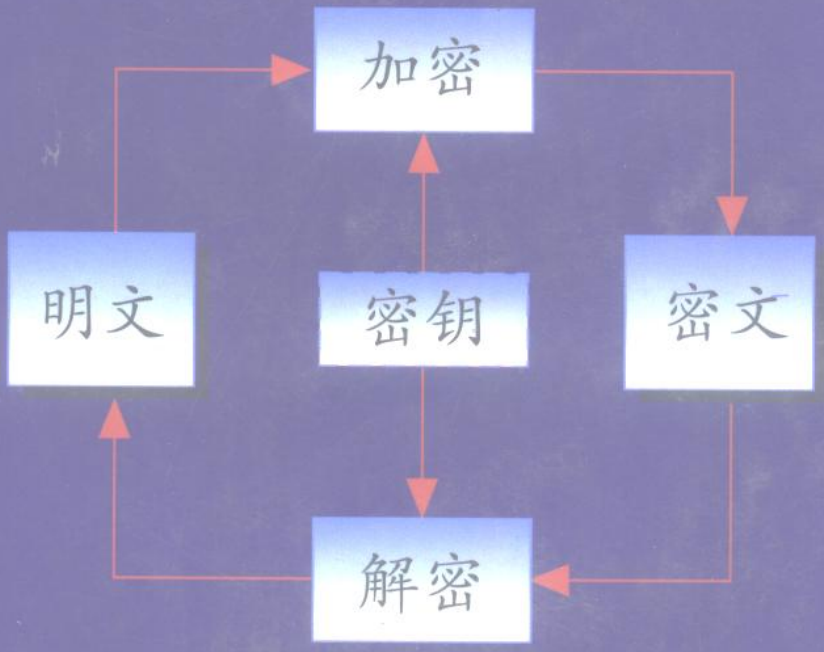
刘氏高强度公开加密算法设计原理与装置

刘尊全 著



清华大学出版社

刘氏高强度公开加密算法设计原理与装置

刘氏高强度公开加密算法设计原理与装置

刘尊全 著

9060

清华大学出版社

(京)新登字 158 号

内 容 简 介

这是一部计算机密码学的专著。全书分为两部分:背景和作者的发明。第一部分阐述了数据加密算法的基本方法和原理,详细剖析了数据加密标准 DES 和公钥密码体制 RSA 算法,指出了它们的脆弱性及其存在的问题,其中一些重要论点首次公布于世;第二部分阐述了作者创立的刘氏高强度公开加密算法体制,详细介绍了设计原理、数学描述、加密解密装置、数值实验、可实际应用的具体实现方法和算法特性。书中理论清晰,内容新颖,并附有程序实例与数值结果,可供读者分析比较和实际应用,具有重要的实用价值和学术价值。

图书在版编目(CIP)数据

刘氏高强度公开加密算法设计原理与装置/刘尊全著. 北京:清华大学出版社,1996
ISBN 7-302-02276-3

Ⅰ.刘… Ⅱ.刘… Ⅲ.电子计算机-加密-算法设计-保密技术 Ⅳ.TP309

中国版本图书馆 CIP 数据核字(96)第 16191 号

出版者:清华大学出版社(北京清华大学校内,邮编 100084)
印刷者:北京市清华园胶印厂
发行者:新华书店总店北京科技发行所
开 本:787×1092 1/16 印张:12 字数:280 千字
版 次:1996 年 11 月第 1 版 1996 年 11 月第 1 次印刷
书 号:ISBN 7-302-02276-3/TP・1117
印 数:0001—3000
定 价:24.00 元

前　言

随着计算机科学技术的迅速发展，特别是计算机系统与通信系统的结合，使信息的传输与加工可以在瞬间跨越地理位置的障碍遍布世界各地，信息处理深入到各个部门和领域并已经进入家庭，这一切使得人类开始进入信息化社会。无疑，信息的重要性与战略地位，使得信息安全与数据保护至关重要，并受到国际社会的普遍关注。

建立新的计算机密码体制和数据加密标准，这是当前国际上急待解决的重大课题。刘尊全教授建立的“刘氏高强度公开加密算法”已获得发明专利，这部专著的出版在我国计算机科学领域是很有意义的事情。

我与刘尊全教授相识已 20 多年。刘尊全是中国科学院的研究员，在计算机领域我们之间有很多的学术交流；1985 年刘尊全参与创建北京电脑天地学校并担任校长，我受聘担任高级顾问，日常交往更加密切。从多年的接触和了解中，我认为他是一位勇于探索和创新的有成就的科学家。他曾受聘在国外担任计算机科学教授，曾在法国、澳大利亚、美国从事研究工作，并取得了一系列重要的研究成果。

