数据安全与软件加密技术

郑雪雪 编著

人民邮电出版社

数据安全与软件加密技术
人民邮电出版社

计 算 机 技 术 丛 书

数据安全与软件加密技术

郑雪雪　编著

人 民 邮 电 出 版 社

图书在版编目（CIP）数据

数据安全与软件加密技术/郑雪雪编著．—北京：人民邮电出版社，1995.6
ISBN 7-115-05693-5

Ⅰ．数… Ⅱ．郑… Ⅲ．①数据管理-安全性约束②软件维护-加密-密码 Ⅳ．①TP311．13②TP311．5

内 容 提 要

本书主要介绍了以下内容：数据安全及其在微机上的实现方法；软件及磁盘信息的加密，DOS 系统中 DEBUG、中断及 TSR 在加、解密中的应用；计算机网络的安全保密。书末还附有常见病毒的种类及特征。

本书内容丰富，深入浅出，对于各种实用方法均给出了翔实的例子，适合于计算机软件开发人员及大专院校有关专业师生参考，也可作为有关专业本科教材。

计算机技术丛书
数据安全与软件加密技术
郑雪雪 编著
责任编辑 王亚明
*
人民邮电出版社出版发行
北京朝阳门内南竹杆胡同 111 号
北京顺义振华印刷厂印刷
新华书店总店科技发行所经销
*
开本：787×1092 1/16 1995 年 6 月 第一版
印张：12.75 1996 年 6 月 北京第 2 次印刷
字数：315 千字 印数：10 101-20 200 册
ISBN7-115-05693-5/TP・213
定价：18.00 元

丛 书 前 言

世界上发达国家普遍重视发展以计算机和通信为核心的信息技术、信息产业和信息技术的应用，一些经济发达国家信息产业发展迅速。

当前，我国处于国民经济高速发展时期。与此相伴随，必将有信息技术、信息产业和信息技术应用的高速发展。各行各业将面临信息技术应用研究与发展的大课题以及信息化技术改造的大任务、大工程。

为了适应信息技术应用大众化的趋势，提高应用水平，我们组织编写、出版了这套“计算机技术丛书”。这套丛书以实用化、系列化、大众化为特点，介绍实用计算机技术。

这套丛书采取开放式选题框架，即选题面向我国不断发展着的计算机技术应用的实际需要和国际上的实用新技术，选题不断增添又保持前后有序。

这套丛书中有的著作还拟配合出版软件版本，用软盘形式向读者提供著作中介绍的软件，以使读者方便地使用软件。

我们希望广大读者为这套丛书的出版多提意见和建议。

前　言

随着计算机科学技术的迅速发展与计算机在各个领域中的广泛应用，数据信息与软件的安全问题成了计算机科学中一个重要的研究课题。

在当今的信息社会中，有大量的数据信息需要传送和交换，因此，数据信息安全保护的重要性是不言而喻的。为了使计算机能更好地应用于各行各业，必然要开发和研制越来越多的软件产品。计算机软件是知识密集型的产品，它制作复杂，研制周期长，而软件的非法复制又十分容易，为了保护软件制作者的知识产权和经济利益，就应采取保护措施。作者在从事计算机的各项工作中也体会到数据安全与软件加密这两方面的重要性。根据密码学的发展与软件加密技术的不断完善，加上作者的经验与总结，在计算机学院为本科高年级同学开设了《数据安全与软件加密》这门课。在多年教学的基础上，结合本科生的毕业设计以及两次《数据安全与软件加密》的讲义，修改、整理而成本书。本书除了介绍一些具体方法外，还介绍了计算机系统较深层的内容及一些软件手段，希望通过本书能为读者自己设计新的加密方法打下良好的基础。

本书共分十章。

第一章从密码学的角度来讨论DES体制与公开密钥体制，介绍不同体制下数据加密的算法与加密思想。

第二章介绍一些能在微机上实现的加密方法。

第三章的重点是dBASE Ⅲ数据库文件的结构与库文件的安全保护。

第四章是有关磁盘信息的加密与特殊格式化的方法。

第五章叙述了COM文件与EXE文件的不同结构及文件加密的各种方法和技术。

第六章是关于版权信息的保护，方法中也包含了软件加密的新思路——指令自生成技术。

第七章是软件工具DEBUG的使用与扩充，第八章是中断（包括部分未公开的中断）与TSR的介绍，设置这两章的目的是使读者增加一些软件手段，能更好地用于加密方法的设计，推动加密技术的发展。

