第3章 经典信息加密方法

夫事以密成，语以泄败，未必其身泄之也；而语及所匿之事，如此者身危。

——《韩非子·说难》

谋成于密，败于泄。三军之事，莫重于密。

——《兵经百言》

加密与解密是既古老又新兴的技术，从最初仅能够提供机密性发展到提供完整性、真实性和非否认性等属性，成为保障信息安全的核心基础技术。密码技术大体上分为对称和非对称两类，分别对应私钥和公钥，前者加密、解密密钥相同或容易相互导出，后者加密、解密密钥相关但不同。对称密码主要用于提供机密性，当前主要包括分组密码、序列密码（也称流密码）；非对称密码由于效率比对称密码低，主要用于数字签名和密钥交换等场合。

第二次世界大战时期，人们已通过不断完善古典密码逐渐获得了一些设计对称密码的原则，Shannon 于 1949 年提出保密通信模型，之后对称密码尤其是分组密码逐步获得发展，美国国家标准机构先后征集和颁布了数据加密标准（Data Encryption Standard，DES）和高级加密标准（Advanced Encryption Standard，AES）。Diffie 和 Hellman 于 1976 年发表在著名刊物《信息理论》上的论文《密码编码学新方向》（*New Directions in Cryptography*），开创了公钥密码学的新纪元。在随后密码学的发展中，出现了如 RSA 算法等大量密码体系和相关的密钥管理技术，密码技术体系逐渐完善。当前，计算机密码学成为信息安全领域的主要研究方向。

本章的主要目的是使学生通过案例、古典的 Caesar 密码等了解密码体系，理解常见的密码术语，特别是加密算法、密钥等；通过古典密码体系的演化了解密码发展过程；重点掌握对称密码与非对称密码的精髓和区别；熟悉 DES 算法和 RSA 算法。

密码学（Cryptology）源于希腊语 kryptós（意为“隐藏的”）和 gráphein（意为“书写”）。密码学是在编码与破译的斗争实践中逐步发展起来的，随着先进科学技术的应用，已成为一门综合性的尖端技术。它的实用研究成果，特别是各国政府现用的密码编制及破译手段都具有高度的保密性。

小小的密码可以决定战争的胜负。例如，1942 年英军和德军在北非展开激战，春夏之交，德国著名的“沙漠之狐”隆梅尔率领德国非洲军团横扫北非，英军一溃千里，6 月退守阿拉曼，后来才守住阵地。8 月，英国名将蒙哥马利出任英国非洲军司令，他率军反攻，同时，英军有效地切断了德军的补给线，几乎每支横穿地中海的德军补给船队都受到英国海空军的拦截。隆梅尔指挥德军进行了顽强的抵抗，终因补给不足、增援无望而败北。这一仗是非洲战争的转折点，从此盟军掌握了战场上的主动权。对阿拉曼战役，史家论述甚详，但其中的一个细节——英军何以能准确地拦截到几乎所有的德军补给船队——却一直是个谜。直到 20 世纪 70 年代才露出谜底：当时数学家图灵领导的一个小组成功破译了德军的密码！

破译工作最出色的是美国。第二次世界大战期间，日本采用的最高级别加密手段是采用 M-209 转轮机械加密改进型——“紫密”，在手工计算的情况下不可能在有限的时间内破解。美国利用 1942 年制造的计算机轻松地破译了日本的“紫密”密码，使日本在中途岛海战中一败涂地，日本海军的主力损失殆尽。1943 年，在解密后获悉日本山本五十六将于 4 月 18 日乘中型轰炸机，由 6 架战斗机护航，到中途岛视察时，罗斯福总统亲自做出决定截击山本五十六，山本五十六乘坐的飞机在飞往中途岛的途中被美机击毁，山本五十六坠机身亡，日本海军从此一蹶不振。密码学的发展直接影响了第二次世界大战的战局。

3.1 从 Enigma 密码机认识密码

密码学充满神奇和挑战，激励人们为之奋斗终生。密码学和数学有千丝万缕的关系，有人觉得这很枯燥；密码学与计算机相关联，有人觉得这很纷繁复杂。但这是一场智慧的角力，从密码的设计到破解无一不闪耀着智慧的光芒；这也是一场耐心的竞赛，只有沉得住气的人才会获得成功。

在密码学史中，Enigma 密码机（恩尼格玛密码机，又译哑谜机或谜）是一种用于加密与解密文件的密码机。确切地说，Enigma 是一系列相似的转子机械的统称，它包括许多不同的型号，图 3-1 所示为 Enigma 密码机的关键部件。

Enigma 密码机在 20 世纪 20 年代早期开始用于商业，一些国家的军队与政府也曾使用过它，主要使用者是第二次世界大战时的纳粹德国。

在 Enigma 密码机的所有版本中，最著名的是德国使用的军用版本。电影《猎杀 U-571》告诉人们 Enigma 密码机是战争中同盟国费尽心机想要获得的尖端秘密，是战胜德国海军潜艇的关键所在。历史也确实如此，对潜艇尤其是德国海军“狼群”战术来说，无线电通信是潜艇在海面上活动获取信息通报情况的最重要手段，而 Enigma 密码机则是关乎整个无线电通信安全的设备，其重要性可想而知。

在使用中，Enigma 密码机每天都需要一份键盘设置清单和一些附加文件。德国海军用 Enigma 密码机的操作步骤比其他军种使用得更复杂、更安全。海军的密码本是用水溶性的红色墨水在粉色纸上印制而成的，这样可以在它可能被敌人缴获的时候轻松地将它销毁。图 3-2 所示为盟军从德军 U-505 号潜艇上缴获的 Enigma 密码本。

尽管 Enigma 密码机的安全性较高，但盟军的密码学家们还是成功地破译了大量由这种机器加密的信息。1932 年，密码学领域“波兰三杰”，即马里安·亚当·雷耶夫斯基（Marian Adam Rejewski，1905—1980 年）、耶日·维托尔德·鲁日茨基（Jerzy Witold Różycki，1909－1942 年）和亨里克·佐加尔斯基（Henryk Zygalski，1906—1978 年），根据 Enigma 密码机的原理破解

了它。1939 年中期，波兰政府将此破解方法告知了英国和法国。盟军的情报部门将破译出来的密码称为 ULTRA，这极大地帮助了西欧的盟军部队。ULTRA 到底有多大贡献还在争论中，但是人们都普遍认为盟军在西欧的胜利能够提前两年，完全是因为 Enigma 密码机被成功破解。