我很高兴看到刘尊全教授的专著中文版问世，并向广大计算机界的读者和关心计算机安全的人员推荐这部著作。我想提出三点意见：

1. 在计算机密码体制中解决加密强度涉及计算机科学的 NP 问题，这是相当困难的事情。刘氏加密算法在很小的计算开销下，可以大幅度提高加密强度，这在学术方面是有重要价值和影响的。

2. 如何评价一个计算机密码体制，刘尊全教授在专著中提出的五点建议，我认为是可取的，即：

① 是否是一个真正的公开加密体制？

② 可否实现加密解密的快速变换？

③ 是否具有高加密强度？

④ 是否在设计方法和原理上透明，使用户确信无陷阱，用户真正有安全感？

⑤ 是否是一个易于普及、使用方便的大众化的信息安全工具？

3. 刘尊全教授在专著中给出了加密强度为 2^{42200} 的实例，这个结果可以说是世界之最，在密码强度方面居于国际领先地位。其实，这也是刘尊全教授向国际密码学界提出的挑战。我希望学术界的朋友能接受这个挑战，认真考虑并研究这个问题。

科学技术在不断地进步，历史在向前发展。我真诚祝愿“刘氏高强度公开加密算法”能得到更大的进步和发展，并在计算机密码学领域为中华民族争得荣誉。

吴几康

1996 年 2 月 23 日

目　录

第 1 章　数据加密算法的基本方法和原理

信息是一种资源，也是一种财富。在现代社会中，信息处理和通信技术日益发展，保护信息的安全，特别是保护重要信息的安全，已成为国际社会普遍关注的重大问题。当前由于信息保护措施的不力或失误，世界各国所遭受的损失是巨大的，在商业（包括金融，特别是银行系统）、交通、工业（控制、通信等）、科学技术、国防、外交等部门的大量事例已充分说明了这一点。据美国“世界日报”1993 年 10 月报导：由于高技术犯罪，利用侦读器拦截卫星通讯电话的用户号码，再转手拷贝出售，1992 年美国就有 20 亿美元的国际电话费转帐混乱，造成有关公司严重的损失。目前仅仅银行的密码遭他人窃取，美国的银行界每年损失达数十亿美元之巨。

数据加密技术已随着计算机技术的迅猛发展，由早期的军事和外交领域，逐步伸展到交通、工业经济、科学技术、社会安全和公共生活的各个领域，成为现代社会中保护信息的重要手段和工具。信息保护的现实需要，使得数据加密算法和技术迅速进入了现代社会，了解并有效使用数据加密技术已成为计算机技术和通信领域的专业技术人员和广大用户的迫切需求，这是信息化社会发展阶段的重要标志。

1.1　基 本 概 念

密码学(cryptography) 是研究加密和解密变换的一门科学。通常情况下，人们将可懂的文本称为**明文**(plaintext)；将明文变换成的不可懂形式的文本称为**密文**(ciphertext)。把明文变换成密文的过程叫**加密**(encipher)；其逆过程，即把密文变换成明文的过程叫**解密**(decipher)。

从密码学的角度看，明文或密文都是一个字符串序列，并且明文与密文的相互变换是可逆的变换，严格讲，应该只存在唯一的可逆变换。完成加密和解密的算法称为**密码体制**(cipher System)，任何密码体制都应该是精确变换过程，即明文至密文之间及其相互变换是一种无误差的变换过程。了解这一基本概念，有助于我们理解任何密码体制下的加密变换和解密变换的过程。

虽然密码的出现及其表现形式，人们可以追溯到远古时代，然而密码学成为一门学科，则是近二十来年的事情。真正有效的密码体制，特别是能赋予实际广泛应用的密码体制，其加密和解密过程都是通过电子计算机系统来实现的。应该特别指出，微型计算机的发展和普及，大大促进了数据加密算法的社会化进程。反之，人们有理由认为：如果一个密码体制不能够通过微型计算机来实现，则它就失去了存在价值和实际意义。因此，任何密码体制的创立，它能否通过微型计算机来实现并投入实际应用，

已成为密码体制能否成功和是否具有生命力的重要标志。

通常情况下，在计算机上实现的数据加密算法，其加密或解密变换是由一个密钥或一组密钥来控制的(如图 1-1 所示)。**密钥**(keyword)是由使用密码体制的用户随机选取的，密钥成为唯一能够控制明文与密文之间变换的关键，它通常是一随机字符串。