第九章介绍了激光加密的原理与反动态跟踪的各种措施，并介绍了一种反反动态跟踪的方法，目的是希望通过这两方面的介绍能促进这种技术的进一步发展。最后还介绍了目前独宠的加密技术——激光软加密。

第十章叙述了计算机网络通信中数据安全保密的原理，阐述了DES体制和RSA体制在网络加密中的作用。

由于水平有限及编写经验的不足，书中难免存在一些缺点和错误，望广大读者不吝赐教，批评指正。

郑雪雪

目　录

第一章 数据安全

随着计算机的广泛应用，高技术不断地相互渗透，人们越来越重视软件及数据的安全保护问题，促使计算机安全保密成为计算机科学中的一个重要的研究课题。

本章主要从密码学的角度来讨论数据安全的问题。

密码学由密码编制学和密码分析学两部分组成，可表示成下列公式：

密码学＝密码编制学＋密码分析学

密码编制学是研究、开发密码系统的方法，通过编码技术，改变需要保护的信息，使编码后的信息除了指定的接收者外，其它人不可理解。

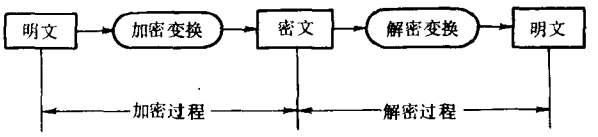

图 1.1 明文、密文与加密、解密的关系

密码分析学是研究攻破密码系统的途径，恢复被隐蔽信息的本来面目。一个密码系统被攻破，人们就会研究和发展新的密码系统，两者的互相促进，推动了密码学的发展。

密码学的发展分为古典密码术、近代密码学与现代密码体制三个阶段。它们的共同特点是：明文通过加密变换成为密文，而密文通过相应的解密变换还原成明文。它们之间的关系可用图 1.1 表示。

1.1 古典密码术

1.1.1 塞塔（sitar）式密码

公元前 400 年，斯巴达人把一长纸条螺旋形地斜绕在一个多棱棒上，将明文沿棒的水平方向从左到右书写，写完一行旋转一下，再从左到右写，直到写完。解下来后，纸条上的文就是密文。

为简单起见，以中文为例来作说明。

明文为“密码学的新方向是公开密钥体制”，按上法在一六棱棒上书写，其纸条上的密文是“密的向公密体码新是开钥制学方”。实际上这是一种最早的移位式或叫转置式的密码。这种密码解密很简单，因它有明显的规律性。

1.1.2 代替式

如舞蹈人形密码（见图 1.2）。

电影、小说里还有五线谱音符式密码，这些都是沿用了这种密码术而发展起来的。

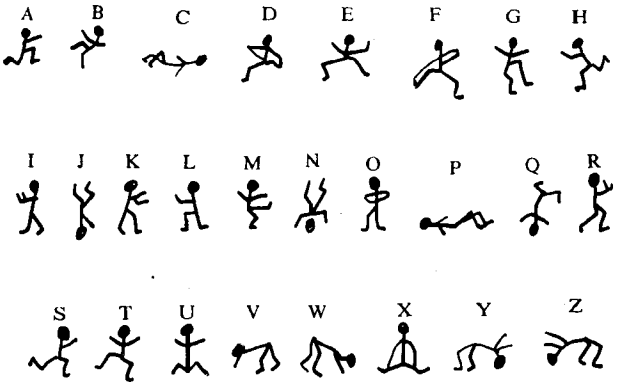

图 1.2　舞蹈人代替式密码

1.1.3　换字式密码

1. 单一换字式

有代表性的是凯撒（Caesar）密表，取定一个密钥（字母），26 个字母按自然序就有一个对应关系。

如取密钥为 D（D 对应于 a），其对应关系如下表：

表 1.1　　密钥为 D 的凯撒密表

明　文	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
密　文	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

若明文为 Computer，密钥为 D，则密文为 FRPSXWHU。

对这种单一换字式密码，可通过对下列三大特征的分析来进行破译：使用频率特征、连接特征和反复特征。

（1）使用频率特征

经过大量统计得出一些统计数字。我们把一万个字母中 26 个字母出现的次数记作 f_a，f_b，f_c，…f_y，f_z。统计结果见表 1.2：

表 1.2　　字母出现次数统计表

f_a	f_b	f_c	f_d	f_e	f_f	f_g	f_h	f_i	f_j	f_k	f_l	f_m
778	141	296	402	1277	197	174	595	667	51	74	372	288
f_n	f_o	f_p	f_q	f_r	f_s	f_t	f_u	f_v	f_w	f_x	f_y	f_z
686	807	223	8	651	622	855	303	112	172	27	153	6