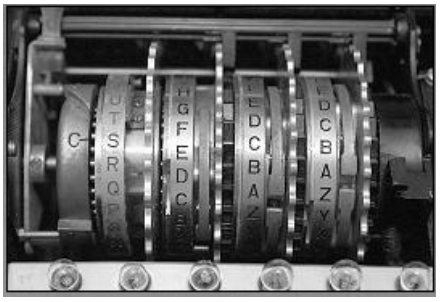


图 3-1　Enigma 密码机的关键部件——转子［3 个转子位于右边的固定接口和左边（标着 C）的反射器两个装置之间］

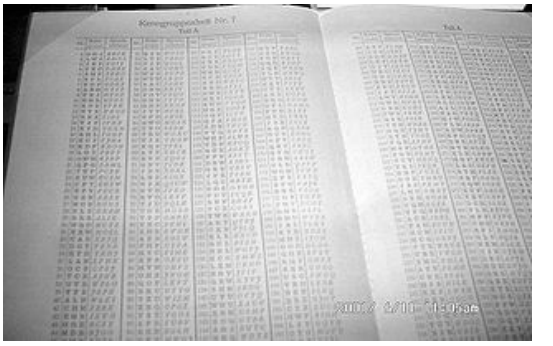


图 3-2　Enigma 密码本

在第二次世界大战期间，Enigma 密码机是在图 3-3 所示的美丽的 Bletchley Park（布莱切利园，又称为 Station X，即 X 电台，是一座位于英格兰米尔顿凯恩斯布莱切利镇内的宅第）被破解的。密码专家在 Bletchley Park 曾破解不少轴心国的密码与密码文件系统。正因如此，Bletchley Park 一度成为解密中心。

图 3-3　Bletchley Park 独特建筑

3.2　初识密码学

3.2.1　从密码的起源了解密码

早期的密码技术主要用于提供机密性，最早可以追溯到公元前 2000 年。在古埃及的尼罗河畔，一位擅长书写者在贵族的墓碑上撰写铭文时有意用加以变形的象形文字而不是普通的象形文字。这种文字由复杂的图形组成，其含义只被为数不多的人掌握，如图 3-4 所示。这是史载的最早的密码形式。

历史上第一件军用密码装置是公元前 5 世纪的斯巴达密码棒（Scytale），如图 3-5 所示，它采用了密码学上的移位法（Transposition）。移位法是将信息内字母的次序调动，而密码棒采用了字条缠绕木棒的方式，把字母进行移位。收信人要使用相同直径的木棒才能得到还原的信息。

图 3-4　古埃及贵族墓碑上的铭文

图 3-5　密码棒（Scytale）

古代隐写术也是战时传递秘密信息的重要手段。罗马“历史之父”希罗多德以编年史的形式记载了公元前 5 世纪希腊和波斯间的冲突，其中介绍到正是由于一种叫隐写术的技术才使希腊免遭波斯暴君薛西斯一世征服的厄运。薛西斯花了足足 5 年的战争准备，计划于公元前 480 年对希腊发动一场出其不意的进攻。但是波斯的野心被一名逃亡在外的希腊人德马拉图斯发现了，他决定给斯巴达带去消息，告诉他薛西斯的侵犯企图。可问题是消息怎样送出才不被波斯士兵发现。他利用一副已上蜡的可折叠刻写板，先将消息刻写在木板的背面，再涂上蜡盖住消息，这样刻写板看上去没写任何字。最终希腊人得到了消息，并提前做好了战争准备，致使薛西斯的侵略失败。德马拉图斯的保密做法与中国古人有异曲同工之妙。中国古人将信息写在小块丝绸上，塞进一个小球里，再用蜡封上，然后让信使吞下这个蜡球以保证信息安全。这种方法在现代电视剧《暗算》中多次使用。

最早将现代密码学概念运用于实际的是恺撒大帝（Gaius Julius Caesar，盖厄斯·尤利乌斯·恺撒，公元前 100—前 44 年，见图 3-6），他是古罗马帝国末期著名的统帅和政治家。虽然他一生从未登上过皇位，但是直到今天在西方国家，他的名字仍是君主的代名词。他博学多才、文武双全，既是卓越的军事家又是雄辩的文学家。在掌权期间，恺撒南征北伐使罗马的版图得到了空前的扩大，他还把自己的亲身经历写成著名的战争回忆录——《高卢战记》和《内战记》。我们现在使用的公历就是从他所采用的“儒略历”演变过来的。恺撒不相信负责他和他手下将领通信的传令官，因此他发明了一种简单的加密算法把他的信息加密，后来被称为 Caesar 密码（见图 3-7）。当恺撒说“Hw wx，Euxwh！”而不是“Et tu，Brute！”（“你这畜生！”）时，他的心腹会懂得他的意思。《高卢战记》中描述恺撒曾经使用密码来传递信息。值得一提的是，大约 2000 年后，联邦将军 A.S. Johnson（约翰逊）和 Pierre Beauregard（皮埃尔·博雷加德）在希洛战斗中再次使用了这种简易的密码。

Caesar 密码是将字母按字母表的顺序排列，并且最后一个字母与第一个字母相连。加密方法是将明文中的每个字母用其后面的第三个字母代替，就变成了密文。例如，“世博上海”

E X P O S H A N G H A I

的 Caesar 密码是

H A S R V K D Q J K D L

图 3-6　恺撒雕像

图 3-7　Caesar 密码

这很容易从 Caesar 密码的代替表（见表 3-1）得到。

表 3-1　Caesar 密码的代替表

明　文	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*
密　文	D	E	F	G	H	I	J	K	L	M	N	O	P
明　文	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*w*	*x*	*y*	*z*
密　文	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Caesar 密码是代替密码，属经典密码的一种，它将一组字母换成其他字母或符号。另一种经典密码是换位密码，它将字母的顺序重新排列。例如，给出密文：

OPXEIAHGNAHS

你能猜出这是什么意思吗？我们只要将每个单词倒过来读，就会迅速恢复明文：

SHANGHAIEXPO

再如，在美国南北战争时期，军队曾经使用过双轨式密码，也称为栅栏密码，加密时先将明文写成双轨的形式，如将 shanghai expo 写成

s a g a e p

h n h i x o

然后按行的顺序书写即可得出密文：sagaephnhixo。解密时，先计算密文中字母的总数，然后将密文分成两部分，排列成双轨形式后按列的顺序读出，即恢复明文。

在第一次世界大战期间，德国间谍曾经依靠字典来编写密文。例如，100-3-16 表示某字典的第 100 页第 3 段的第 16 个单词。但是，这种加密方法并不可靠，美国情报部门搜集了所有德文字典，只用几天时间就找出了德方所用的字典，从而破译了这种密码，致使德军损失惨重。

计算机的出现，大大地促进了密码学的变革，正如德国学者 T.Beth 所说：“突然，现代密码学从半军事性的角落里解脱出来，一跃成为通信科学一切领域中的中心研究课题。”由于商业应用和大量计算机网络通信的需要，人们对数据保护、数据传输的安全性越来越重视，这更大大地促进了密码学的发展与普及。