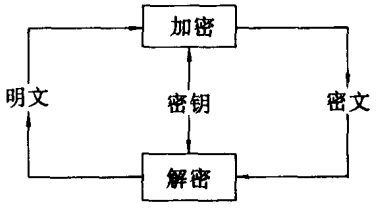


图 1-1　加密或解密变换

通常情况下的密码体制采用移位法、代替法和代数方法来进行加密和解密的变换，可以采用其中的一种或几种方法相结合的方式作为数据变换的基本模式。

移位法也称置换法。移位法把明文中的字符重新排列，字符本身不变，但其位置改变了。作为移位法最简单的例子是：把明文中的字母或字符倒过来写，然后以规定的长度的字符组发送或记录密文，如下例所示：

明文：Data security has evolved rapidly since 1975

密文：5791EC NISYLD IPARDE VLOVES AHYTIR UCESAT AD

作为移位法的另一种形式，可以将明文分组后倒过来写，然后以规定的长度的字符组发送或记录密文，如下例所示：

明文：CRYPTOGRAPHY AND DATA SECURITY BY LIU

密文：RGOTPYRC DDNAYHPA RUCESATA UILYBYTI

请注意，后一种分组移位法的形式，显著提高了密文的不可懂属性。

代替法是利用对照表方式，用另一个字符表来对应明文中的字符表，这样一来密文中的字符应保持明文中的原来位置，但其本身改变了。作为代替法的一个最简单的例子是单密字母表，它由明文部分和密文部分组成：

明文字母表：ABCDEFGHIJKLMNOPQRSTUVWXYZ

密文字母表：CDEFGHIJKLMNOPQRSTUVWXYZAB

在将明文变换成密文时，把明文中的字符用密文字符表中对应的字符来代替，并且密文可采用分组记录的方式：

明文：The Cryptology is a hot research area

密文：VJGETARV QNQIAKUC JQVTGUGC TEJCTGC

代数法加密可以对下列两种明文表示法进行相关的变换：

1. 将明文中的字符按指定的变换方法用数字来代替，然后对这些数字的值进行一系列可逆的数学运算，运算后产生的数字结果再通过逆初始变换的过程生成密文。应注意，采用代数法加密必须是无误差的数学运算，在密码学的运算中采用实数型数据运算是没有意义的。

2. 按照二-十进制，把明文字符的二进制等效值当作一组逻辑和算术运算的输入，产生的二进制结果再变回到二-十进制作为密文。

通常情况下，代数法加密可以采用微型计算机或其它类型的计算机来自动计算。代数法加密可以作为复杂加密体制的一种方法。

作为代数法的例子，这里介绍 Hill 发明的以求解联立方程为基础的加密体制。下面给出任意建立的字符对照表：

A	B	C	D	E	F	G	H	I	J	K	L	M
4	8	25	2	9	20	16	5	17	3	0	22	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
24	6	21	15	23	19	12	7	11	18	1	14	10

注意，在字符对照表中，对应 26 个英文字母其取值范围为 0—25。我们取 x 代表明文字母，y 代表密文字母，采用 4 个字符分组的明文序列，这种加密方法又称四元代替法，并有下列的加密方程：

$$y_1=8x_1+6x_2+9x_3+5x_4$$
$$y_2=6x_1+9x_2+5x_3+10x_4$$
$$y_3=5x_1+8x_2+4x_3+9x_4$$
$$y_4=10x_1+6x_2+11x_3+4x_4$$

根据加密方程，可以给出下面的解密方程：

$$x_1=23y_1+20y_2+5y_3+1y_4$$
$$x_2=2y_1+11y_2+18y_3+1y_4$$
$$x_3=2y_1+20y_2+6y_3+25y_4$$
$$x_4=25y_1+2y_2+22y_3+25y_4$$

加密或解密过程中对数字结果的处理是按模 26 进行的。

例：对明文 HELP，首先把明文翻译成下列一组数

$$x_1=\mathrm{H}=5$$
$$x_2=\mathrm{E}=9$$
$$x_3=\mathrm{L}=22$$
$$x_4=\mathrm{P}=21$$

用加密方程组求其密文值：

$$y_1 = 8x_1 + 6x_2 + 9x_3 + 5x_4 = 397 \text{ Mod } 26 = 7$$
$$y_2 = 15$$
$$y_3 = 10$$
$$y_4 = 14$$

