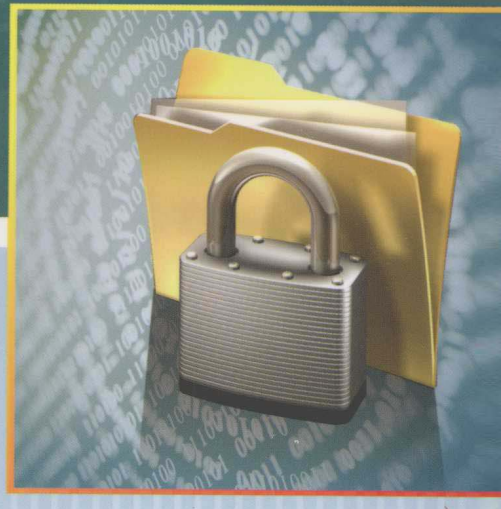
普通高等学校计算机科学与技术专业规划教材

信息安全综合实验

INFORMATION SECURITY SYNTHESIS EXPERIMENT

蒋朝惠　武　彤　邓少勋　王晓鹏　编著

光盘内附部分源代码



中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

普通高等学校计　　专业规划教材

信息安全综合实验

蒋朝惠　武　彤　邓少勋　王晓鹏　编著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

本书是为满足现代密码学、信息安全原理与技术、网络安全、计算机病毒原理与防治、网络攻击与防范、网络程序设计、数据库系统安全、操作系统安全、数据备份与恢复技术等信息安全专业课程实践教学需要而编写的一本实验指导书。

本书以操作性和设计性实验为主，内容丰富，图文并茂，所有实验步骤和程序代码都通过实际操作与调试，对提高读者的实际操作和动手能力很有帮助。另外，本书的相关素材、部分章节实验所需的环境软件与样例程序源代码均可从附书光盘中找到。

本书可作为计算机专业本科学生的教材，也可作为信息安全、通信工程和网络工程等相关专业的本科生、研究生教材，还可供企事业单位的网络管理人员、安全维护人员和系统管理人员以及其他相关科研与工程技术人员参考。

图书在版编目（CIP）数据

信息安全综合实验 / 蒋朝惠等编著. —北京：中国铁道出版社，2010.8
普通高等学校计算机科学与技术专业规划教材
ISBN 978-7-113-09804-9

Ⅰ.①信… Ⅱ.①蒋… Ⅲ.①信息系统－安全技术－高等学校－教材 Ⅳ.①TP309

中国版本图书馆 CIP 数据核字（2010）第 018453 号

书　　名：信息安全综合实验
作　　者：蒋朝惠　武　彤　邓少勋　王晓鹏　编著

策划编辑：秦绪好　杨　勇
责任编辑：秦绪好　　**编辑部电话：**（010）63583215
编辑助理：巨　凤　　**特邀编辑：韩玉彬**
封面设计：付　巍　　**封面制作：白　雪**
版式设计：郑少云　　**责任印制：李　佳**

出版发行：中国铁道出版社（北京市宣武区右安门西街 8 号　　邮政编码：100054）
印　　刷：北京新魏印刷厂
版　　次：2010 年 8 月第 1 版　　2010 年 8 月第 1 次印刷
开　　本：787mm×1092mm　1/16　　**印张：**20.5　　**字数：**503 千
印　　数：3 000 册
书　　号：ISBN 978-7-113-09804-9
定　　价：34.80 元（附赠光盘）

普通高等学校计算机科学与技术专业规划教材

编审委员会

序言

PREFACE

计算机学科虽然是一门年轻的学科，但它已经成为一门基础技术学科，在各个学科发展中扮演着重要的角色。因此，社会产生了对计算机科学与技术专业人才的巨大需求。目前，计算机科学与技术专业已成为我国理工专业中规模最大的专业，为高等教育发展做出了巨大贡献。近些年来，随着国家信息化建设的推进，作为核心技术的计算机技术，更是占有重要的地位。信息化建设不仅需要更先进、更便于使用的先进计算技术，同时也需要大批的建设人才。瞄准社会需求准确定位，培养计算机人才，是计算机科学与技术专业及其相关专业的历史使命，也是实现专业教育从劳动就业供给导向型向劳动就业需求导向型转变的关键，从而也就成为提高高等教育质量的关键。

