微型计算机实用大

第12篇 计算机安全与保密

12.1 密码学

12.1.1 一些基本概念

密码学 研究将可懂文本(明文)变换成不可懂形式(密文),以及通过其逆变换将不可懂形式变成原来的可懂文本的方法和过程的学科称为密码学。它的研究范围包括密码编码学和密码分析学。

密码编码学 研究如何编制出好的密码系统的方法;保护信息不被敌方侦察、窃取和盗用。

密码分析学 研究攻破一个密码系统的途径,恢复被隐蔽起来的信息的本来面目。

加密和解密 从可懂文本变成不可懂文本的变换称为加密。从不可懂文本变成原来可懂文本的变换称为解密。

被动攻击 敌手不经许可靠窃听而截取数据。可分为:

搭线窃听:利用导线联接,对通信线路或计算机网络上传送的数据进行截收。

电磁窃听:对无线电传输信息进行截收。如,对无线电和微波传输,或对从电子设备(计算机设备)辐射出的带有电磁能的辐射电磁波进行截收。

声音窃听:对由人的语言,或者由打印、穿孔和发送设备产生的声音进行截收。

主动攻击 敌手对在传送过程中,或对存储的信息进行非法删除、更改或插入等操作,这种攻击叫主动攻击。

密码体制 将完成加密和解密的算法称为密码体制。一般分传统密码体制和公开密钥密码体制。传统密码体制又分为,换位加密法、代替加密法和代数加密法。

密　　钥 为了使加密手段有效,应该尽一切可能将所使用的加密与解密算法中的全部细节保密。但实际上这是不可能的。因为一种算法经过长期、多次使用,难免不泄露出去。为了安全就要经常改变加密算法。可经常改变算法是有困难的。实际上,经常使用的算法不变,或者干脆公开,甚至将它作为一种标准加以颁布。但这种算法的进行过程应该能用一串适当长的字符串或数字串加以控制。该字符串或数字串就称为密钥。

12.1.2 传统密码学

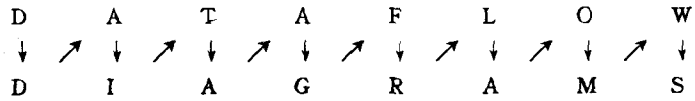
换位加密法 将明文字母按一定的算法改变其顺序,重新排列成为密文。此法很少单独使用,因为它们比较容易被破译。这是因为明文中的字母和密文中的字母没变,只是改变了它们的顺序,有可能找出算法破译它。它分为栅栏式加密法、路线加密法和钥控序列加密法。

栅栏式加密法 美国内战时期的简单加密法。把明文的前一半写成一行,后一半直接写在它的下面,然后按

列的顺序重新组合，就形成密文。例：

明文：DATA FLOW DIAGRAMS

变换：



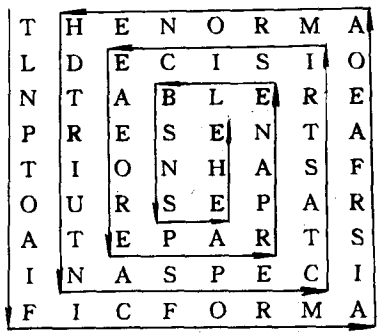
密文：DDAI TAAG FRLA OMWS

这种变换可以是多种多样的，只要是通信双方事先约定好即可。

路线加密法 路线加密法是把明文的字母按规定的顺序安排在一个矩阵中，然后用另一种顺序选出矩阵中的字母，排列起来就成为密文。这种排列的方法和选出的顺序是通信双方事先约定好的。例：

明文：The normal decision table representation has four separate parts in a specific format.

