是安全的。

RSA 算法描述如下：

1. 公钥

选择两个互异的大素数 p 和 q，n 是二者的乘积，即 n = pq，使Φ(n)=(p-1)(q-1)，Φ(n)为欧拉函数。随机选取正整数 e，使其满足 gcd(e，Φ(n))=1，即 e 和Φ(n)互质，则将(n,e)作为公钥。

2. 私钥

求出正数 d，使其满足 e×d=1 mod Φ(n)，则将(n,d)作为私钥。

3. 加密算法

对于明文 M，由 $C=M^e \bmod n$ ，得到密文 C。

4. 解密算法

对于密文 C，由 $M=C^d \bmod n$，得到明文 M。

如果窃密者获得了 n、e 和密文 C，为了破解密文必须计算出私钥 d，为此需要先分解 n。为了提高破解难度，达到更高的安全性，一般商业应用要求 n 的长度不小于 1024 位，更重要的场合不小于 2048 位。

三、实验环境

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

四、实验内容和步骤

(1) 为了加深对 RSA 算法的了解，根据已知参数：p=3，q=11，M=2，手工计算公私钥，并对明文进行加密，然后对密文进行解密。

(2) 光盘中给出了一个可以进行 RSA 加密和解密的对话框程序 RSATool，运行这个程序加密一段文字，了解 RSA 算法原理。尝试着加密一大段文字，记录程序的运行时间。使用 DES 算法加密相同的文字，比较两种算法加密的速度。

五、实验报告要求

(1) 编写一个程序，随机选择 3 个较大的数 x、e、n，然后计算 $x^e \bmod n$，记录程序运行时间。实际中应用的素数为 512 位，n 也就为 1024 位。这样的大数在计算机上如何表示、如何进行运算，查阅资料给出简单说明。

(2) 计算机在生成一个随机数时，并不一定就是素数，因此要进行素性检测。是否有确定的方法判定一个大数是素数，要查阅资料，找出目前实际可行的素数判定法则，并且比较各自的优缺点。

(3) 光盘附录中给出了一个密码算法库，其中包括各种对称加密算法、非对称加密算法、Hash 算法和数字签名算法。找出其中关于 RSA 算法的部分，并且基于标准输入输出写一段用 RSA 加密文件的程序。

下面是有关 RSA 接口调用的示例程序，写程序时可以参考。

```
#include <mycrypt.h>
```