教材在人才培养中占有重要地位，承担着“重要的责任”，这就确定了“教材必须高质量”这一基本要求。社会对计算机专业人才需求的多样性和特色，决定了教材建设的针对性，从而也造就了百花齐放、百家争鸣的局面。

关于高质量教材建设，教育部在提高本科教育质量的文件中都提出了明确要求。教高〔2005〕1号（2005年1月7日）文件指出，“加强教材建设，确保高质量教材进课堂。要大力锤炼精品教材，并把精品教材作为教材选用的主要目标。”“要健全、完善教材评审、评价和选用机制，严把教材质量关。”为了更好地落实教育部的这些要求，我们按照教育部高等学校计算机科学与技术教学指导委员会发布的《高等学校计算机科学与技术专业发展战略研究报告暨专业规范（试行）》所构建的计算机科学与技术专业本科教育的要求，组织了这套教材。

作为优秀教材的基础，我们首先坚持高标准，以对教育负责的精神去鼓励、发现、动员、选拔优秀作者，并且有意识地培育优秀作者。优秀作者保证了“理论准确到位，既有然，更有所以然；实践要求到位、指导到位”等要求的实现。

其次是按照人才培养的需要适当强调学科形态内容。粗略地讲：计算机科学的根本问题是“什么能被有效地自动计算”，科学型人才强调学科抽象和理论形态的内容；计算机系统工程的根本问题应该是“如何低成本、高效地实现自动计算”，工程型人才强调学科抽象和设计形态的内容；计算机应用的根本问题是“如何方便、有效地利用计算机系统进行计算”，应用型人才的培养偏重于技术层面的内容，强调学科设计形态的内容，在进一步开发基本计算机系统应用的层面上体现学科技术为主的特征。教材针对不同类型人才的培养，在满足基本知识要求的前提下，强调不同形态的内容。

第三是重视知识的载体作用，促进能力培养。在教材内容的组织上，体现大学教育的学科性和专业性特征，参考《高等学校计算机科学与技术专业发展战略研究报告暨专业规范（试行）》示例性课程大纲，覆盖其要求的基本知识单元。叙述上力争引导读者进行深

入分析，努力使读者在知其然的基础上，探究其所以然。通过加强对练习和实践的引导，进一步培养学生的能力，促使相应课程在专业教育总目标的实现中发挥作用。

第四是瞄准教学需要，提供更多支持。近些年来，随着计算机技术、网络技术等在教学上的应用，教学手段、教学方式不断丰富，教材的立体化建设对丰富教学资源发挥了重要作用。通常，除主教材外，还要配套教学参考书、实验指导书、电子讲稿，有的还提供网络教学服务，等等。

第五是面向主要读者，强调教材的写作特征，努力做到叙述清晰易懂，语言流畅，深入浅出，有吸引力而不晦涩；追求描述的准确性，强调用词和描述的一致性，语言表达的清晰性和叙述的完整性；分散难点，循序渐进，防止多难点、多新概念的局部堆积。

我们相信，这套教材一定能够在培养社会需要的计算机专业人才上发挥重要作用，希望大家广为选用，并在使用中提出宝贵建议，使其内容不断丰富。

普通高等学校计算机科学与技术专业规划教材编审委员会

前言

FOREWORD

随着计算机技术与网络通信技术以及信息产业的高速发展，接入 Internet 的个人和单位主机数量快速增长，网络与信息安全已上升为一个事关国家主权、政治稳定、社会安定、经济有序运行和精神文明建设的全局性问题。信息安全已成为信息科学的热点课题，信息安全专业也受到了社会各界的普遍关注。

