分组密码的设计与分析

冯登国　吴文玲

清华大学出版社

(京)新登字 158 号

内 容 简 介

本书主要介绍了设计和分析分组密码的理论和技术,包括现有的有代表性的分组密码及其攻击方法,评测分组密码的统计特性的原理,评测 S-盒的安全性能的准则及准则之间的关系,构造安全性能好的 S-盒的方法,最新公布的 AES 候选算法及其分析。

本书是作者在长期从事科研和教学实践的基础上完成的,内容新颖,系统性强,深入浅出,易于理解。

本书可作为计算机专业、通信专业、信息安全专业的硕士生、博士生和本科高年级学生的选修课教科书,也可供从事相关专业的教学、科研和工程技术人员参考。

图书在版编目(CIP)数据

分组密码的设计与分析/冯登国,吴文玲编著. —北京:清华大学出版社,2000
ISBN 7-302-03986-0

Ⅰ. 分… Ⅱ. ① 冯… ② 吴… Ⅲ. 密码-基本知识 Ⅳ. TN918.2

中国版本图书馆 CIP 数据核字 (2000) 第 37145 号

出版者:清华大学出版社(北京清华大学学研大厦,邮编 100084)
http://www.tup.tsinghua.edu.cn
印刷者: 印刷厂
发行者:新华书店总店北京发行所
开 本:787× 1092 1/16 印张:8 字数:119 千字
版 次:2000 年 9 月第 1 版 2000 年 9 月第 1 次印刷
书 号:ISBN 7-302-03986-0/TP・2336
印 数:0001～0000
定 价: 元

前　言

随着计算机和通信技术的发展，信息安全技术越来越重要。信息的保密是信息安全的一个重要方面。保密的目的是防止敌手破译信息系统中的机密信息。加密是实现信息保密的一种重要手段。加密技术可使一些重要数据存储在一台不安全的计算机上，或在一个不安全的信道上传送。在商业应用领域，分组密码是目前比较重要而流行的一种加密技术，主要用于数据的保密传输。

国际上非常重视分组密码的设计与评测。美国早在 1977 年就制定了自己的分组加密标准，但除了公布具体的算法之外，从来没有公布其详细的设计原则和方法。随着美国的分组加密标准的出现，人们对分组密码的设计与评测展开了深入的研究和讨论，设计了大量的分组密码，给出了一系列的评测准则，欧洲一些国家和前苏联也纷纷提出了自己的分组加密标准。但能被人们普遍接受和认可的算法却寥寥无几。何况一些好的算法已经被攻破或已经不适用于技术的发展要求。比如目前只需花 25 万美元 56 小时就能搜索到美国的分组加密标准的加密密钥。1997 年 4 月 15 日美国国家标准技术研究所(NIST)发起征集 AES(Advanced Encryption Standard)算法的活动，并专门成立了 AES 工作组。目的是为了确定一个非保密的、公开披露的、全球免费使用的分组密码，用于保护下一世纪政府的敏感信息。也希望能够成为秘密和公开部门的数据加密标准(DES)。1998 年 8 月 20 日 NIST 召开了第一次 AES 候选会议，并公布了 15 个 AES 候选算法。1999 年 3 月 22 日召开了第二次 AES 候选会议，公开了 15 个候选算法的讨论结果。目前已从这 15 个算法中挑选出了 5 个作为进一步讨论的主要对象。NIST 声称最终将在这 5 个算法中遴选出一个或多个算法作为 AES，预计于 2001 年出台 AES。

我国政府高度重视国家信息化建设。我国的通信业务以世界最快的速度发展，金系列工程推动了国民经济各个重要领域的信息基础设施的建设，Internet 在我国也成为信息化应用的热点。网络化、数字化的特点使信息空间跨越国境，有别于传统的运作模式，信息安全成为数字化安全生存的基础，信息革命成败的关键。特别是面对某些妄图以信息能力称霸的超级大国的信息战的威胁，我们必须高度重视维护国家的主权独立和安全，高度重视在信息化基础上增强我国的经济竞争实力。而密码技术是信息安全技术中的核心技术，只能自主开发，不能引进外国技术。