密码学的发展大致分为 3 个阶段。

第一阶段：古代到 1949 年

这个阶段的密码技术可以说是一种艺术，而不是一种科学，密码学专家常常是凭知觉和信念来进行密码设计和分析的，而不是推理和证明，没有形成密码学的系统理论。这个阶段设计

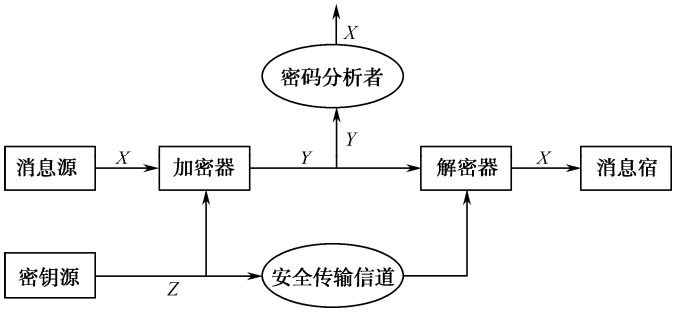
的密码称为经典密码或古典密码。

这个阶段发明的密码算法在现代计算机技术条件下都是不安全的，但是其中的一些算法思想（如代替、换位）是分组密码算法的基本模式。

密码棒（Scytale）属于这一时期的杰作。

第二阶段：1949—1975 年

1949 年 C.E.Shannon（香农）发表在《贝尔实验室技术杂志》上的《保密系统的信息理论》（*Communication Theory of Secrecy System*）为私钥密码体系（对称密码体系）建立了理论基础，从此密码学成为一门科学。图 3-8 所示为 Shannon 提出的保密通信模型。密码学直到今天仍具有艺术性，是一门具有艺术性的科学。在这段时期，密码学理论的研究工作进展不大。



X—明文；*Y*—密文；*Z*—数字信号

图 3-8　Shannon 提出的保密通信模型

20 世纪 70 年代，在 IBM 沃森公司工作的 Pfister 提出了一种被称为 Pfister（菲斯特）密码的密码体系，成为当今著名的数据加密标准（Data Encryption Standard，DES）的基础。1976 年，Pfister 和美国国家安全局（National Security Agency，NSA）一起制定了 DES，这是一个具有深远影响的分组密码算法。

这一时期，美、英、法等许多国家已投入大量人力和物力进行相关研究；另外，作为个人，既没有系统的知识，更没有巨大的财力来从事密码学研究。这一状况一直持续到 1967 年 David Kahn 发表了《破译者》（*The Code Breakers*）一书，它详尽地阐述了密码学的发展和历史，使人们开始了解和接触密码。

第三阶段：1976 年至今

1976 年 Diffie 和 Hellman 发表的论文《密码编码学新方向》引发了密码学的一场革命。他们首先证明了在发送端和接收端无密钥传输的保密通信是可能的，从而开创了公钥密码学的新纪元。从此，密码开始充分发挥它的商用价值和社会价值。

1978 年，在 ACM 通信中，Rivest、Shamir 和 Adleman 公布了 RSA 密码体系，这是第一个真正实用的公钥密码体系，可以用于公钥加密和数字签名。在 EuroCrypt'91 年会上，瑞士联邦技术学院 X. J. Lai 和 James L. Massey 提出了 IDEA，成为分组密码发展史上的又一个里程碑。

为了对付美国联邦调查局（Federal Bureau of Investigation，FBI）对公民通信的监控，Zimmerman 在 1991 年发布了基于 IDEA 的免费电子邮件加密软件 PGP。该软件提供了具有军用安全强度的算法并得到广泛传播，因此成为一种事实标准。

总之，在实际应用方面，古典密码算法有代替密码和换位密码，对称密码算法包括 DES

算法和 AES 算法，非对称密码算法包括 RSA 算法、背包算法、Rabin 算法和椭圆曲线密码算法等。目前，在数据通信中使用较普遍的算法有 DES 算法和 RSA 算法等。

3.2.2　从基本概念了解密码

密码学的基本目的是使得两个在不安全信道中通信的人，称为 Alice 和 Bob，以一种使他们敌手 Cracker 不能明白和理解通信内容的方式进行通信。不安全信道在实际中是普遍存在的，如电话线或计算机网络。Alice 发送给 Bob 的未被加密的信息，通常称为明文（Plaintext），如英文单词、数字、符号和图像。Alice 使用预先商量好的密钥（Key）对明文进行加密，加密过的明文称为密文（Ciphertext），Alice 将密文通过信道发送给 Bob。对于 Cracker，他可以窃听到信道中 Alice 发送的密文，但是无法知道其所对应的明文；而对于接收者 Bob，由于他知道密钥，可以对密文进行解密，从而获得明文。图 3-9 所示为加密通信的基本过程。

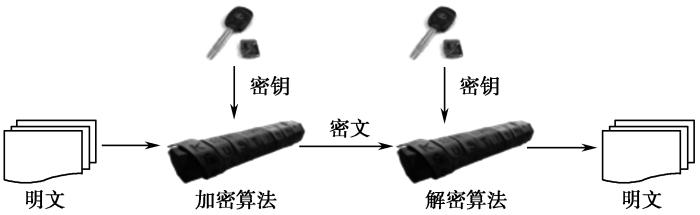


图 3-9　加密通信的基本过程

1. 基本概念

- 明文消息（Plaintext）：未加密的原消息，简称明文。
- 密文消息（Ciphertext）：加密后的消息，简称密文。
- 加密（Encipher、Encode）：明文到密文的变换过程。
- 解密（Decipher、Decode）：密文到明文的恢复过程。
- 加密算法（Encryption Algorithm）：对明文进行加密时所采用的一组规则的集合。
- 解密算法（Decryption Algorithm）：对密文进行解密时所采用的一组规则的集合。
- 密码算法强度（Algorithm Strength）：对给定密码算法的攻击难度。
- 密钥（Key）：加、解密过程中只有发送者和接收者知道的关键信息，分为加密密钥（Encryption Key）和解密密钥（Decryption Key）。
- 密码分析（Cryptanalysis）：虽然不知道系统所用的密钥，但通过分析可能从截获的密文推断出原来的明文，这一过程称为密码分析。
- 密码编码学（Cryptography）：主要研究对信息进行编码，实现对信息的隐蔽。
- 密码分析学（Cryptanalytics）：主要研究加密消息的破译或消息的伪造。
- 密码学（Cryptology）：由密码编码学和密码分析学组成，前者寻求提供信息机密性、完整性、真实性和非否认性等的方法，后者研究加密消息的破译和伪造等破坏密码技术所能提供安全性的方法。