我国从 2000 年开始批准在高校中建立信息安全本科专业，以期为社会培养更多的精通信息安全技术的专业人才。在信息安全专业课程体系中，相关专业课程的理论性很强，有很多知识如果缺乏必要的实验很难理解与掌握。为了加深对信息安全专业相关课程知识的学习，培养与提高学生的动手能力和感性认识，借鉴了国内先进院校的相关专业实验教学内容，我们结合多年教学经验编写了本实验指导书。

全书共 8 章。第 1 章介绍了对称密码、非对称密码、报文摘要、数字签名、信息隐藏等密码算法方面的实验。第 2 章介绍了 Windows 与 Linux 操作系统、SQL Server 和 Oracle 数据库系统等系统安全方面的实验。第 3 章介绍了地址转换（NAT）、虚拟局域网（VLAN）、防火墙（FW）、入侵检测系统（IDS）、虚拟专用网（VPN）、网络蜜罐（Honeypot）等网络安全方面的实验。第 4 章介绍了 PGP 电子邮件系统、Windows CA 系统、基于 Web 的 SSL 应用和 Kerberos 认证系统等应用安全方面的实验。第 5 章介绍了宏、脚本、蠕虫等病毒原理与防治方面的实验。第 6 章介绍了 Ghost 和 EasyRecovery 等常用文件与数据备份与恢复工具实验、SQL Server 与 Oracle 数据库备份与恢复实验；第 7 章介绍了网络嗅探、漏洞与端口扫描等常用网络安全工具、木马、拒绝服务（DoS/DDoS）、缓冲区溢出、欺骗（ARP/DNS）、账号等网络攻击与防范方面的实验。第 8 章介绍了注册表、文件系统、驻留程序、客户/服务器通信和网络文件传输等网络编程方面的实验。另外，随本书附有一张光盘，内有部分章节实验所需的环境软件与样例程序源代码以及信息安全基础操作（包括 ping、traceroute、nslookup、netsh、net、ipconfig、netstat、arp、at、cacls、Windows 网络监视器、网卡 MAC 地址修改、通信对方的 IP 地址查看、PSTools 等常用命令与管理工具）。

全书由蒋朝惠、武彤、邓少勋、王晓鹏编者。第 4 章和第 7 章由蒋朝惠编写；第 2 章 2.3 节和第 6 章由武彤编写；第 2 章 2.1 节与 2.2 节、第 5 章和第 8 章由邓少勋编写；第 1 章和第 3 章由王晓鹏编写。祁振杰、马国彬、沈洁、李悦等人对本书做了一些图表绘制、程序调试、校对和纠错等工作。

本书的编写得到了贵州省工业攻关项目（合同号为黔科合 GY 字[2006]3019）和贵州省高层次人才特助经费项目（TZJF-2007-26）和贵州大学 2010 年规划教材项目的资助。

需要声明的是，本书介绍了一些网络攻击原理方面的实验，目的是希望让读者更好地进行防范，决不是为网络攻击者提供技术支持，也不承担因为技术被滥用而产生的连带责任。另外，在本书的编写过程中参考了一些出版物和因特网资料，主要参考书已在书后“参考文献”中列出，但由于资料较多且时效性强，无法一一注明原出处，故在此声明，原文版权属于原作者。

在此，我们特别感谢这些作者们为我们提供了丰富的编写素材，是你们的优秀思想与研究成果帮助我们完成了本书的编写工作。最后感谢在本书的编写和出版过程中付出辛勤劳动的所有老师与朋友们。

虽然我们的目标是编写一套优秀的教材，但是，由于水平有限，时间仓促，不足之处在所难免，恳请读者和同行专家批评指正。

编　者

2010 年 6 月

CONTENTS

目录

第1章 密码算法实验

1.1 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。本节将介绍 DES、triple-DES、AES 这 3 种优秀对称密码算法的原理与实现方法。