用 P_a，P_b，…表示 a，b，…的使用频率，有 $P_a=\lim\limits_{N\to\infty}\dfrac{f_a}{N}$（$N$ 为总的字母数）

近似地取

$$P_a=\frac{f_a\pm\sqrt{f_a}}{N}$$

根据统计数字可作出频率曲线（图 1.3）。

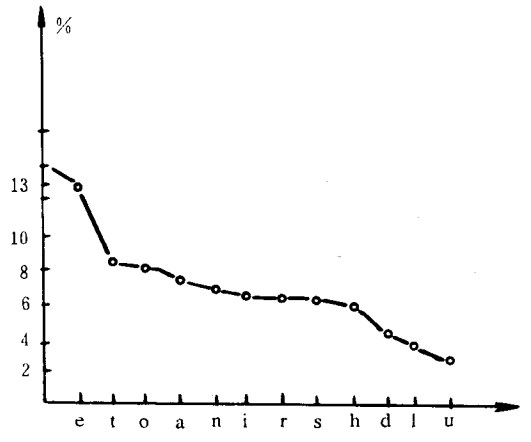

图 1.3　字母使用频率曲线

解密时可根据密文中某个字母出现的频率，从频率曲线来推测对应的明文字母。

（2）连接特征

连接是指某一字母（如 a）与另一字母（如 b）的前连接（ab）、后连接（ba）、间断连接（a$\overset{r\text{个}}{\times\times\times\times}$b）。根据观察统计，可得到概率值 P（a→b）、P（b→a）和 P（a$\xrightarrow{(r)}$b）。

当用“使用频率特征”分析尚不能推测出明文时，可根据密文的连接情况与统计概率值作比较来判定。

（3）反复特征

反复是指某一字母组合的重复。字母组合可分三连码、四连码、五连码等。如 CAT 为三连码。

通过对以上三种特性的分析，单一换字式密码的破译就比较容易。下面看一个简单的例子。

例 1.1　密文共 62 个字母：

WKHHOHFWURQLFFRPSXWHULVZLGH

OBXVHGLQVROYLQJPDWKHPDWLF

DOSUREOHPV

先用使用频率进行分析，知 H 出现 8 次，概率为 13%，W 出现 5 次，为 8%。由图 1.3，可假定 H 替代了 e，W 替代了 t。这正是密钥为 D 的凯撒密表的对应关系，故可根据凯撒密表来推测明文，明文为：

The electronic computer is widely used in solving mathematical problems.

（译文为：电子计算机被广泛地用于解决一些数学问题。）

由于单一换字式在定下密钥后，每个字母的对应关系是固定的，一般都可通过以上三种特性的分析来破译，因而，在此基础上又发展了一种“密钥字”，即用某一个字作为密钥，反复使用。

如以“duck”为密钥字，对明文 Computer 的密文为 FIOZXNGB。这种密码体制消除了单一换字式的缺点，但它有一定的规律（密钥字重复使用），对每一密钥又都是自然序。

2. 多表换字式

有代表性的是维吉尼亚（Vigenere）方阵（见表 1.3）。

先定下一个密钥，以 D 为例，即密钥从 D 开始，每个字母一变（顺序向下）。明文为 Computer，则 C 的密钥为 D，O 的密钥为 E，m 的密钥为 F…，以此类推。故当 D 对应 a 时，C 的密文为 F；E 对应 a 时，o 的密文为 s；F 对应 a 时，m 的密文为 R…，以此类推，Computer 的密文为 FSRVBBNB。不同的明文字母 u、t、r 对应同一密文字母 B。故对于多表换字式的

破译就要困难多了。

另外还有一种 Beaufort 方阵也是很著名的（见表 1.4）。

表 1.3　　Vigenere 方阵

	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	a
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	b
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	c
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	d
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	e
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	f
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	g
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	h
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	i
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	j
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	k
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	l
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	m
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	n
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	o
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	p
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	q
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	r
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	s
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	t
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	u
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	v
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	w
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	x
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	y
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	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	Z	