2. 密码体系的基本类型

在密码技术的发展中出现了各种密码体系（Cryptosystem），它是明文变换密文的法则。密码体系也常被称为密码方案（Scheme），它指一个密码算法、相关参数及其使用方法的总和，其中，参数主要包括密钥、明文和密文。指示这种变换的参数，称为密钥。它们是密码编制的

重要组成部分。

密码体系的基本类型有 4 种。

1）错乱（也可称换位）：按照规定的图形和线路，改变明文字母或数码等的位置成为密文。

2）代替：用一个或多个代替表将明文字母或数码等代替为密文。

3）密本：用预先编定的字母或数字编码组，代替一定的词组、单词等明文为密文。

4）加乱：用有限元素组成的一串序列（全为乱数），按规定的算法，同明文序列相结合变成密文。

当然，上述 4 种密码体系可以混合使用。

密码体系由密码算法和密钥组成。例如，前面提到的 Caesar 密码体系的密码算法是代替算法，密钥 r=3（即每个字母向后移 3 位）。再如，密码棒（Scytale）密码体系中，密码算法是错乱算法，密钥是棒的直径。

直觉上，若密码算法也是保密的，则安全性更高，但这往往不现实，因为开发密码算法的人一般不是使用密码的人。Kerckhoffs 早在 1883 年就指出，密码算法的安全性必须建立在密钥保密的基础上，即使敌手（Opponent）知道算法，若不掌握特定密钥也应难以破解密码，这就是著名的 Kerckhoffs 准则。

3. 密码体系举例说明

以表 3-1 所示的 Caesar 密码为例，假定数字 0, 1, 2, …, 24, 25 分别和字母 a, b, c, …, y, z 相对应，如表 3-2 所示。

表 3-2　字母与数字对应表

字　母	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*
数　字	0	1	2	3	4	5	6	7	8	9	10	11	12
字　母	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*w*	*x*	*y*	*z*
数　字	13	14	15	16	17	18	19	20	21	22	23	24	25

密文字母对应的数字 c 可以用明文字母对应的数字 p 表示为

$$c \equiv (p+3) \bmod 26 \tag{3-1}$$

其中，mod 为模运算。若明文字母为 y，即 p=24，则

$$c \equiv (24+3) \bmod 26 = 1$$

因此密文为 B。

式（3-1）是 Caesar 密码的数学形式，也表示一种算法，Caesar 密码体系即由式（3-1）和其中密钥 3 组成。我们不知道当时恺撒（Caesar）为什么偏爱数字 3，他其实可以选择 1～25 之中的任何一个数字作为密钥。因此，式（3-1）可以推广成任意密钥 k，即

$$c \equiv (p+k) \bmod 26 \tag{3-2}$$

这其实就是移位密码。这里，$k \in K$，$K = \{1,2,3,\cdots,24,25\}$，$K$ 是密钥集合或称密钥空间。

一个密码体系是满足以下条件的五元组（P, C, K, E, D）：

1）P 是所有可能的明文集合；

2）C 是所有可能的密文集合；

3）K 是所有可能的密钥集合；

4）任意 $k \in K$，有一个加密算法 $e \in E$ 和相应的解密算法 $d \in D$，使得 $e(x)$ 和 $d(x)$ 分别为

加密和解密函数，满足 $d(e(x))=x$，这里 $x\in P$。

上述移位密码的密码体系描述如下。

密码体系 3.1　移位密码

令 P=C={0, 1, 2, …, 24, 25}，K={1, 2, 3, …, 24, 25}，对于 $k\in K$，任意 x∈{0, 1, 2, …, 24, 25}，定义

$$e(x)=(x+k)\bmod 26 \tag{3-3}$$

及

$$d(e(x))=(e(x)-k)\bmod 26 \tag{3-4}$$

算法是一些公式、法则或程序，它规定明文和密文之间的变换方法；密钥可以看成算法中的参数。例如，在式（3-2）中取 $k=3$，就可以得到式（3-1），即 Caesar 密码；如果取 $k=25$，就可以得出美军多年前使用过的一种加密算法，即将明文中的字母用其前面的字母取代形成密文的方法。例如，当明文是 shanghai expo 时，则对应的密文是 RGZMFGZH DWON。

密码体系 3.2　Hill（希尔）密码

设 m≥2 为正整数，$\boldsymbol{P}$=$\boldsymbol{C}$={0, 1, 2, …, 24, 25}^{m}，且 $\boldsymbol{K}$ 为定义在{1, 2, 3, …, 24, 25}^{m} 上的 $m\times m$ 可逆矩阵，$\boldsymbol{X}$ 为定义在{0, 1, 2, …, 24, 25}^{m} 上的 $m\times m$ 可逆矩阵，对任意的密钥 $\boldsymbol{K}$，定义加密变换：

$$\boldsymbol{E}(\boldsymbol{X})=(\boldsymbol{K}\boldsymbol{X})\bmod 26$$

解密变换：

$$\boldsymbol{D}(\boldsymbol{E}(\boldsymbol{X}))=(\boldsymbol{K}^{-1}\boldsymbol{E}(\boldsymbol{X}))\bmod 26$$

例如，选取 2×2 的密钥，$\boldsymbol{K}=\begin{bmatrix}1 & 1\\ 3 & 4\end{bmatrix}$，明文 hill 的矩阵形态为 $\begin{bmatrix}h & l\\ i & l\end{bmatrix}=\begin{bmatrix}7 & 11\\ 8 & 11\end{bmatrix}$，加密过程

$\boldsymbol{E}(\boldsymbol{X})=(\boldsymbol{K}\boldsymbol{X})\bmod 26=\left(\begin{bmatrix}1 & 1\\ 3 & 4\end{bmatrix}\cdot\begin{bmatrix}7 & 11\\ 8 & 11\end{bmatrix}\right)\bmod 26=\begin{bmatrix}15 & 22\\ 53 & 77\end{bmatrix}\bmod 26=\begin{bmatrix}15 & 22\\ 1 & 25\end{bmatrix}$，而 $\begin{bmatrix}15 & 22\\ 1 & 25\end{bmatrix}=\begin{bmatrix}p & w\\ b & z\end{bmatrix}$，所以密文为 PBWZ。

算法是相对稳定的，不能想象在一个密码体系中经常改变加密算法。反之，密钥则是一个变量，密钥需要频繁更换。现代密码学的一个基本原则是一切秘密都存在于密钥之中，即在设计密码体系时，总是假设密码算法是公开的，真正需要保密的是密钥。所以，在分发和存储密钥时应当特别小心。