1.1.1 DES 算法

一、实验目的

① 了解 DES 算法的基本原理。

② 熟悉 DES 算法的编程实现方法。

二、实验原理

1973 年 5 月，美国国家标准局发出通知，公开征求对计算机数据在传输和存储期间进行数据加密的算法。1975 年 IBM 公司提出了 DES 算法，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。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。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 算法是将二进制序列的输入明文，以 64 位为数据分组，然后用 56 位密钥对这些明文进行替换和换位，最后形成密文。如果明文长度不足 64 位，则将其扩展为 64 位（如补零等方法）。DES 的具体加密过程如图 1-1 所示。

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} 实行逆初始换位 IP^{-1}，即可得到加密数据。解密过程与此类似，不同之处在于子密钥的使用顺序正好相反。

表 1-1 和表 1-2 所示为初始换位 IP 和逆初始换位 IP^{-1}。初始换位 IP 是将 $T=t_1t_2t_3\cdots t_{63}t_{64}$ 变换成 $T_0=t_{58}t_{50}t_{42}\cdots t_{15}t_7$。$IP^{-1}$ 为 IP 的逆变换。

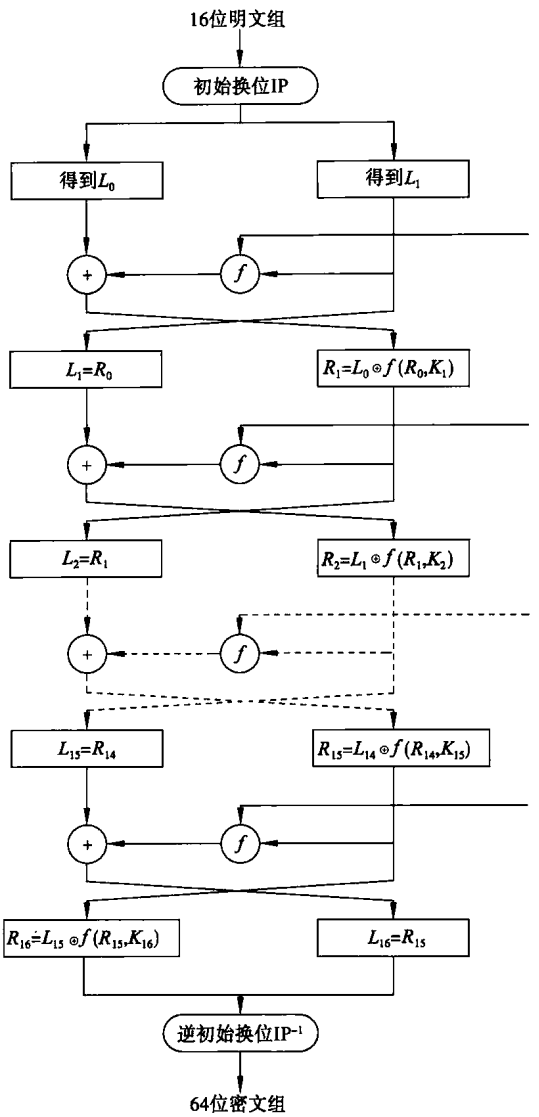


图 1-1 DES 加密过程

表 1-1 初始换位 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

表 1-2　逆初始换位 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

1. 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 位的并联 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 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。