表 1.4 Beaufort 方阵

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

1.1.4 分置式密码

在第一次世界大战中，德国间谍使用过把文字分散在一个图案中的方法。如图 1.4 表示“YPRES 8TH”（译文：伊普尔 8 日），即隐含接头地点和时间。

图 1.4 绘画分置式密码

1.1.5 转置式密码

有逆序和方阵转置等方式。

(1) 逆序：分别取每一个词的逆序。

例 1.1 的明文可写成：

EHT CINORTCELE RETUPMOC SI YLEDIW DESU NI GNIVLOS LACITAMEHTAM SMELBORP

(2) 方阵转置：取方阵为 $N\times N$，以 $N=4$ 为例明文按行书写，以列的顺序取作密文。

明文→	1	2	3	4
密↓1	T	H	E	E
文 2	L	E	C	T
3	R	O	N	I
4	C	C	O	M

P	U	T	E
R	I	S	W
I	D	E	L
Y	U	S	E

D	I	N	S
O	L	V	I
N	G	M	A
T	H	E	M

A	T	I	C
A	L	P	R
O	B	L	E
M	S		

则密文为：

TLRCHEOCECNOETIMPRIYUIDUTSESEW

LEDONTILGHNVMESIAMAAOMTLBSIPLCRE

1.1.6 Playfair 加密算法

根据指定的密钥导出一个 5×5 方阵，如取密钥为 Data security，导出下列方阵：

$$\begin{bmatrix} D & A & T & S & E \\ C & U & R & I & Y \\ B & F & G & H & K \\ L & M & N & O & P \\ Q & V & W & X & Z \end{bmatrix}$$

这里只能安排 25 个字母，J 属罕见，故省略。

取密文的方法是先把明文分成两个字母一组，在这个方阵中找对应的密文，取密文时，按下列的规则：

(1) 若明文字母在同行，取其右边的字母为密文，第一列为第五列的右方（如 DA 的密文为 AT）；

(2) 若明文字母在同列，取其下方的字母为密文，第一行为第五行的下方（如 YP 的密文为 KZ）；

(3) 若明文字母不同行不同列，取其对角（同行）的字母为密文（如 EN 的密文为 TP）；

（4）若分组时有两个相同的字母分在一组，在字母中间加一个空字母（如Q）后再重新分组，直到所有组没有相重的字母；

（5）最后一组只有一个字母时，最后补Q。

例1.2 明文为Data Encryption Standard，先分为下列各组：

DA TA EN CR YP TI ON ST AN DA RD

其密文为：ATSTTPUIKZSRPOESTMATCT

1.2　近代密码学

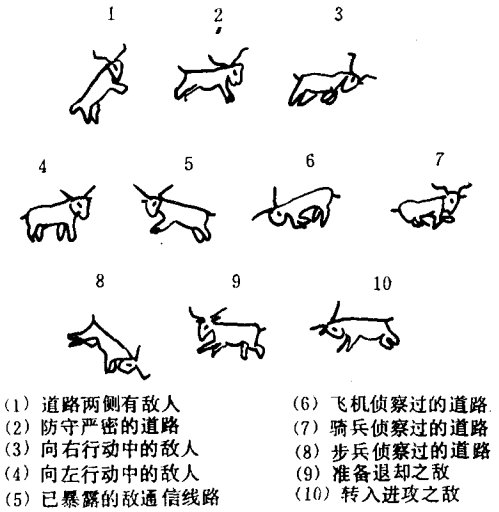

图1.5　山羊式密码

惠斯登(Wheastone)1867年发明了圆盘式密码机。在第一次世界大战期间，德军破译了俄军的密电，得知俄国第一军的给养已断。德军采取相应措施，取得了这一战役的胜利。当时，德军还使用山羊式密码来传递情报，即用十种不同的山羊姿态代表不同的敌情（见图1.5）。

1920年，美国电报公司提出弗纳姆（Vernam）密码，它用一个密钥码与五位的电报码进行模2加得出密文。

这里的“模2加”就是异或运算，即有1+1=0，0+0=0，0+1=1，1+0=1。模2加有一个特点：信息码与密钥码作模2加后得出的码再与同一密钥码作模2加，则还原为信息码，也即加密过程与解密过程一致。

如：（电报码）　信息码　00111

密钥码　11001　（模2加）

11110

密钥码　11001　（模2加）

信息码　00111

只要把明文与电报码建立对应关系，再取一个密钥序列，就可用此法形成密文。开始时使用的是一个定长的密钥序列，像密码字一样循环使用，这样产生的密文能形成有规律的反复，易被破译；后来采用的密钥与明文同长，且密钥序列只用一次，称为“一次一密体制”，其传送方式见图1.6。其安全性很强，Shannon曾证明过一次一密密码体制是不可破的。