4. 根据密钥的特点对密码体系分类

根据密钥的特点将密码体系分为以下两种。

- 对称密码体系（Symmetric Cryptosystem）。
- 非对称密码体系（Asymmetric Cryptosystem）。

对称密码体系又称为私钥（Private Key）或单钥（One-Key）或传统（Classical）密码体系。在对称密码体系中，加密密钥和解密密钥是一样的或者彼此之间是容易相互确定的。私钥密码体系按加密方式可分为流密码（Stream Cipher）和分组密码（Block Cipher）两种。流密码是指将明文消息按字符逐位地进行加密。分组密码是指将明文消息分组（每组含有多个字符），逐组地进行加密。

非对称密码体系又称为公钥（Public Key）或双钥（Two-Key）密码体系。在非对称密码

体系中，加密密钥和解密密钥不同，从一个难以推出另一个，可将加密能力和解密能力分开。现在大多数公钥密码属于分组密码，只有概率密码体系属于流密码。

对称密码（私钥）的效率高，常用于数据量较大的保密通信中，而非对称密码（公钥）常用于数字签名、密钥分发等场合。

5. 对密码的攻击

评判密码算法安全性的重要方法是进行密码分析。在密码学术语中，“分析”与“攻击”意义相近，因此密码分析也可称为密码攻击。根据密码分析者破译时具备的条件，通常人们将攻击类型分为 4 类：①唯密文攻击（Ciphertext-only Attack），即分析者有一个或更多的用同一个密钥加密的密文；②已知明文攻击（Known Plaintext Attack），即除了待破解的密文，分析者还有一些明文和用同一密钥加密的对应密文；③选择明文攻击（Chosen Plaintext Attack），即分析者可得到所需要的任何明文对应的密文，这些密文和待破解的密文是用同一密钥加密的；④选择密文攻击（Chosen Ciphertext Attack），即分析者可得到所需要的任何密文对应的明文，类似地，这些密文和待破解的密文是用同一密钥加密的，获得密钥是分析者的主要目的。上述 4 种攻击类型的强度按序递增，如果一个密码体系能抵抗选择明文攻击，那么它当然能够抵抗唯密文攻击和已知明文攻击。

3.2.3 古典密码体系的演化

密码技术的应用一直伴随着人类文明的进步，其古老甚至原始的方法奠定了现代密码学的基础。使用密码的目标就是使一份消息或记录对非授权的人是不可理解，而原定的接收方能解读的。因此，不一定要求加密和解密方法特别复杂，它必须适应使用它的人员的智力、知识及环境。下面介绍古典密码体系的发展演化过程。

1. 信息隐藏

最为人们所熟悉的古典加密方法，莫过于隐写术。它通常将秘密消息隐藏于其他消息中，使真正的秘密通过一份无伤大雅的消息发送出去。隐写术分为两种，即语言隐写术和技术隐写术。技术方面的隐写比较容易想象：如不可见的墨水（如图 3-10 所示），橙汁法和牛奶法（如美国电影《国家宝藏》）也是普遍且有效的方法（只要在背面加热或紫外线照射即可复现）。语言隐写术与密码编码学关系比较密切，它主要提供两种类型的方法：符号码和公开代码。

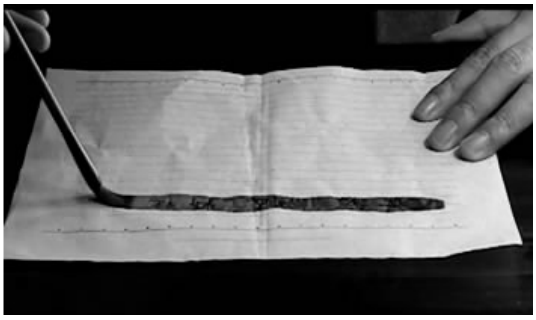


图 3-10　电视剧《暗算》剧照：涂上液体后隐藏信息显示

（1）符号码

符号码是以可见的方式，如手写体字或图形，隐藏秘密的书写符号；可以在书或报纸上标

记所选择的字母，如用点或短画线，这比上述方法更容易被人怀疑，除非使用显隐墨水，但此方法易于实现；一种变形的应用是降低所关心的字母，使其水平位置略低于其他字母，而这种降低几乎让人觉察不到。

（2）公开代码

一份秘密的信件或伪装的消息要通过公开信道传送，需要双方事前的约定，也就是需要一种公开代码。这可能是保密技术的最古老形式。古代东方及远东的商人和赌徒在这方面有独到之处，他们非常熟练地掌握了手势和表情的应用。在美国的纸牌骗子中较为盛行的方法有：手拿一支烟或用手挠一下头，表示所持的牌不错；一只手放在胸前并且跷起大拇指，意思是“我将赢得这局，有人愿意跟我吗？”；右手手掌朝下放在桌子上，表示“是”，手握成拳头表示“不”。特定行业或社会阶层经常使用的语言，往往被称为行话。一些乞丐、流浪汉及地痞流氓使用的语言还被称为黑话，它们是这些社会群体的护身符。其实这些信息也是利用了伪装，伪装的秘密因此也称为专门隐语。曲波的长篇小说《林海雪原》中写到杨子荣进威虎山时，记载了很多类似的说法，像“蘑菇溜哪路？什么价？”“天王盖地虎，宝塔镇河妖”等，就是东北土匪的一种黑话。法语也有很多例子，其中有的现在还成了通俗用法。例如，rossignol（夜莺）表示“万能钥匙”，最早始于 1460 年；mouche（飞行）表示“告密者”等。

公开代码的第二种类型就是利用虚码和漏格进行隐藏。隐藏消息的规则比较常见的有某个特定字符后的第几个字符，如空格后的下一个字母（“家庭代码”，第二次世界大战中在参战士兵中广为流传，但引起了审查机关的极大不满），更好一些的还有空格后的第三个字母，或者标点符号后的第三个字母。

漏格方法可以追溯到卡达诺（Cardano，1550 年）时代，这是一种容易掌握的方法，但不足之处是双方需要相同的漏格，特别是战场上的士兵，使用时不太方便。

2．代替密码

代替密码就是将明文字母表中的每个字符替换为密文字母表中的字符。这里对应密文字母可能是一个，也可能是多个。接收者对密文进行逆向替换即可得到明文。代替密码有 5 种表现形式。

（1）单表代替密码

单表代替密码即简单代替密码，或者称为单字母代替密码，明文字母表中的一个字符对应密文字母表中的一个字符。这是所有加密中最简单的方法。

（2）多名码代替密码

多名码代替密码就是将明文字母表中的字符映射为密文字母表中的多个字符。多名码代替密码早在 1401 年就由 DuchyMantua 公司使用。在英文中，元音字母出现频率最高，降低对应密文字母出现频率的一种方法就是使用多名码。