本书主要包括两个方面的内容，即分组密码的设计和分组密码的评测。在分组密码的设计方面，主要论述了设计分组密码的非线性资源。因为一个分组密码是由一些简单而密码结构好的组件搭配而成的，所以这些组件对密码的设计极为重要。这些组件主要包括密码性能好的置换模式和工作模式、密码性能好的单输出函数和多输出函数等。在分组密码的安全性评测方面，论述了分析分组密码的一些典型方法，同时也介绍了一些切实可行的、有效的评估分组密码的安全性的准则和原理。本书的目的是为设计好而安全的分组密码提供理论基础，加速我国分组密码算法的应用进程，推动我国信息安全产业的发展。

本书在写作和出版过程中得到了许多部门和专家的大力支持和帮助,他们是:国家科学技术学术著作出版基金委员会,清华大学出版社,中国科学院软件所,中国科学院高技术局局长桂文庄研究员,中国科技大学研究生院裴定一教授,中国科学院信息安全技术工程研究中心主任卿斯汉研究员,在这里向他们表示衷心的感谢。

由于水平和时间有限,本书一定存在许多不足之处,希望诸位读者指导。

作者

2000 年 2 月 2 日

目　　录

第 1 章　绪　　论

1.1　分组密码的研究背景与意义

随着计算机和通信技术的发展,用户对信息的安全存储、安全处理和安全传输的需求越来越迫切。特别地,随着 Internet 的广泛应用,以及个人通信、多媒体通信、办公自动化、电子邮件、电子自动转账支付系统和自动零售业务网的建立与实现,信息的安全保护问题就显得更加重要。而解决这一问题的有效手段之一是使用现代密码技术。

“密码学新方向”[1]的发表和美国数据加密标准 DES[2]的颁布实施标志着现代密码学的诞生,从此揭开了商用密码研究的序幕。此后实用密码体制的研究基本上沿着两个方向进行,即以 RSA[3]为代表的公开密钥密码体制和以 DES 为代表的秘密密钥分组密码体制。分组密码具有速度快、易于标准化和便于软硬件实现等特点,通常是信息与网络安全中实现数据加密、数字签名、认证及密钥管理的核心体制,它在计算机通信和信息系统安全领域有着最广泛的应用。

当前,分组密码之所以受到广泛关注并且成为密码学研究的热点课题之一,主要是由于以下几个原因:

(1) 加密算法标准化的需要

标准化是工业社会的一个基本概念,它意味着生产规模化、降低成本、方便维修和更换。为了实现非相关团体之间的保密通信,加密体制的标准化是必要的。分组密码由于其固有特点,已经成为标准化进程的首选体制。1977 年美国国家标准局颁布了联邦信息处理标准 DES,以保护非机密信息在存储和传输过程中免受未经授权的篡改或泄露。此后,DES 作为数据加密的工业标准,得到了 IBM 等计算机制造厂商的大力支持,并陆续被其他组织机构所采纳。1979 年美国银行家协会批准使用 DES,1980 年 DES 又成为美国标准化协会(ANSI)的标准。继而,DES 也受到国际标准化组织(ISO)的关注,1984 年成立的数据加密技术委员会 SC20 准备在 DES 基础上制定数据加密的国际标准。尽管 DES 是目前世界上使用最广和最成功的算法,但是它的 56 比特密钥对今天的许多安全应用已太短了;三重 DES 作为临时的解决方案已出现在许多像银行这类安全性高的应用中,但是对于某些应用,它的加密速度太慢。最根本的是,当同 一密钥加密大量数据时,DES 的 64 比特分组长度为密码攻击开了方便之门。正是由于这些原因,1997 年 4 月 15 日美国国家标准技术研究所(NIST)发起征集 AES(Advanced Encryption Standard)[4, 5]算法的活动,并专门成立了 AES 工作组,目的是为了确定一个非保密的、公开披露的、全球免费使用的分组密码算法,用于保护下一世纪政府的敏感信息,也希望 AES 能够成为秘密和公开部门的数据加密标准。