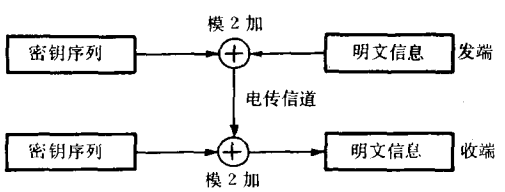

图1.6　“一次一密”的传送方式

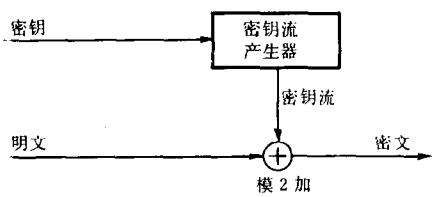

图1.7　序列密码体制的运行

虽然“一次一密”的效果很好，但密钥太长，既不好传送，又不好处理。后改用两个不同长度的密钥序列，其长度分别为 j 和 k（互素），同步作模 2 加操作，产生一个新的密钥序列，其长度为 $j\times k$。只要 j、k 取得适当的大，就能产生一次一密的效果，也解决了密钥序列不好传送、不好处理的问题。

以 $j=5$，$k=4$ 为例，密钥序列分别为 11001 和 1001，有：

$$\begin{array}{rl} & \underline{11001}\ \underline{11001}\ \underline{11001}\ \underline{11001} \\ \text{模 2 加} & \underline{1001}\ \underline{1001}\ \underline{1001}\ \underline{1001}\ \underline{1001} \\ \hline & 01010111111010100000 \end{array}$$

新的密钥序列的长为 $5\times 4=20$。

通常取 $j=775$，$k=776$，则最后的密钥序列长为 $j\times k=601400$。

1.3　现代密码体制

所谓密码体制就是用各种加密方法组合起来所形成的一种算法。它是以现代数学为基础，用电子计算机实现加密、解密运算的一种方法，是从古典密码术进化、演变来的，弗纳姆的加密方法是现代密码体制的萌芽。

密码体制分序列密码体制和分组密码体制两种。

序列密码体制是用伪随机序列作为密钥序列的加密体制。其运行如图 1.7 所示。

其中密钥流产生器实际上是一给定的算法，产生的密钥流是一个二元随机序列。若这种随机序列周期长的话，使密钥序列长度能与明文长度相等，则相当于做到了一次一密。

分组密码体制是把明文按 Bit 分组进行加密，解密时也按同样的分组进行。这里仅介绍几种分组加密体制。

1.3.1　代数加密体制

代数加密体制是 1929 年由美国纽约亨特大学的副教授希尔（Hill）提出的，是用代数编码方式来进行加密和解密的。基本思想是采用解方程式的方法把明文变为密文。先把明文按码分组，如果以 n 个码为一组，就用 n 个方程式。再建立一个字母与 0～25 的对应表，使字母与 0～25 之间的数值一一对应（这里不区分大小写）。

常用的有 Hill 表：

表 1.5　　**Hill 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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

也可取成乱序表，例如：

表 1.6　　**乱序表**

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
5	23	2	20	10	15	8	4	18	25	0	16	13	7	3	1	19	6	12	24	21	17	14	22	11	9

以四码代替为例，把明文按 4 个字母分成组，建立一个系数固定的方程组如下：

$Y_1=8X_1+6X_2+9X_3+5X_4$

$Y_2=6X_1+9X_2+5X_3+10X_4$

$Y_3=5X_1+8X_2+4X_3+9X_4$

$Y_4=10X_1+6X_2+11X_3+4X_4$

其系数矩阵为：

$$A=\begin{pmatrix} 8 & 6 & 9 & 5 \\ 6 & 9 & 5 & 10 \\ 5 & 8 & 4 & 9 \\ 10 & 6 & 11 & 4 \end{pmatrix}$$

通过一个对应表，如上面给出的乱序表，查出明文 4 个字母对应的数码 X_1、X_2、X_3、X_4，代入方程，取以 26 为模（即 mod26）的余数得到 Y_1、Y_2、Y_3、Y_4，再通过乱序表查出对应的字母，即为密文。