（3）多音码代替密码

多音码代替密码就是将多个明文字符代替为一个密文字符。例如，将字母 C 和 M 对应的 K、A 和 Z 代替为 L。最古老的这种多字母加密方式始见于 1563 年由波他的《密写评价》（*Defurtiois Literarum Notis*）一书。

（4）多表代替密码

多表代替密码由多个单表代替密码组成，也就是使用了两个或两个以上的代替表。例如，使用有 5 个简单代替表的代替密码，明文的第一个字母用第一个代替表，第二个字母用第二个表，第三个字母用第三个表，以此类推，循环使用这 5 个代替表。

多表代替密码由莱昂·巴蒂斯塔·阿尔贝蒂（Leon Battista Alberti，文艺复兴时期意大利的建筑师、建筑理论家、作家、诗人、哲学家、密码学家）于 1568 年发明。由 1586 年法国亨利三世王朝的外交官布莱兹·维吉尼亚（Blaise Vigenère）发明的、著名的维吉尼亚（Vigenère）密码及弗朗西斯·博福尔（Francis Beaufort）密码均是多表代替密码。表 3-3 为维吉尼亚表。维吉尼亚密码把 Caesar 密码做了另一种改进，增加密钥的长度，克服了 Caesar 密码的缺点，提高了密码的保密程度。两百年后，维吉尼亚密码被英国人巴比奇和德国人卡西斯基破译。由于英国情报机关的要求，巴比奇破译维吉尼亚密码的事一直到 20 世纪才公之于世。直到第一次世界大战结束，破译在与加密的角逐中占据上风。

表 3-3　维吉尼亚表

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

维吉尼亚密码是如何加密和解密的呢？

例如，如果明文为 shanghai expo，密钥为 THEDANCINGMEN，则密文是什么？

明文的第一个字母为 s，则先在表格中找到 S 列。由于密钥的第一个字母为 T，于是在 S 列从上往下找到 T。这一 T 对应的行号为 B，因而 B 便是密文的第一个字母。以此类推，可以得到密文。以下便是密钥为福尔摩斯探案集中电影名字 *The Dancing Men* 时的例子。

明文：SHANGHAIEXPO

密钥：THEDANCINGMEN

密文：BAEQUGCAJJXQ

解密时，以密文字母选择行，从此行中找到密钥字母，那么密钥字母所在的列号就是明文字母了。例如，要解密密文中第一个字母 B，在表中找到 B 行中对应的密钥字母 T，T 所在的列号 S 即为明文。

从上例中可以看到，对于同一个明文字母，其在明文中的位置不同，将得到不同的密文字母。例如，明文中的字母 H 可能对应的密文字母有 A 和 G，这样就在密文中消除了明文中字母出现频率的规律了。

多表代替密码显然比单表代替密码要好，但只要给密码分析员足够数量的密文样本，这个算法总是可以破译的，这里的关键在于密钥。所以，为了提高加密的安全性，通常采用的方法是加长密钥的长度。

（5）密本

密本不同于代替表，一个密本可能是由大量单词、片语、音节、字母这些明文单元和数字密本组组成的，如 1563-baggage、1673-bomb、2675-catch、2784-custom、3645-decide to、4728-from then on 等。在某种意义上，密本就是一个庞大的代替表，其基本的明文单位是单词和片语，字母和音节主要用来拼出密本中没有的单词。实际使用中，密本和代替表的区别还是比较明显的：代替表是按照规则的明文长度进行操作的，而密本是按照可变长度的明文组进行操作的。密本最早出现在 1400 年左右，后来大多应用于商业领域。第二次世界大战中的商船密本、美国外交系统使用的 GRAY 密本就是典型的例子。

3. 换位密码

在换位密码（也称置换密码）中，明文字符集保持不变，只是字母的顺序被打乱了。例如，简单的纵行换位，就是将明文按照固定的宽度定在一张图表纸上，然后按照垂直方向读取密文。

在第二次世界大战中，德军曾一度使用一种被称为 bchi 的双重纵行换位密码，而且作为陆军和海军的应急密码，只不过密钥字每天变换，并且在陆军团以下单位使用。此时英国人早就能解读消息了，即使使用两个不同的密钥字甚至三重纵行换位密码也无济于事。

在这种密码中，最简单的是 3.2.1 节提到的栅栏密码。破译这类密码很简单，一种更为复杂的方案是以一个矩形逐行写出消息，再逐列读出该消息，并以行的顺序排列，列的阶则成为该算法的密钥。

实例　采用一个字符串 SECURITY 为密钥，把明文 Electoral Law revision key to equal rights 进行列换位加密。

在列换位加密算法中，按照密钥各个字母大小的顺序排出列号，以列号的顺序将矩阵中的字母读出，就构成了密文。

密钥：SECURITY

明文：Electoral Law revision key to equal rights

密文：EAOQTLLIEHOEELBTRKAAELSOGRVYRCCWNUSAITID

密钥	S	E	C	U	R	I	T	Y
顺序	5	2	1	7	4	3	6	8
	E	L	E	C	T	O	R	A
	L	L	A	W	R	E	V	I
	S	I	O	N	K	E	Y	T
	O	E	Q	U	A	L	R	I
	G	H	T	S	A	B	C	D

3.2.4 对称密码算法的精粹

对称密码算法是指从加密信息使用的密钥可以推出解密信息的密钥，反之亦然。绝大多数对称密码算法使用的加密密钥和解密密钥都是相同的。典型的对称密码算法有 DES 算法、3DES 算法、AES 算法、RC5 算法等。实际上，前面介绍的 Caesar 密码、Hill 密码和换位密码等古典密码都是对称密码算法。

对称加密算法根据其工作方式，可以分成两类：一类是每次只对明文中的一个位（有时是对一个字节）进行运算的算法，称为序列加密算法；另一类是每次对明文中的一组位进行加密的算法，称为分组加密算法。现代典型的分组加密算法的分组长度是 64 位。这个长度既方便使用，又足以防止分析破译。对称密码算法的结构图如图 3-11 所示。

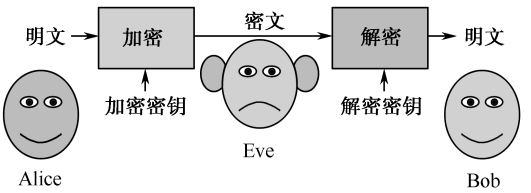


图 3-11　对称密码算法的结构图

DES（Data Encryption Standard，数据加密标准）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。64 位 DES 算法的详细情况已在美国联邦信息处理标准（EIPS PUB46）上发表，后来被国际标准化组织（International Standard Organization，ISO）采纳为国际数据加密标准。DES 以算法实现快、密钥简短等特点成为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，目前已广泛用于电子商务系统中。