从而得到密文 UQZY。在解密过程中，采用解密方程组求其明文值来进行处理。

数据的加密和解密变换可以采用一种或两种以上的方法、算法的结合。这些方法或算法可以多种多样，并且千变万化，寻找简单而有效的算法是密码学中始终关注的问题。**需要强调指出，任何字符都能表示成等效的二进制代码，不同数制之间可以进行转换，加密技术是不同编码之间的等效变换，并且这种正逆变换必须具有唯一属性。**

通常情况下，一个密码体制由以下五个部分组成：

1. 明文信息空间 M；
2. 密文信息空间 C；
3. 密钥空间 K；
4. 加密变换 E_k：$M \to C$，其中 $k \in K$；
5. 解密变换 D_k：$C \to M$，其中 $k \in K$。

对于密码体制，加密和解密变换是矛和盾的统一。建立和使用密码体制，都必须考虑数据加密所处的环境：用户为保护信息安全所使用的密码体制；攻击者为获取信息而拥有的破译手段和所使用的计算机工具。

密码分析学(cryptanalysis)是研究破译密码的一门科学。如果通过密文能够决定明文或密钥，或者通过明文—密文的比对能够决定密钥，则称一个密码是可破译的。通常有三种基本破译方法：

1. 单纯密文破译；
2. 已知明文破译；
3. 选择明文破译。

所谓**单纯密文破译**(ciphertext-only attack)是指破译者必须仅由截获的密文来决定密钥。所谓**已知明文破译**(known-plaintext attack)是指破译者已知某些明文—密文的比对来决定密钥。所谓**选择明文破译**(chosen-plaintext attack)是指破译者能够获取选择的明文所对应的密文。

对于公开密钥体制(public-key systems)还有第四种破译：**选择密文破译**(chosen-ciphertext attack)，在明文不掌握的情况下，破译者推断密钥。

通常情况下，密码体制应该满足下面三个基本要求：

1. 密码体制必须易于使用，特别是应当可以在微型计算机上使用；
2. 对所允许选择的密钥，加密和解密变换都必须迅速有效；
3. 密码体制的安全性应该只依赖密钥的保密性，而不应该依赖于加密算法 E 和解密算法 D 的保密性。

显然，对于任何的密码体制，对解密变换的密钥是必须要保护的。如果加密和解密的密钥是不同的，在没有暴露解密密钥可能的条件下，加密变换的密钥是可以公开的。这如同很多人都可以往指定的地址发送信件，而只有授权的接收者才有钥匙开启信箱并阅读有关的函件。

从数学方法角度来看，我们可以把破译方法分为两大类：

1. 系统分析法；

2. 穷举法。

系统分析法(system analysis method)又可分为**解析法**(analysis method)和**统计法**(statistical method)。采用解析法破译时，破译者必须根据算法的性质，通过表达式从已知量来求解未知量，即求解密钥或明文。设 C 是通过密钥 K 加密明文 M 而得到的密文，即

$$C=E_k(M)$$

则破译密码体制的解析法就是求解

$$M=D_k(C)$$

或者

$$K=F(M,C)$$

使用统计法破译，破译者根据明文、密文和密钥的统计规律来破译密码体制。因此，为了防止破译者用统计方法来破译密码体制，加密变换得到的密文序列必须是随机的，尽量使密文不呈现任何的统计特性。

穷举法(exhaust algorithm)是基于搜索的破译方法。使用密钥穷举法进行破译时，可以对密钥的所有可能取值用于已知明文加密，把加密结果与它对应的已知密文进行比较，使两者相等的密钥，即是所要求的密钥。从理论上讲，只要搜索密钥的所有可能取值，总是可以找到所求的密钥。但是，从实际上对一个有效的密码体制采用全局搜索密钥的策略往往是不可行的。破译者如果获得密码体制的设备(如密码机或密码发生器等)，在不掌握密钥的情况下，也可以将所有可能的明文加密成相应的密文，进而建立一个明文—密文的字库。这种字库可以将密文转换成明文，而不必求解密钥，这是明文穷举的破译方法。虽然从理论上明文穷举法是一种破译方法，而在实际上涉及计算机开销和存储量太大，难以实施。

在一个密码体制中，密钥具有特别的重要性。**加密强度**(encryption intensity)是破译密码体制的一种度量，它是由破译该体制的密码所用算法的计算复杂性所决定的。破译者往往尝试采用穷尽搜索整个密钥空间来破译密码，即试探每个可能的密钥，判定它是否能将密文解密为某个已知明文或有意义的明文。对于通常的密码体制，密钥长度的线性增加，可以导致破译这种密码的难度呈指数增长。问题的关键在于，一个通常的密码体制其加密或解密变换都是非线性数学运算，当密钥长度增加时，其加密或解密的计算开销也呈指数增长，使其在现有密码体制下无法提高其系统的加密强度。因此，如何提高密码体制(特别是公开加密算法体制)的加密强度是国际