(2) 加密算法本土化的需要

信息安全的最大特点之一是自主性,因而其核心技术—— 密码学的研究与开发应当

是一种本土性的科学。对于有些产品,可以通过外方引进来解决由于技术落后而带来的问题。然而对于安全产品,除非能完全确信它在硬件和软件上没有陷门,否则,贸然使用可能带来不可预测的后果。而要做到软硬件上的确认通常是十分困难的。因此,最明智的方法是依靠自己的力量并汲取现有的先进经验进行研究、设计和开发。

(3) 官方组织维护通信和社会安全的需要

为了维护通信安全、打击犯罪,1993 年 4 月,美国政府宣布了一项新的建议,该建议倡导联邦政府和工业界使用新的具有密钥托管功能的联邦加密标准[6]。该建议称为托管加密标准(escrowed encrytion standard, EES),又称 Clipper 建议。其目的是为用户提供更好的安全通信方式,同时允许政府机构在必要情况下进行监听。EES[7]系统中嵌入了分组加密算法 Skipjack[8],尽管目前对该系统和算法有许多争议,但从维护国家通信安全的角度,这项建议是有积极意义的。

(4) 多级安全的需要

在区域通信系统中,用户较多,他们的地位、作用都不相同,所流通的信息的重要性也不可能完全相同,因此他们要求得到的安全保护等级也不应该相同。由此可见,研究多安全级密码算法非常必要。迭代分组密码(所谓迭代分组密码就是以迭代一个简单的轮函数为基础的密码,即通过选择某个较简单的密码变换,在密钥控制下以迭代方式多次利用它进行加密变换,例如 Feistel 型密码就是一种迭代密码,详见 4.2.1 节)是分组密码的典型代表,其数学思想简单而灵巧。特别是在相同的轮函数之下,迭代次数的不同即代表了安全强度的不同级别。

(5) 网络安全通信的需要

在 Internet/ Intranet 中随着通信量和业务种类的增加,对安全认证和保密业务的需求日益迫切。比如,PGP(Pretty Good Privacy)就是一种广泛应用于 Internet 中 E-mail 系统的一种安全技术方案,它也可以用于其他网络中。PGP 的安全业务包括机密性、认证性、不可抵赖性等,其中的机密性就是利用分组密码算法 IDEA[9, 10]来保证的。另外,分组密码的工作模式可提供一些人们所需要的其他密码技术,比如流密码技术和杂凑技术等。

1.2 分组密码的研究现状

现代分组密码的研究始于 20 世纪 70 年代中期,至今已有 20 余年的历史,这期间人们在这一研究领域已经取得了丰硕的研究成果。大体上,分组密码的研究包括三方面:分组密码的设计原理,分组密码的安全性分析和分组密码的统计性能测试。

分组密码的设计与分析是两个既相互对立又相互依存的研究方向,正是由于这种对立促进了分组密码的飞速发展。早期的研究基本上围绕 DES 进行,推出了许多类似于 DES 的密码,例如,LOKI[11~15]、FEAL[16~21]、GOST[22]等[27~31]。进入 90 年代,人们对 DES 类密码的研究更加深入,特别是差分密码分析(differential cryptanalysis)[35~38]和线性密码分析(linear cryptanalysis)[44~48]的提出,迫使人们不得不研究新的密码结构。IDEA 密码的出现打破了 DES 类密码的垄断局面,IDEA 密码的设计思想是混合使用来自不同代数群中的运算。随后出现的 Square[23]、Shark[24]和 Safer-64[25, 26]都采用了结构非常清晰的

代替-置换(SP)网络,每一轮由混淆层和扩散层组成。这种结构的最大优点是能够从理论上给出最大差分特征概率和最佳线性逼近优势的界,也就是密码对差分密码分析和线性密码分析是可证明安全的。