2. 子密钥的生成

图 1-3 所示为生成每一轮使用的 48 位子密钥的过程。

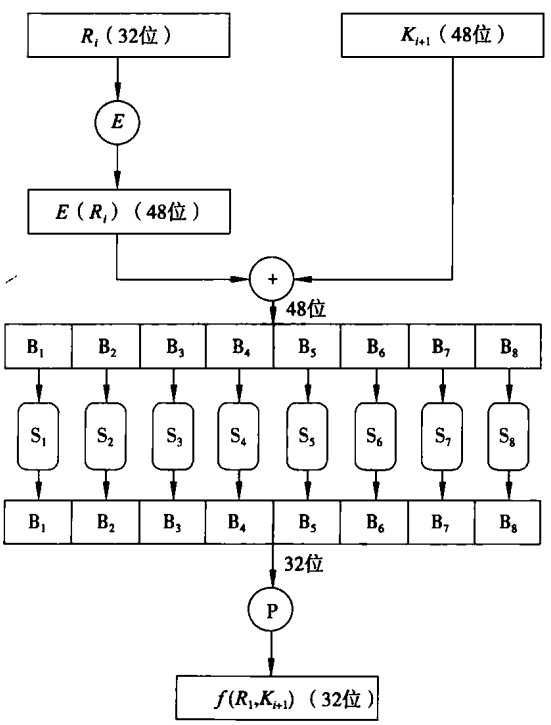


图 1-2　f 函数的处理流程

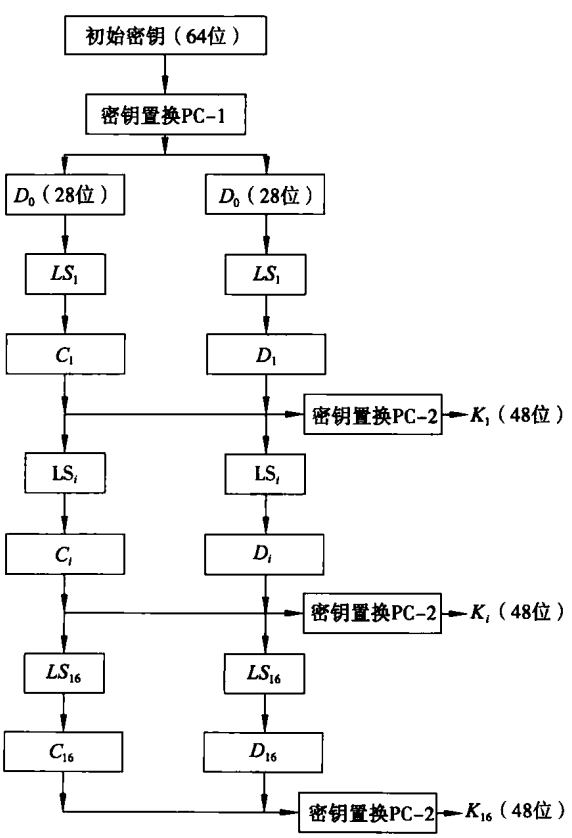


图 1-3　子密钥的产生流程

输入的初始密钥值为64位，但DES算法规定，其中第8、16、…、64位是奇偶检验位，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（见表1-3）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（见表1-4）即密钥置换PC-2，从而得到了密钥K_1（48位）。依此类推，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1-5所示的规则进行。

表1-3 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1-4 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

表1-5 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

三、实验环境

安装有Windows操作系统和Visual C++ 6.0（或Turbo C/C++ 3.0）的计算机。

四、实验内容和步骤

本实验为一个设计性实验，要求学生自己根据实验原理，自行设计实验步骤，选择自己熟悉的编程语言，实现对一个文件进行加密和解密。

对程序设计的基本要求：

① 有输入/输出界面；

② 密钥长度可变（64或128位）。

有关DES算法的样例程序可参见本书所附光盘。

五、思考题

① DES 算法中大量的置换运算的作用是什么？

② DES 算法中 S 盒变换的作用是什么？

③ 通过查阅相关资料了解目前破解 DES 算法的基本原理或方法。

1.1.2　triple-DES 算法

一、实验目的

① 掌握 triple-DES 算法的基本原理。

② 熟悉 triple-DES 算法的编程实现方法。

二、实验原理

随着密码分析技术的不断发展，DES 算法已被攻破，2000 年 10 月美国商业部提出采用以 Rijndael 算法的高级加密标准（AES）作为新一代的加密算法。在不对原有应用系统做大的改动的情况下，triple-DES 算法有了很大的生存空间，被大量用来替换已不安全的 DES 算法。所以对 triple-DES 算法的高速实现，仍具有一定的实际应用意义。