社会普遍关注的迫切问题，既是一个重要的理论课题，也是一个具有广泛应用价值的实际课题。

1.2 数据加密标准 DES 的算法分析

1.2.1 背景

建立一个密码体制，密码体制的设计者必须考虑到数据加密技术所处的环境。早期建立的**密码本**(code book)方式，尽管目前在某些特殊的部门和领域仍在使用，但其存在着根本性的缺陷：(1)密码本本身要保密，这一致命的弱点本身就局限了使用者要安全可靠，使用者的人数和范围必然受到限制，从而使密码本方式限于人数少的小范围环境。(2)从安全角度，密码本方式的使用周期越短越安全；反之，使用周期长就失去了密码体制的安全性。(3)随着现代计算机技术的飞速发展和破译方式、手段的提高，研制新的密码本日益困难，研制周期长而使用周期越来越短。因此，密码体制面临新的挑战：密码体制如何在大范围使用？密码体制的算法内容可否公开？密码体制的内容公开，就意味着用户和破译者都可以完全了解密码体制的本身，这就要求密码体制本身必须具备用户使用容易而破译者解密困难。说到底，也只有密码体制的内容可以公开，才能够为大范围的用户使用，才能具有较长的稳定的使用周期，使密码体制成为一个工业化数据加密体制。

必须指出，研制和建立一个公开加密算法体制的难度是相当大的。所谓**公开加密算法**(publicly available cryptographic algorithm)是指密码体制的算法内容可以公开。至今而言，还没有一个真正的将密码体制设计原理、算法细节全部公开的公开加密算法体制。

DES 算法是由美国 IBM 公司的沃尔特·塔奇曼(W. Tuchman)和卡尔·迈耶尔(C. Meyer)于 1971 年至 1972 年研制成功的。这个加密算法是根据 1967 年美国霍斯特·菲斯特尔(Horst Feistel)提出的理论而研制的。美国国家标准局(NBS, National Bureau of Standard)于 1973 年 5 月至 1974 年 8 月两次发布通告，公开征求能用于电子计算机的加密算法。经过评选，从一大批算法中采纳了 IBM 公司提出的 LUCIFER 方案。

DES 算法在 1975 年 3 月公开发表，1977 年 1 月 15 日由美国国家标准局颁布为数据加密标准(Data Encryption Standard)，并从 1977 年 7 月 15 日生效，这是一个国家级标准。DES 是为美国联邦政府各机构在非军用场合需要密码保护的计算机系统或网络中使用的数据加密标准算法。

应当指出，美国国家安全局(NSA，National Security Agency)参与了美国国家标准局制订这一数据加密标准的过程。美国国家标准局接受了美国国家安全局的某些建议，对算法作了修改，并将密钥的长度从 IBM 公司的 LUCIFER 方案中的 128 位压缩到 56 位。而后面的这项改动引起了许多不满和怀疑，很多实业界人士认为美国国

家安全局的这个安排，将使其能利用现代的技术手段把有关部门和机构的活动置于美国国家安全局的监督和控制之下。

在 DES 算法公布以前，密码体制的设计者总是设法掩盖算法的实际细节。DES 开创了公开加密算法的先例，并向全世界提出向它攻击的挑战，这在密码学发展史上是有重大影响的历史事件。

目前，DES 成为数据加密的工业标准，它得到了 IBM、Burrough 等计算机制造厂商的支持，并陆续被其它组织机构所采纳。1979 年美国银行协会批准使用 DES。1980 年 DES 又成为美国标准化协会(ANSI)的标准。此后，DES 也受到国际标准化组织(ISO)的注意，1984 年 2 月成立的数据加密技术委员会(SC20)在 DES 基础上制订数据加密的国际标准工作。

DES 已被美国国家标准学会和美国银行协会用来保护通信系统的现金和证券传送。美国国家标准局还协助美国财政部使用 DES 用于电子设备传送每年的联邦资金。

自 1977 年以来，DES 在美国和国际上得到了广泛的应用。按原来规定，DES 每 5 年由美国国家标准局和商业部进行审查，以验证此标准对计算机处理数据的安全程度，并计划在 10 年后采用新的数据加密标准。

随着计算机技术的迅速发展，原拟提出的新的数据加密标准没有实现。在已经不能确保 DES 处理数据安全的情况下，1988 年美国国家标准局重申今后 5 年继续使用 DES，并且宣布这项标准将继续是保护计算机处理数据的有效方法。