变换矩阵：



密文：

T	L	N	P	T	O	A	I	F		I	C	F	O	R	M	A	I	S
R	F	A	E	O	A	M	R	O		N	E	H	D	T	R	I	U	T
N	A	S	P	E	C	T	A	S		T	R	I	S	I	C	E	A	E
O	R	E	P	A	R	P	A	N		E	L	B	S	N	S	E	H	E

这种路线很多，矩阵的大小也可以变化，这些只要通信双方约定好即可。这种方法增加了保密强度。

如在矩阵中有空格，可用双方事先约定好的干扰字填满矩阵。如明文太长可填入多个矩阵，也可以填入多个不同大小的矩阵，每个矩阵的路线也可不同。如，该例中的最后一个字母T，就要填入下一个矩阵中。

钥控序列加密法 选一字符串或一单词作为密钥，每一字母赋以一个顺序号，然后再将密文按一定规则排列起来成为一个矩阵，将密钥排在第一行。按密钥中字母顺序依次将每列读出，写成序列即成密文。例：

明文：仍用上例之明文。

密钥：选为COMPUTER，其各字母顺序为：

C	O	M	P	U	T	E	R
1	4	3	5	8	7	2	6

变换矩阵：

C	O	M	P	U	T	E	R
1	4	3	5	8	7	2	6
T	H	E	N	O	R	M	A
L	D	E	C	I	S	I	O
N	T	A	B	L	E	R	E
P	R	E	S	E	N	T	A
T	I	O	N	H	A	S	F
O	U	R	S	E	P	A	R
A	T	E	P	A	R	T	S
I	N	A	S	P	E	C	I
F	I	C	F	O	R	M	A

密文：

T	L	N	P	T	O	A	I	F		M	I	R	T	S	A	T	C	M
E	E	A	E	O	R	E	A	C		H	D	T	R	I	U	T	N	I
N	C	B	S	N	S	P	S	F		A	O	E	A	F	R	S	I	A
R	S	E	N	A	P	R	E	R		O	I	L	E	H	E	A	P	O

代替加密法 代替加密法是用另一个字母表来代替明文中的字母，代替后的各字母均保持原来的位置。例：

明文：This example illustrates how a decision table can be used to define a program。

变换：

明文字母表 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

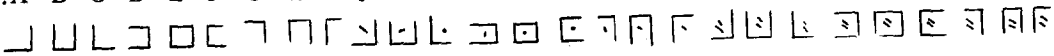
密文字母表 G H I J K L M N O P Q R S T U V W X Y Z A B C D E F

密文：Znoy kdgsurk orrayzxgzky nuc gjkioyout zghrk igt hk aykj zu jklothg vxumxgs。

可分为单表代替、多表代替、同音代替和多字母组代替密码。

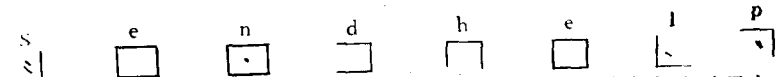
兽栏密码 它的变种很多，有一种方法是先画一个棋盘，将一个平面分成九个部份，每个部分代替一个字母，将字母A到I按从左到右，从上到下的顺序将字母填入棋盘格中。再用类似的方法将字母J至R填入每格加入一点的棋盘格中。再将字母S至Z填入加入两点的棋盘格中。这样就可得到新的代替字母表(密文字母表)。

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：

例：明文：



密文：

单表代替 单表代替密码是明文中的每个字母，用密文字母表中的对应字母代替，在全部加密过程中，是从明文字母表到密文字母表的一一映射。有个著名的单表代替称为凯撒(Caesar)代替密码(见凯撒代替密码。)

一般的单表代替密码算法可写成：

$$\Phi \equiv (a\theta + b) \bmod n$$

其中，Φ——密文字母在明文字母表中的位置序号(由0开始)；

θ——明文字母在明文字母表中的位置序号(由0开始)；

a——与n为两个互素的正整数。

多表代替密码 大多数多表代替密码是周期代替密码。当周期为1时，就是单表代替密码。即密钥周期反复

使用。多表代替密码种类很多，下面举Vigenere密码和游动钥密码为例来说明。

Vigenere密码 该密码中有一个有限序列$K=(K_1,K_2,\cdots,K_d)$为用户密钥，可以多次使用用户密钥而得到工作密钥，因此工作密钥为无限序列。