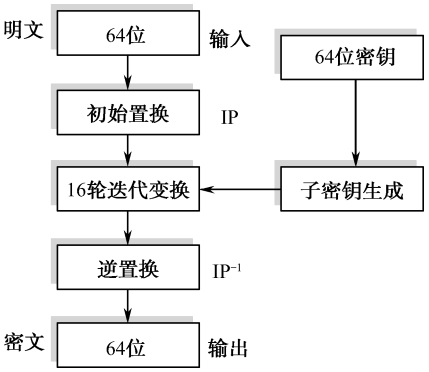


图 3-12　DES 算法加密过程的流程图

1. DES 算法流程

DES 算法是一个分组密码算法。对于任意长度的明文，首先对其进行分组，每组数据长度为 64 位（8 字节），然后分别对每个 64 位的明文分组进行加密。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 的整个体系是公开的，体系的安全性全靠密钥的保密。其加密过程大致分成 3 个步骤：初始置换、16 轮迭代变换（即后面介绍的 16 轮循环）和逆置换（即后面介绍的终结置换）。DES 算法加密过程的流程图如图 3-12 所示。

2. DES 算法加密过程

本部分内容较烦琐，可根据实际情况酌情选读。

（1）DES 算法的分组

DES 算法是一个分组密码算法，每次加密或解密的分组大小均为 64 位，所以 DES 算法没有密文扩充问题。对于大于 64 位的明文，只要按每 64 位一组进行切割即可；而对于小于 64 位的明文，只要在后面补 0 即可。

另外，DES 算法所用的加密或解密密钥也是 64 位，但因其中 8 位是奇偶校验位，所以 64 位密钥中真正起作用的只有 56 位，密钥过短也是 DES 算法最大的缺点。

DES 算法加密和解密所用的算法除了子密钥的顺序不同外，其他部分完全相同。DES 算法的结构图如图 3-13 所示。

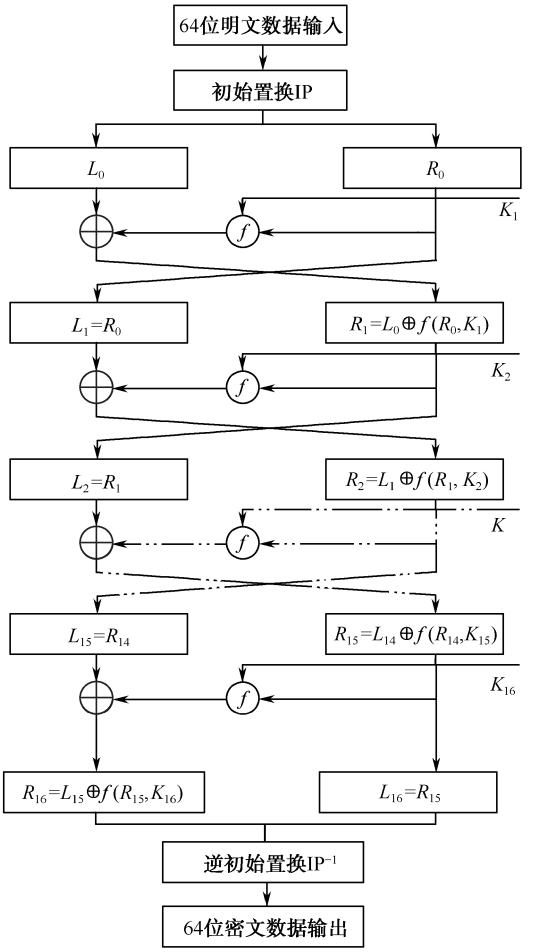


图 3-13　DES 算法的结构图

（2）初始置换

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），输入分组按照初始置换表重排次序，进行初始置换。置换方法如下：初始置换表（见表 3-4）从左到右、从上到下读取，如第 1 行第 1 列为 58，意味着将原明文分组的第 58 位置换到第 1 位，初始置换表的下一个数 50，意味着将原明文分组的第 50 位置换到第 2 位，

以此类推，将原明文分组的 64 位全部置换完成。

表 3-4　初始置换表

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

（3）16 轮循环

DES 算法对经过初始置换的 64 位明文进行 16 轮类似的子加密过程。每一轮的子加密过程要经过 DES 函数 f 变换，其过程如下。

1）将 64 位明文在中间分开，划分为两个部分，每部分 32 位，左半部分记为 L_0，右半部分记为 R_0，以下的操作都是对右半部分数据进行的。

2）扩展置换。首先要对 32 位右半部分明文数据进行扩展置换，扩展置换将 32 位的输入数据扩展成 48 位的输出数据，它有 3 个目的：第一，它产生了与子密钥同长度的数据以进行异或运算；第二，它提供了更长的结果，使得在以后的子加密过程中能进行压缩；第三，它产生雪崩效应（Avalanche Effect），这也是扩展置换最主要的目的，使得输入的一位将影响两个置换，所以输出对输入的依赖性将传播得更快。扩展置换的置换方法与初始置换相同，只是置换表不同，扩展置换表如表 3-5 所示。

表 3-5　扩展置换表

31	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

3）不进位加法运算（或异或运算）。将 48 位的明文数据与 48 位的子密钥进行异或运算（48 位子密钥的产生过程后面将详细讨论）。$0\oplus 0=0$，$0\oplus 1=1$，$1\oplus 0=1$，$1\oplus 1=0$。异或以后的 48 位结果将继续进行 S 盒置换。

4）S 盒置换。S 盒置换是 DES 算法中最重要的部分，也是最关键的步骤，因为其他运算都是线性的，易于分析，只有 S 盒置换是非线性的，它比 DES 算法中任何一步都提供了更强的安全性。

经过异或运算得到的 48 位输出数据要经过 S 盒置换，置换由 8 个盒完成，记为 S 盒。每个 S 盒都有 6 位输入、4 位输出，如图 3-14 和图 3-15 所示。