AES 的征集掀起了分组密码研究的新高潮,15 个 AES 候选算法反映了当前分组密码设计的水平,可以说是近几年研究成果的一个汇总。目前分组密码所采用的整体结构[61~67]可分为 Feistel 结构(例如 CAST-256、DEAL、DFC、E2 等)、SP 网络(例如 Safer+ 、Serpent 等)及其他密码结构(例如 Frog 和 HPC)。Feistel 结构由于 DES 的公布而广为人知,已被许多分组密码所采用。Feistel 结构的最大优点是容易保证加解密相似,这一点在实现中尤其重要。而 SP 网络比较难做到这一点,但是 SP 网络的扩散特性比较好。在现有的分组密码中,所用的基本运算有异或、加、减、查表、乘及数据依赖循环等。查表运算提供了 DES 的安全基础,仔细地选择 S-盒[68~85]能较好地抗击线性和差分密码分析,提供好的数据及密钥比特的雪崩特性。不过,S-盒需要一些存储器,所以 S-盒[68~87]的规模不能太大。15 个 AES 候选算法所采用的 S-盒规模有 6 种,分别是 4× 4、8× 8、8× 32、11× 8、13× 8 及 8× 32。S-盒的另一种称呼是黑盒子,它常给人造成故意设置陷门的嫌疑,因此,Safer+ 等选取公开的数学函数,避免嫌疑。S-盒的设计与分析是分组密码设计中的重要环节,它的好坏直接影响密码体制的安全性,目前对 S-盒的设计并没有一个完备的要求,但总的希望是增强 S-盒的非线性度、差分均匀性及分量函数的代数次数和项数。

目前对分组密码安全性的讨论主要包括差分密码分析、线性密码分析和强力攻击[33,34]等。从理论上讲,差分密码分析和线性密码分析是目前攻击分组密码的最有效的方法,而从实际上说,强力攻击是攻击分组密码最可靠的方法。到目前为止,已有大量文献讨论各种分组密码的安全性,同时推出了譬如截段差分分析、非线性密码分析及插值攻击等多种分析方法[35~60]。自 AES 候选算法公布以后,国内外许多专家学者都致力于候选算法的安全性分析,预计将会推出一些新的攻击方法,这无疑将进一步推动分组密码的发展。

分组密码是现代密码学中的一个重要研究分支,其诞生和发展有着广泛的实用背景和重要的理论价值。目前这一领域还有许多理论和实际问题有待继续研究和完善。这些问题包括:如何设计可证明安全的密码算法;如何加强现有算法及其工作模式的安全性;如何测试密码算法的安全性;如何设计安全的密码组件,例如 S-盒、扩散层及密钥扩展算法等。

1.3　本书的安排

本书的安排及其主要内容如下:

第 2 章简要介绍了国际上现有的一些有代表性的分组密码,包括 DES, IDEA, Skipjack 等,同时介绍了分组密码的数学模型和工作模式。

第 3 章介绍了国内外现有的攻击分组密码的典型方法,包括差分密码分析、高阶差分密码分析、截段差分密码分析、线性密码分析、多重线性密码分析、非线性密码分析、插值攻击、密钥相关攻击等。目的是使设计者全面了解各种攻击方法的基本思想以及操作技

巧,从中吸取经验和教训,增进设计经验和技巧,提高设计和分析分组密码的能力。

第4章介绍了分组密码的一般设计原理。给出了分组密码各个组件的设计准则及构造方法,包括几种常用的整体结构及其各自的优缺点、轮函数的设计准则和构造方法、S-盒的设计准则和构造方法、P置换的设计准则和构造方法以及设计密钥扩展算法应遵循的几个准则。

第5章介绍了二项分布的 χ^2 拟合检验在分组密码测试中的应用原理,包括数据变换的有效性测试原理、算法对明文的扩散性测试原理和密钥变换的有效性测试原理。简要讨论了密钥的生成、分配及保护等问题。