自从 DES 交付使用以来，至今还没有发现任何数学上可行的解析破译方法。在现阶段，对于计算机专业技术人员和广大使用计算机的用户，了解并掌握 DES 仍然是很有必要的，特别是认真分析 DES 的机制，从中掌握对信息进行加密和解密的方法和技术是颇有益处的。

1.2.2 DES 概述

DES 是一种为二进制编码数据设计的，可以对计算机数据进行密码保护的数学运算。DES 通过密钥对 64 位的二进制信息进行加密，把明文的 64 位信息加密成密文的 64 位信息。由于 DES 的加密算法是公开的，所以加密强度取决于密钥的保密程度。加密后的信息可用加密时所用的同一密钥进行求逆变换成对应的明文。

DES 的设计中，将 64 位密钥中的 56 位用于加密过程，其余 8 位用于奇偶校验位。确切地说，密钥分成八个 8 位的字节，在每一个字节中的 7 位用于加密算法，第 8 位用于奇数校验。事实上，对于 DES 加密体制共有 2^{56} 个密钥可供用户选择。2^{56} 相当于 7.6×10^{16}，若采用穷举法进行攻击，即使 1 微秒可以穷举一个密钥，也需要用 2283 年的时间。

通常情况下，在计算机和有关的通信装置中 DES 是用硬件技术实现的。根据 1993 年 8 月的计算机检索，美国国内市场 DES 的硬件产品有 88 种之多，对于不同的

数据加密场合、环境，有着不同的数据加密设备和产品。当然，对于某些用户，也可以在微型计算机上用软件方式来实现 DES 数据加密算法。

为了便于叙述，我们采用符号形式和流程图来介绍 DES 算法，见图 1-2。

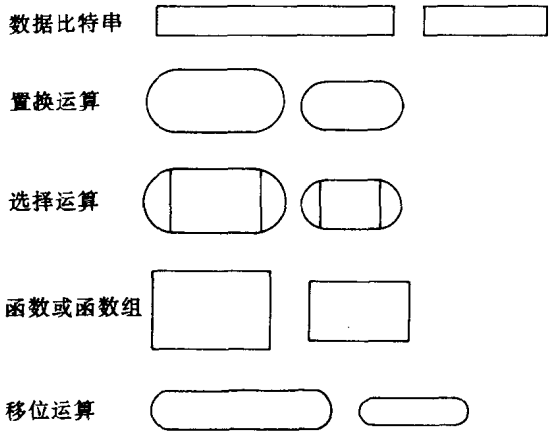


图 1-2　在 DES 流程图中所用的符号及说明

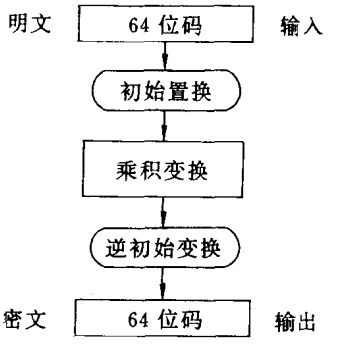


图 1-3　DES 算法的主要步骤

DES 数据加密系统流程的逻辑框图见图 1-3。

DES 算法的主要步骤如下：

1. 输入，即 64 位码的明文；

2. 初始置换(IP)，移位操作。注意，在初始置换过程不使用密钥，仅仅对 64 位码进行移位操作；

3. 乘积变换，这是一个与密钥有关的对码组加密运算；

4. 逆初始置换(IP^{-1})，它是第 2 步中所完成变换的逆变换，这一变换过程也不使用密钥；

5. 输出，即 64 位码的密文。

初始置换和逆初始置换是简单的移位操作。DES 算法属于分组加密体制，在乘积变换这一步骤中，代替是在密钥控制下进行的，而移位是按固定顺序进行的，它将数据码组作为一个单元来进行变换，相继使用代替法和移位法加密，从而具有增多代替和重新排列的功能。

乘积变换是 DES 算法的核心部分，图 1-4 表示乘积变换中一次迭代逻辑框图。

乘积变换包括以下运算：

(1) 把明文的 64 位码组分成两个 32 位的码组，分别用 L_{i-1}及 R_{i-1}表示左 32 位和右 32 位。

(2) 把输入码组的右边 32 位变成输出码组的左边 32 位。在图 1-4 中用 R_{i-1}到 L_i 的箭头表示。

(3) 输入码组的右边 32 位(R_{i-1}表示)，经过一个选择过程产生一个 48 位的数据码组。这是一个与密钥无关的固定选择。

(4) 用 64 位密钥(去掉 8 位奇偶校验位,实际为 56 位密钥)产生一组 48 位的子密钥 K_i,其中 $1 \leqslant i \leqslant K$,每个 K_i 都是独立的,并对应于乘积变换的第 i 次迭代。