1999 年，美国国家标准与技术研究所（NIST）将 triple-DES 指定为过渡的加密标准。triple-DES 是 DES 的一个更安全的变形。DES 算法的结构如图 1-4 所示。其中 S 盒是 triple-DES（DES）算法的心脏，靠它实现非线性变换。

triple-DES 算法可以描述如下：设 $e_k(x)$和 $d_k(x)$表示用 DES 算法对 64 位的位串的加密和解密，密钥为 K；则 64 位的密文 c 通过执行下面的运算得到：

$$c = e_{K_3}(d_{K_2}(e_{K_1}(x)))$$

其中，K_1、K_2、K_3是 56 位的 DES 密钥。从密文 c 导出明文 x 的 triple-DES 的解密过程是加密过程的反过程，其描述如下：

$$x = d_{K_1}(e_{K_2}(d_{K_3}(c)))$$

triple-DES 结构如图 1-5 所示。

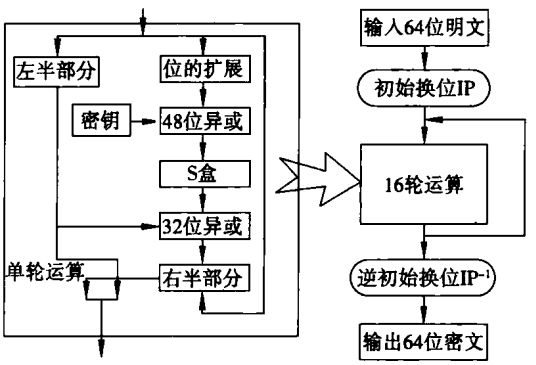


图 1-4　DES 算法结构

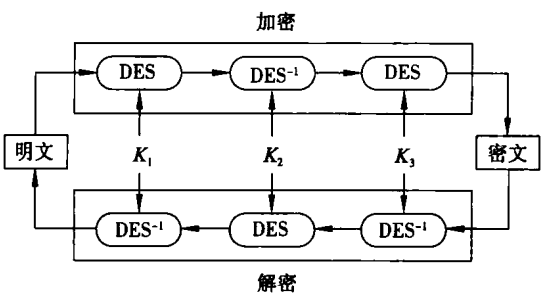


图 1-5　triple-DES 算法结构

为了获得更高的安全性，3 个密钥应该是互不相同的。这样，本质上就相当于用一个长为 168 位的密钥进行加密。多年来，它在对付强力攻击时是比较安全的。对安全性需要不那么高的数据，K_1可以等于 K_3。在这种情况下，密钥的有效长度为 112 位。

三、实验环境

安装有 Windows 操作系统和 Visual C++ 6.0（或 Turbo C/C++ 3.0）的计算机。

四、实验内容和步骤

本实验为一个设计性实验，要求学生自己根据实验原理，自行设计实验步骤，选择自己熟悉的编程语言，实现对一个文件进行加密和解密。

对程序设计的基本要求：

① 有输入/输出界面；

② 密钥长度可变（64 或 128 位）；

③ 运行方式可选择密钥“K_1、K_2、K_3不等”与“K_1=K_3、K_1与 K_2不等”两种。

有关 triple-DES 算法的样例程序可参见本书所附光盘。

五、思考题

请对“密钥 K_1、K_2、K_3不等”、“K_1=K_3、K_1与 K_2不等”两种情况的安全性与用途进行分析比较。

1.1.3 AES 算法

一、实验目的

① 掌握 AES 算法的基本原理。

② 熟悉 AES 算法的编程实现方法。

二、实验原理

1997 年 1 月，美国国家标准与技术研究所（NIST）开始公开征集、筛选 DES 的替代者，称为高级加密标准 AES（advanced encryption standard）。经过 3 轮筛选，2000 年 10 月 2 日，比利时的两位密码学家 Joan Daemen 和 Vincent Rijmen 设计的 Rijndael 算法因在安全性、实现代价和实现特性等方面都超过其他算法而胜出，成为高级加密标准 AES 算法。