第6章简要介绍了AES候选算法及其评估准则,并对其发展现状作了详细介绍。

第 2 章　典型分组密码简介

2.1　分组密码的数学模型

分组密码是将明文消息编码表示后的数字(通常是 0 与 1)序列 $x_1, x_2, \cdots$ 划分成长为 m 的组 $x=(x_1, x_2, \cdots, x_m)$,各组(长为 m 的向量)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 $y=(y_1, y_2, \cdots, y_n)$(长为 n 的向量),分组密码的数学模型如图 2.1.1 所示。分组密码有其自身的优点。首先,分组密码容易被标准化,因为在今天的数据网络通信中,信息通常是被成块地处理和传输的。其次,使用分组密码容易实现同步,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随后的组的解密的正确性产生影响。分组密码的主要缺陷表现在两个方面,一是分组加密不能隐蔽数据模式,即相同的密文组蕴含着相同的明文组;二是分组加密不能抵抗组的重放、嵌入和删除等攻击。但分组密码的上述缺陷可以通过在加密处理中引入少量的记忆来克服。例如可以通过密码分组链接(CBC)模型来克服这些缺陷。

图 2.1.1　分组密码的数学模型

若 $n>m$,则为有数据扩展的分组密码。若 $n<m$,则为有数据压缩的分组密码。若 $n=m$,则为无数据扩展和压缩的分组密码,通常研究的均为这种情况。在本节中,我们设明文 x 和密文 y 均为二元数字(0 与 1)序列。设 F_2 是二元域,F_2^s 表示 F_2 上的 s 维向量空间。假定明文空间和密文空间均为 F_2^m,密钥空间 S_K 是 F_2^t 的一个子集合。m 是明文和密文的分组长度,t 是密钥的长度。

一个分组密码可定义为:

定义 2.1.1　分组密码是一种满足下列条件的映射 $E: F_2^m \times S_K \to F_2^m$:对每个 $k \in S_K$,$E(\cdot, k)$ 是从 F_2^m 到 F_2^m 的一个置换。

通常称 $E(\cdot, k)$ 为密钥为 k 时的加密函数,称 $E(\cdot, k)$ 的逆为密钥为 k 时的解密函数,记为 $D(\cdot, k)$。分组密码的真正的密钥规模被定义为 $l=\log_2 \#S_K$ 比特。因而,密钥长度等于真正的密钥规模当且仅当 $S_K=F_2^t$。例如 DES 的真正的密钥规模 $l=56$ 比特,且 l 也就是密钥长度。

我们知道,F_2^m 上的置换共有 $2^m!$ 个。由定义 2.1.1 知,一个分组密码的密钥顶多有 2^t 个,t 不能太大,因此 $E(\cdot, k)$ 是 F_2^m 上的全体置换所构成的集合的一个子集合。可见,设计分组密码的问题在于找到一种算法,能在密钥控制下从一个足够大且足够“好”的置换子集合中,简单而迅速地选出一个置换。一个好的分组密码应该是既难破译又容易实现,

即加密函数 $E(\cdot,k)$ 和解密函数 $D(\cdot,k)$ 都必须容易计算，但是至少要从方程 $y=E(x,k)$ 或 $x=D(y,k)$ 中求出密钥 k 应该是一个困难问题。

2.2 数据加密标准(DES)