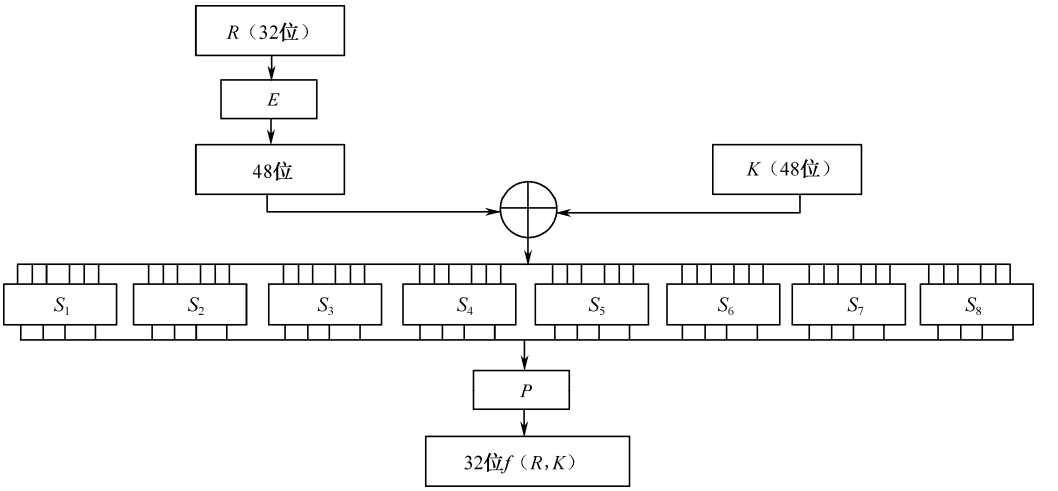


图 3-14　DES 算法中 f 变换（轮函数）

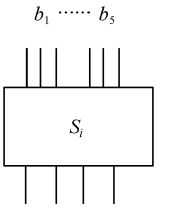


图 3-15　DES 算法中 S 盒示意

这 8 个 S 盒是不同的，每个 S 盒的置换方法如表 3-6 所示。

表 3-6　DES 算法中每个 S 盒的置换方法

		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	1	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	1	14	11	2	12	4	7	13	1	4	0	15	10	3	9	8	6

续表

		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
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
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

这个表的使用方法如下：48 位输入数据分成 8 组，每组 6 位，分别进入 8 个 S 盒，将每组的 6 位输入记为 $b_0b_1b_2b_3b_4b_5$，那么表中的行号由 b_0b_5 决定，而列号由 $b_1b_2b_3b_4$ 决定。例如，第一个分组 111 000 要进入第一个 S 盒 S_1，那么行号为 10（b_0b_5），即第 2 行，列号为 1100（$b_1b_2b_3b_4$），即第 12 列，第 2 行第 12 列对应的数据为 3，所以这个 S 盒的 4 位输出就是 3 的二进制表示 0011。

48 位输入数据根据 S 盒置换表置换成 32 位输出数据。

- 直接置换。S 盒置换后的 32 位输出数据将进行直接置换，该置换把每个输入位映射到输出位，任意一位不能被映射两次，也不能略去。表 3-7 为直接置换表，该表的使用方法与初始置换表相同。

表 3-7　直接置换表

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

- 经过直接置换的 32 位输出数据与本轮的 L 部分进行异或操作，结果作为下一轮子加密过程的 R 部分。本轮的 R 部分直接作为下一轮子加密过程的 L 部分。然后进入下一轮子加密过程，直到 16 轮全部完成。

（4）终结置换

终结置换与初始置换相对应，它们都不影响 DES 算法的安全性，主要目的是更容易地将明文和密文数据以字节大小放入 f 算法或者 DES 芯片中。表 3-8 为终结置换表，该表的使用方法与初始置换表相同。

表 3-8　终结置换表

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 算法按照终结置换表进行终结置换，64 位输出就是密文。

3. 子密钥的产生过程

明文和密文的位数是一致的。在每轮的子加密过程中，48 位的明文数据要与 48 位的子密钥进行异或运算。DES 算法子密钥的产生过程如图 3-16 所示。

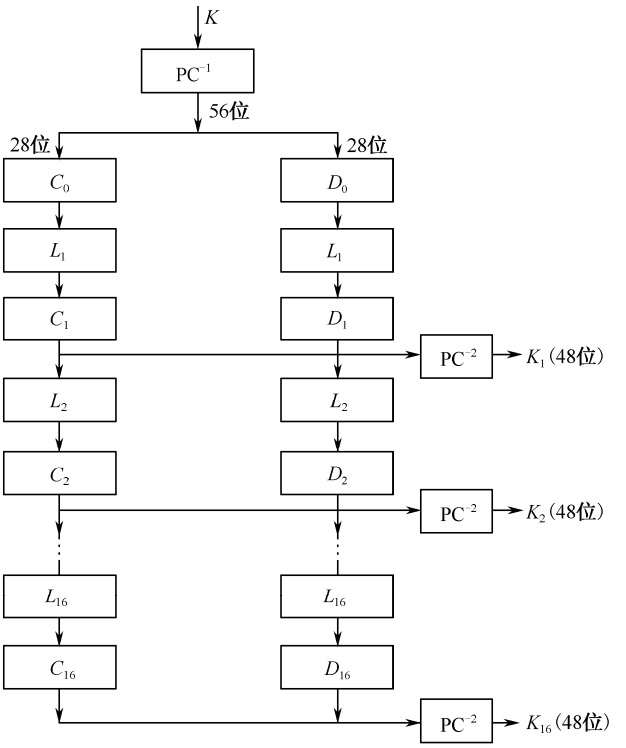


图 3-16　DES 算法子密钥的产生过程

（1）压缩型换位 1

64 位初始密钥就是使用者所持有的 64 位密钥 K，初始密钥根据压缩型换位 1 置换表（见表 3-9）进行置换，将初始密钥的 8 个奇偶检验位剔除，并且将留下的 56 位密钥顺序按位打乱。

表 3-9　压缩型换位 1 置换表

PC^{-1}	57	49	41	33	25	17	9
	1	58	50	42	34	26	18

续表

PC^{-1}	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

（2）分组

经过压缩型换位 1，64 位密钥被压缩为 56 位。将这 56 位密钥在中间分开，每部分 28 位，左半部分记为C_0，右半部分记为D_0，然后进入子密钥生成的 16 轮循环，每一轮循环将产生一个子密钥。

（3）16 轮循环

C_0和D_0分别循环左移L_1（见表 3-11，L_1=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根据压缩型换位 2 置换表（见表 3-10）进行置换，生成 48 位的子密钥K_1。

表 3-10　压缩型换位 2 置换表

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和D_1分别循环左移L_2（见表 3-11，L_2=1）位，再合并，经过压缩型换位 2，生成子密钥K_2。以此类推，直至生成子密钥K_{16}。注意，L_i（$i=1,2,\cdots,16$）的值是不同的，具体如表 3-11 所示。

表 3-11　L_i（i=1,2,…,16）的值

循环顺序（i）	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
左移位数（L_i）	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

4. DES 算法解密过程

DES 算法解密过程和 DES 算法加密过程完全类似，只不过将 16 轮循环的子密钥序列K_1，$K_2,\cdots,K_{16}$的顺序倒过来，即第一轮用第 16 个子密钥K_{16}，第二轮用K_{15}，以此类推。DES 算法解密过程的第一轮运算如图 3-17 所示。

5. DES 算法的安全性分析

破译 DES 算法的唯一可行途径是尝试所有可能的密钥（穷举法）。为了提高 DES 算法的安全性，加大密钥长度是一种简便的方法。表 3-12 说明了不同的密钥长度受到不同的攻击时，