1. AES 算法的基本结构

AES 为分组密码算法，数据块长度为 128 位，密钥长度为 128、192 或 256 位。分别称为 AES－128、AES－192 和 AES－256。下面介绍 AES－128 算法的基本原理。

AES 算法主要由密钥扩展、加密模块和解密模块 3 部分组成。分组长度（N_B）、密钥长度（N_K）和加密轮数（N_R）关系如表 1-6 所示。

表 1-6 N_B、N_K 和 N_R 的关系

算法模块 / 算法类别	分组长度 N_B/32 位	密钥长度 N_K/32 位	加密轮数 N_R
AES-128	4	4	10
AES-192	4	6	12
AES-256	4	8	14

2. AES 算法流程

AES-128 将输入的明文分成 16B（字节），在第一轮 AddRoundkey 变换后一共进行 10 轮迭代。

AES－128 的加密过程中前 9 轮完全相同。依次经过 SubBytes、ShiftRows、MixColumns、AddRoundKey 等 4 个子模块，最后一轮跳过 MixColumns。加密过程如图 1-6 所示。

AES-128 的解密过程与加密过程结构类似，但描述内容和执行顺序有些差别。前 9 轮依

次经过 InvShiftRows、InvSubBytes、AddRoundKey、InvMixColumns，最后一轮跳过 InvMixColumns。解密过程如图 1-7 所示。

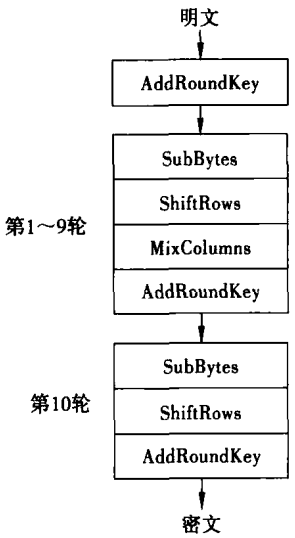


图 1-6 AES 算法加密流程

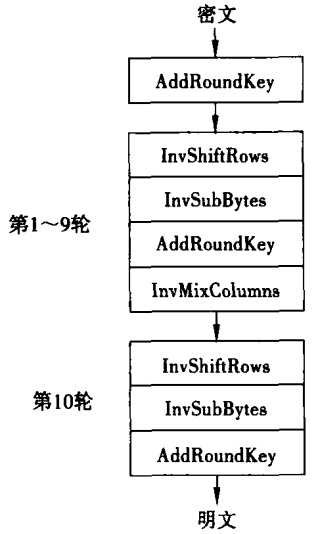


图 1-7 AES 算法解密流程

（1）SubBytes 操作

SubBytes 变换是作用于状态中每个字节上的非线性变换，其 S 盒是可逆的且由以下两部分组成：

首先，在域 GF（2^8）中取字节的乘法逆。其中，'00'的乘法逆是它本身。

其次，在域 GF（2）中进行仿射变换：$y = \boldsymbol{A}x^{-1} + \boldsymbol{b}$，其中

$$\boldsymbol{A}=\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \quad \boldsymbol{b}=\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

（2）ShiftRows 操作

ShiftRows 将状态中的各行以不同的位移量进行循环移位。0 行不移，第一行移 1B，第二行移 2B，第三行移 3B。

（3）MixColumns 操作

MixColumns 把状态中每一列看做域 GF（2^8）上的多项式 $C(x)$与一固定多项式相乘然后模多项式 x^4+1。其中 $C(x)$为

$$C(x)='03'x^3+'01'x^2+'02'$$

$C(x)$与 x^4+1 互质，因此是可逆的。

（4）AddRoundKey 操作

AddRoundKey 中，轮密钥被简单地按位异或到状态中。轮密钥通过密钥表得到，其长度为 4。