计算机通信网的发展对信息的安全保密的要求日益增长，未来的数据传输和存储都要求有密码保护，为了实现同一水平的安全性和兼容性，提出了数据加密标准化。标准化便于联网、训练操作维护人员、降低生产成本和推广使用。为此，美国商业部所属国家标准局(NBS, National Bureau of Standards)在 1972 年开始了一项计算机数据保护标准的发展规划。NBS 在 1973 年 5 月 13 日的联邦记录(FR1973)中公布了一项公告，征求在传输和存储数据中保护计算机数据的密码算法的建议，这一举措最终导致了数据加密标准(DES)的研制。DES 是迄今为止世界上最为广泛使用和流行的一种分组密码算法，它是由美国 IBM 公司研制的，是早期的称作 Lucifer 密码的一种发展和修改。DES 在 1975 年 3 月 17 日首次被公布在联邦记录中，在做了大量的公开讨论后于 1977 年 1 月 15 日正式批准并作为美国联邦信息处理标准，即 FIPS-46，同年 7 月 15 日开始生效。规定每隔五年由美国国家保密局(NSA, National Security Agency)作出评估，并重新批准它是否继续作为联邦加密标准。最近的一次评估是在 1994 年 1 月，美国已决定 1998 年 12 月以后将不再使用 DES。美国目前正在征集、评估和制定新的数据加密标准，新的标准被称作 AES。尽管如此，DES 对于推动密码理论的发展和应用起了重大作用，对于掌握分组密码的基本理论、设计思想和实际应用仍然有着重要的参考价值。下面我们来描述这一算法。

DES 是一个分组密码。DES 使用长度为 56 比特的密钥加密长度为 64 比特的明文，获得长度为 64 比特的密文，它的加密工作程序如下:

(1) 给定一个明文 x，通过一个固定的初始置换 IP 置换 x 的比特，获得 x_0，记 $x_0=IP(x)=L_0R_0$，这里 L_0 是 x_0 的前 32 比特，R_0 是 x_0 的后 32 比特。

(2) 然后进行 16 轮完全相同的运算，在这里数据与密钥结合。我们根据下列规则计算 L_iR_i，$1\leq i\leq 16$:

$$L_i=R_{i-1}$$

$$R_i=L_{i-1}\oplus f(R_{i-1},K_i)$$

这里 $\oplus$ 表示两个比特串的异或，f 是一个函数(f 将在下面描述)，$K_1,K_2,\cdots,K_{16}$都是密钥 K 的函数，长度均为 48 比特(实际上，每一个 K_i 是来自密钥 K 的比特的一个置换选择)，$K_1,K_2,\cdots,K_{16}$构成了密钥方案。

(3) 对比特串 $R_{16}L_{16}$应用初始置换 IP 的逆置换 IP^{-1}，获得密文 y，即 $y=IP^{-1}(R_{16}L_{16})$。注意最后一次迭代后，左边和右边未交换，而将 $R_{16}L_{16}$作为 IP^{-1}的输入，目的是为了使算法可同时用于加密和解密。

函数 $f(A,J)$ 的第一个变量 A 是一个长度为 32 的比特串，第二个变量 J 是一个长度为 48 的比特串，输出是一个长度为 32 的比特串，f 的计算过程如下:

(1) 将 f 的第一个变量 A 根据一个固定的扩展函数 E 扩展成一个长度为 48 的比特串。

(2) 计算 $E(A) \oplus J$，并将所得结果分成 8 个长度为 6 的比特串，记为 $B = B_1B_2B_3B_4B_5B_6B_7B_8$。

(3) 使用 8 个 S-盒 $S_1, S_2, \cdots, S_8$。每一个 S_i 是一个固定的 4× 16 阶矩阵，它的元素来自 0 到 15 这 16 个整数。给定一个长度为 6 的比特串，比方说 $B_j = b_1b_2b_3b_4b_5b_6$，我们按下列办法计算 $S_j(B_j)$：用两个比特 b_1b_6 对应的整数 $r(0 \leq r \leq 3)$ 来确定 S_j 的行(所谓两个比特 b_1b_6 对应的整数 r 意指 r 的二进制表示为 b_1b_6，以下的含义类同)，用 4 个比特 $b_2b_3b_4b_5$ 对应的整数 $c(0 \leq c \leq 15)$ 来确定 S_j 的列，$S_j(B_j)$ 的取值就是 S_j 的第 r 行第 c 列的整数所对应的二进制表示。记 $C_j = S_j(B_j)$，$1 \leq j \leq 8$。

(4) 将长度为 32 的比特串 $C = C_1C_2C_3C_4C_5C_6C_7C_8$ 通过一个固定的置换 P 置换，将所得结果 $P(C)$ 记为 $f(A, J)$。