(5) 把 48 位的子密钥与第(3)步变换得到的结果进行模 2 加法,得到 48 位的结果。

(6) 把第(5)步得到的 48 位结果分成八个 6 位的组,每一组经过一次独特的代替法加密,即选择函数变换,产生八个 4 位的组,形成一个 32 位的输出结果。

(7) 把第(6)步得到的 32 位输出进行置换,即通过一种简单的移位变换,产生出一个 32 位的码组。

(8) 把第(7)步的 32 位输出与输入码组的左边 32 位 L_{i-1}进行模 2 加法,产生出 R_i,它是 64 位输出码组的右边 32 位。

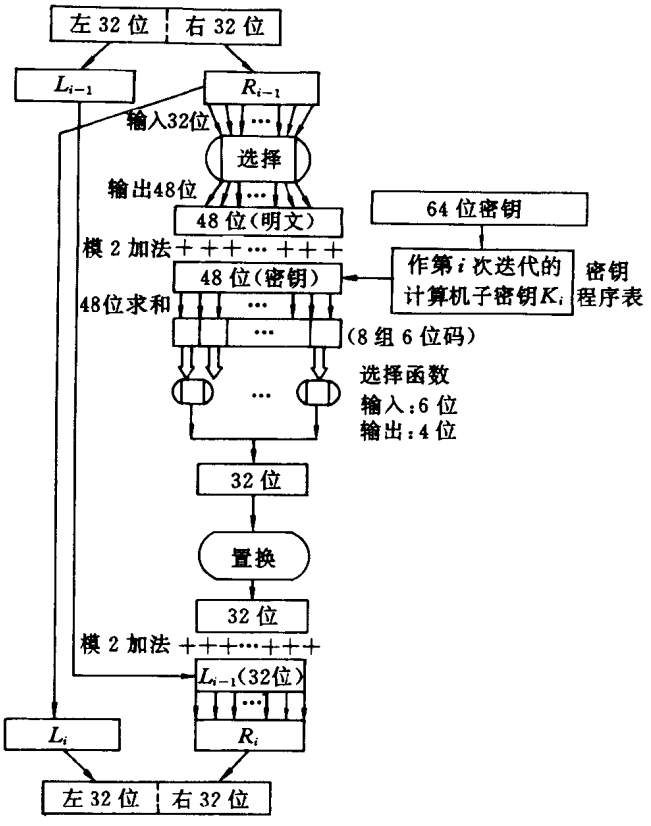


图 1-4 乘积变换中的一次迭代

从第(1)步到第(8)步的运算一共计算 16 次,即 16 次迭代,这样就构成了乘积变换的主要部分。注意,乘积变换的最后一步是把最后一次迭代输出的左边一半和右边一半进行码组变换(即交换)。

解密过程是加密的逆过程,以相反的顺序使用乘积变换中的子密钥,即从 K_{16}到 K_1。

1.2.3 DES 算法的剖析

为了分析 DES 算法，我们对数据流的加密和解密过程进行剖析。首先对其各主要的组成部分进行剖析，然后再介绍各组成部分相结合的加密和解密过程。

DES 算法的基本设计思想：通过循环或迭代，将简单的基本运算（例如左移、右移、模 2 加法等）和变换（选择函数、置换函数）构造成数据流的非线性变换（加密变换或解密变换）。DES 算法的数据流程的基本框架是固定的，通过密钥分解将一个实际上是 56 位（二进制）（64 位密钥去掉奇偶校验位，刚好是 56 位）的密钥分解成 16 个 48 位（二进制）的子密钥，每个子密钥控制一次循环或迭代。加密与解密的密钥和流程是完全相同的，区别仅仅是加密与解密使用子密钥序列的施加顺序刚好相反。

一、DES 的构成

DES 的基本组成部分如下：

（1）计算密钥表，将一个 64 位密钥转换成一组 16 个 48 位的子密钥；

（2）模 2 加法运算；

（3）加密函数，包括乘积变换中的选择函数和置换运算；

（4）码组移位，将乘积变换中最后一次迭代的输出经码组变换后产生一个 64 位的结果；

（5）初始置换，它是一个选择表；

（6）逆初始置换，也是一个选择表。

二、密钥表计算

计算密钥表的目的是产生加密和解密过程所需要的 16 个子密钥，K_1，K_2，K_3，…，K_{16}，记作 K_i。每个 K_i 长 48 个二进制，是通过置换、选择和移位操作得到的。