例 1.3 求明文 Delay operation 的密文。

先把明文分组，不足 4 个的用虚码补足，分成：Dela yope rati onac（ac 为虚码）。

对第一组，查乱序表有 $X_1=20$（D）、$X_2=10$（e）、$X_3=16$（l）、$X_4=5$（a），代入方程组得：

$Y_1=$（$8\times20+6\times10+9\times16+5\times5$）mod26$=25\rightarrow$J

$Y_2=$（$6\times20+9\times10+5\times16+10\times5$）mod26$=2\rightarrow$C

$Y_3=$（$5\times20+8\times10+4\times16+9\times5$）mod26$=3\rightarrow$O

$Y_4=$（$10\times20+6\times10+11\times16+4\times5$）mod26$=14\rightarrow$W

以此类推，可得密文 ZLVB DVLE VXAA。而解密的方程式为：

$X_1=23Y_1+20Y_2+5Y_3+1\cdot Y_4$

$X_2=2Y_1+11Y_2+18Y_3+1\cdot Y_4$

$X_3=2Y_1+20Y_2+6Y_3+25Y_4$

$X_4=25Y_1+2Y_2+22Y_3+25Y_4$

其系数矩阵为：

$$B=A^{-1}=\begin{pmatrix} 23 & 20 & 5 & 1 \\ 2 & 11 & 18 & 1 \\ 2 & 20 & 6 & 25 \\ 25 & 2 & 22 & 25 \end{pmatrix}$$

对上述 Y 值，通过此解密方程式，可解出对应的明文为：

Delayoperationac。

对于三码（即 $n=3$），其加密系数矩阵为：

$$A=\begin{pmatrix} 11 & 2 & 19 \\ 5 & 23 & 25 \\ 20 & 7 & 1 \end{pmatrix}$$

解密系数矩阵为：

$$A^{-1}=\begin{pmatrix} 6 & 21 & 11 \\ 21 & 25 & 16 \\ 19 & 3 & 7 \end{pmatrix}$$

如果能找到一个矩阵 A，有 $A \cdot A \equiv I \bmod 26$，（即 $A^{-1}=A$）则 A 既是加密矩阵又是解密矩阵，这样加密、解密过程就能统一了。

以 $n=2$ 为例，我们能找出很多矩阵 A 满足 $A \cdot A \equiv I \bmod 26$。如取

$$A=\begin{pmatrix} 12 & 3 \\ 13 & 14 \end{pmatrix}$$

$$A \cdot A=\begin{pmatrix} 12 & 3 \\ 13 & 14 \end{pmatrix}\begin{pmatrix} 12 & 3 \\ 13 & 14 \end{pmatrix}=\begin{pmatrix} 183 & 26\times 3 \\ 26\times 13 & 235 \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}_{\bmod 26}$$

1.3.2 密码反馈体制

这是单一换字式中采用“密钥字”的一种发展，把明文按密钥字的长度分组，第一组的密钥是密钥字，而第二组的密钥是第一组的密文，以此类推，直到明文结束。

明文 Computer 以 duck 为密钥字时的密文为 FIOZXNGB，采用反馈体制时密文为 FIOZZBSQ。

明文	comp	uter
密钥	duck	fioz
密文	FIOZ	ZBSQ

这样的密文不具有周期性，破译就更困难了。

1.3.3 DES 体制

DES（Data Encryption Standard）体制是本世纪 70 年代由 IBM 公司研究推出的，是美国国家标准局的数据加密标准。

DES 体制的算法全部公开，1975 年 3 月公开发表，1977 年 1 月 15 日公布定为加密标准，1977 年 7 月 15 日生效。其核心是乘积变换。

DES 作为乘积密码的典型代表在密码学发展历史上具有重要的地位。

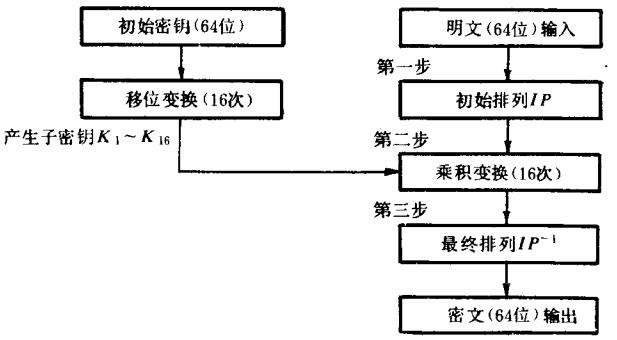

图 1.8 DES 体制的过程图

1. DES 体制的描述(算法介绍)

对明文按 64 位分组，每组明文经过初始排列（第一步）；通过子密钥 $k_1 \sim k_{16}$ 进行 16 次乘积变换（第二步）；再通过最终排列（第三步）得到 64 位密文，其过程见图 1.8。

16 次乘积变换的目的是使明文增大其混乱性和扩散性，使得输出不残存统计规律，使破译者不能从反向推算出密钥。