下面我们来描述 DES 中所使用的具体函数和密钥方案的计算。

初始置换 IP 及其逆置换 IP^{-1} 如表 2.2.1 和表 2.2.2 所示。

表 2.2.1　初始置换 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 2.2.2　初始逆置换 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

这意味着 x 的第 58 比特是 IP(x) 的第 1 比特，x 的第 50 比特是 IP(x) 的第 2 比特，等等。初始置换 IP 及其逆置换 IP^{-1} 没有密码意义，因为 x 与 IP(x)(或 y 与 $IP^{-1}(y)$)的一一对应关系是已知的。它们的作用在于打乱原来输入 x 的 ASCII 码字划分的关系，并将原来明文的检验位 $x_8, x_{16}, \cdots, x_{64}$ 变成 IP 的输出的一个字节。

扩展函数 E 如表 2.2.3 所示。置换 P 如表 2.2.4 所示。

表 2.2.3　扩展函数 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	1

表 2.2.4　置换 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

密钥方案的计算:每一轮都使用不同的、从初始密钥(又称种子密钥)K 导出的 48 比特密钥 K_i。K 是一个长度为 64 的比特串,实际上它只有 56 比特密钥,在第 8, 16, …, 64 位为校验比特,共 8 个,这主要是为了检错。在位置 8, 16, …, 64 的比特是按下述办法给出的:使得每一个字节(8 比特长)含有奇数个 1。因此在每一个字节中的一个错误能被检测出。在密钥方案的计算中,不考虑校验比特。密钥方案的计算过程如下:

(1) 给定一个 64 比特的密钥 K,删掉 8 个校验比特并利用一个固定的置换 PC-1 置换 K 的剩下的 56 比特,记 $PC\text{-}1(K) = C_0D_0$,这里 C_0 是 PC-1(K)的前 28 比特,D_0 是 PC-1(K)的后 28 比特。

(2) 对每一个 i, $1 \le i \le 16$, 计算

$$C_i = LS_i(C_{i-1})$$

$$D_i = LS_i(D_{i-1})$$

$$K_i = PC\text{-}2(C_iD_i)$$

其中 LS_i 表示一个或两个位置的左循环移位,当 i= 1, 2, 9, 16 时,移一个位置,当 i= 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15 时,移两个位置。PC-2 是另一个固定置换。

置换 PC-1 和置换 PC-2 分别如表 2.2.5 和表 2.2.6 所示。

表 2.2.5　置换 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

表 2.2.6　置换 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	30	36	29	32

8 个 S-盒如表 2.2.7 所示。

表　2.2.7

行＼列	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
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	S_1
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	
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	S_2
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	

续表

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

采用同一算法实现解密，把密文 y 作为输入，倒过来使用密钥方案即以逆序 K_{16}，K_{15}，…，K_1 使用密钥方案，输出将是明文 x。

S-盒的设计：S-盒是 DES 算法的心脏，DES 靠它实现非线性变换，关于 S-盒的设计准则还没有完全公开。许多密钥学家怀疑 NSA 设计 S-盒时隐藏了“陷门”，使得只有他们才可以破译算法，但没有证据能表明这一点。在 1976 年，NSA 披露了 S-盒的下面几条设计原则：

P_0. 每一个 S-盒的每一行是整数 0 到 15 的一个置换；

P_1. 每个 S-盒的输出都不是它的输入的线性或仿射函数；

P_2. 改变 S-盒的一个输入比特，其输出至少有两比特产生变化；

P_3. 对任何 S-盒和任何输入 x，S(x) 和 S(x　001100) 至少有两比特不同(这里 x 是一个长度为 6 的比特串)；

P_4. 对任何 S-盒和任何输入 x，以及 e，f ∈{0，1}，S(x) ≠S(x　11ef 00)，其中 x 是

一个长度为 6 的比特串;