把 64 位密钥中的各位从左至右按 1 到 64 进行编号，但是并非密钥中的所有位都用于计算密钥表。这个 64 位密钥可用 8 个字节（每个字节是 8 个二进位）表示，而每个字节中有一位是用于奇校验而不是用于密钥表计算的。校验位的编号是 8，16，24，32，40，48，56 及 64，而真正用于密钥表计算的是下列各位：

1 到 7，9 到 15，17 到 23，25 到 31，

33 到 39，41 到 47，49 到 55，57 到 63。

密钥表按下列步骤进行计算：

（1）密钥中的非校验位共计 56 位，通过置换运算生成两个 28 位的码组，记作 C_0 及 D_0。这是计算子密钥序列的起点，通过置换选择 1（见图 1-6）来进行。

（2）把 C_0 和 D_0 循环左移一位，产生 C_1 和 D_1。

（3）把 C_1 和 D_1 中选定的一些位抽出来产生子密钥 K_1，这个变换通过置换选择 2（见图 1-7）来进行。

（4）把 C_1 和 D_1 循环左移一位，产生 C_2 和 D_2。

（5）把 C_2 和 D_2 中选定的一些位抽出来产生子密钥 K_2，这个变换仍然通过置换

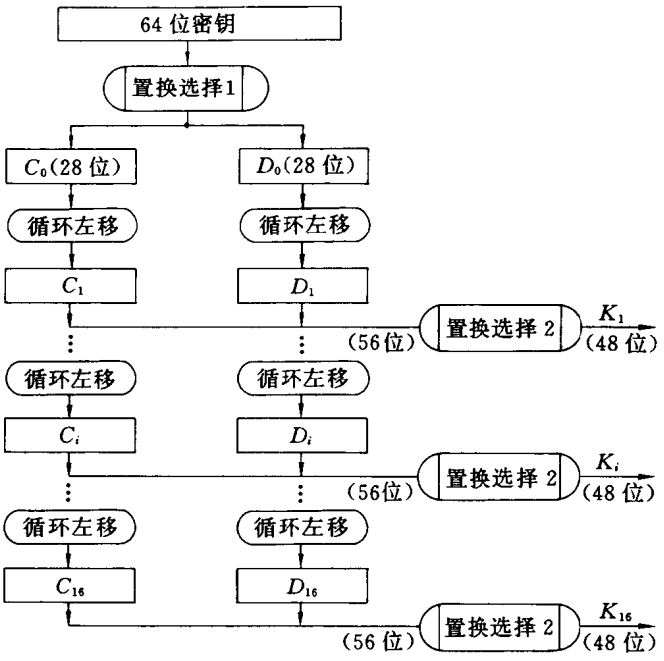


图 1-5　密钥表的计算逻辑(粗框)

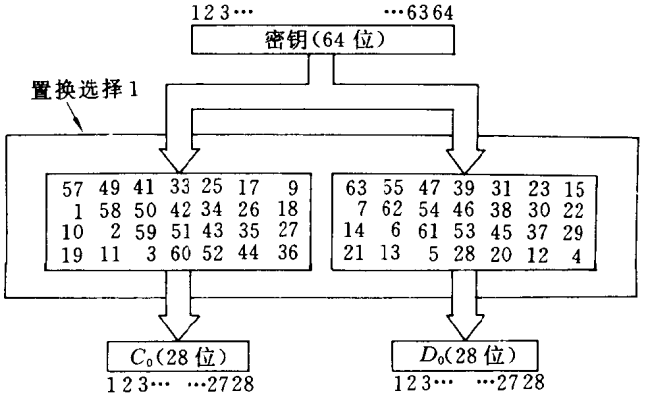


图 1-6　用于计算 C_0 和 D_0 的置换选择 1

选择 2 来进行。

(6) 继续这一过程,求得 K_3 至 K_{16}的子密钥。每个 C_i 和 D_i 都是经过规定的循环左移次数后得到的值求得的。

每个记作 K_i 的子密钥是从 C_i 和 D_i 中通过置换选择 2 的操作求得的,而 C_i 和 D_i 是分别从 C_{i-1}和 D_{i-1}经过规定的移位操作而得到的。在不同层次的 C_i 和 D_i 中,其循环左移位数有时是 1,有时是 2,其具体规定见表 1-1。