P_5. 对任何 S-盒, 当它的任一输入位保持不变, 其他 5 位输入变化时, 输出数字中的 0 和 1 的总数接近相等。

穷尽密钥搜索攻击: 对 DES 的安全性批评意见中, 较为一致的看法是 DES 的密钥太短, 其密钥长度为 56 比特, 密钥量为 $2^{56} \approx 10^{17}$ 个, 不能抵抗穷尽密钥搜索攻击(所谓穷尽密钥搜索攻击是指攻击者在得到一组明文-密文对条件下, 可对明文用不同的密钥加密, 直到得到的密文与已知的明文-密文对中的相符, 就可确定所用的密钥, 也许有不只一个这样的密钥), 事实证明的确如此。1997 年 1 月 28 日, 美国的 RSA 数据安全公司在 RSA 安全年会上公布了一项"秘密密钥挑战"竞赛, 分别悬赏一千美金、五千美金和一万美金用于攻破不同密钥长度的 RC5, 同时还悬赏一万美金破译密钥长度为 56 比特的 DES。RSA 发起这场挑战赛是为了调查 Internet 上分布式计算的能力, 并测试不同密钥长度的 RC5 和密钥长度为 56 比特的 DES 的相对强度。到目前为止, 密钥长度为 40 比特和 48 比特的 RC5 已被攻破, 美国克罗拉多州的程序员 Verser 从 1997 年 3 月 13 日起, 用了 96 天的时间, 在 Internet 上数万名志愿者的协同工作下, 于 6 月 17 日成功地找到了 DES 的密钥, 获得了 RSA 公司颁发的一万美金的奖励。这一事件表明依靠 Internet 的分布式计算能力, 用穷尽密钥搜索攻击方法破译 DES 已成为可能。从而使人们认识到随着计算能力的增长, 必须相应地增加算法的密钥长度。1998 年 7 月电子边境基金会(EFF)使用一台 25 万美元的电脑在 56 小时内破解了 56 比特的 DES。1999 年 1 月 RSA 数据安全会议期间, 电子边境基金会用 22 小时 15 分钟就宣告完成 RSA 公司发起的 DES 的第三次挑战。

2.3 国际数据加密算法(IDEA)

X. J. Lai 和 J. L. Massey 提出的第一版 IDEA 于 1990 年公布, 当时称为 PES(建议加密标准)。1991 年, 在 Biham 和 Shamir 对其采用了差分密码分析之后, 设计者为抗此种攻击, 增加了他们的密码算法的强度。他们把新算法称为 IPES, 即改进型建议加密标准。1992 年, 设计者又将 IPES 改名为 IDEA。IDEA 的明文和密文分组都是 64 比特, 秘密密钥的长度是 128 比特, 同一算法既可用于加密又可用于解密, 该算法所依据的设计思想是"混合使用来自不同代数群中的运算"。该算法所需要的"混乱"可通过连续使用三个"不相容"的群运算于两个 16 比特子块来获得, 并且该算法所选择使用的密码结构可提供必要的"扩散"。该算法的密码结构的选择也考虑了该密码算法硬件和软件实现功能。

IDEA 的描述: IDEA 是由 8 轮和随后的一个输出变换组成, 图 2.3.1 所示的计算框图刻画了该密码算法的整个第一轮和输出变换。

在三个不同的群运算中, 要特别注意模 $2^{16}+1$ 整数乘法运算 $\odot$, 这里除了将 16 比特的全零子块处理为 2^{16} 外, 其余 16 比特的子块均按通常处理成一个整数的二进制表示对待, 例如, $(0, 0, \cdots, 0) \odot (1, 0, \cdots, 0) = (1, 0, \cdots, 0, 1)$, 这是因为 $2^{16}2^{15} \bmod (2^{16}+1) = 2^{15}+1$。

64 比特明文块 x 被分成 4 个 16 比特子块 x_1, x_2, x_3, x_4, 即 $x = x_1x_2x_3x_4$, 然后这 4 个 16 比特明文子块被变成 4 个 16 比特的密文子块 y_1, y_2, y_3, y_4, 即 $y = y_1y_2y_3y_4$。由明文变