例如：明文为System，密钥为dog，加密过程如下：

明　　文：S ys tem

工作密钥：d og dog

密　　文：V mg wrs

在这个例子中，每三个字母中的第一、第二和第三个字母分别移动(mod26)3个、14个和6个位置。

表12.1-1 Vigenere表

密文 / 明文 / 密钥	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	D F G H I J K L M N I 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 K 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

表12.1-1所示的Vigenere表可作为加密和解密的工具。如明文字母为S，密钥为D，则查表得，S列和D行相交处的字母为V，即为密文字母。同样，解密时先查密钥字母所在行，在该行中找出密文字母。再查该密文字母所在列的明文字母。

凯撒(Julius Caesar)代替密码 公元前约50年，罗马皇帝朱利叶·凯撒发明了一种用于战时秘密通信的方

法，后来被称之为凯撒代替密码，简称为凯撒密码。他将字母按其原来顺序排列，最后一个字母与第一个字母相连。将明文中的每个字母用其后的第三个字母代替，就变成了密文。例：

明文：C o m p u t e r

密文：F r p s x w h u

凯撒密码可用公式表示为：

$$\Phi \equiv \theta + 3 (\mathrm{mod}\ 26)$$

上式中的3为凯撒密码的密钥。不知为什么当时凯撒把密钥选成3，实际上在1－25之间的任何一个数字均可作为密钥。用K表示密钥的集合，即$K=\{1, 2, 3, \cdots, 24, 25\}$。$K$也称之为密钥空间。取密钥为k，显然$k \in K$。

一个密码系统包括明文字母空间、密文字母空间、密钥空间和算法。密码系统的两个基本单元是算法和密钥。算法是一些公式、法则或程序，规定明文和密文之间的变换，密钥可以看做是算法中的参数。

游动密钥密码 游动密钥密码是一种非周期性的Vigenere密码，它的密钥和明文信息一样长，没有周期性重复。

例如，给明文The object of…加密，游动密钥可以取某一本书作为游动密钥文本。本例取美国1776年7月4日发布的独立宣言为密钥文本，从第一段开始。

明文：T h e o b j e c t o f …

密钥：W h e n i n t h e c o …

密文：P o i b j w x j x q t …

同音代替密码 一个明文字母表中的字母a，可以变换成若干个密文字母f(a)，f(a)称为同音字母。这种代替称为同音代替密码。

例：假定同音代替密码的密钥如表12.1-2所示的短文，单词的编号写在左边。每个词的首字母都和一个数字相对应。加密时可以用与字母对应的任何一个数字代替该字母。

表12.1-2 作为同音代替密码的密钥短文

(1) The techniques described above for
(6) breaking the Caesar cipher can
(11) also be used on other
(16) monoalphabetic ciphers. Short words, words
(21) with repeated patterns, and common
(26) initial and final letters all
(31) give clues for guessing the
(36) permutation. In English, some letters
(41) are used more frequently than
(46) others.

如果给明文Computer加密，则其过程如下：

例如字母C与数字8,9,10,17,25,32相对应。o,m,p,u,e,r也一样可以找到与之对应的数字。故Computer可用数字

8 14 16 23 42 2 38 22

来代替。当然也可以用其它数字来代替。所以同音代替的密文并不是唯一的。

多字母组代替密码 多字母代替密码每次加密一组(2个以上)字母。Playfair密码就是2字母组代替密码。

Playfair密码 Playfair密码是英国曾在第一次世界大战期间使用过的一种二字母组代替密码。Playfair密码密钥由25个英文字母(J与I相同)组成的五阶方阵。如图12.1-1所示。

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

图12.1-1 Playfair密码的密钥方阵

每一对明文字母m_1和m_2，都根据下面的6条规则进行加密。

(1)若m_1和m_2在密钥方阵中的同一行，则密文字母c_1和c_2分别是m_1和m_2右边的字母(第一列视为在第五列的右边)；

(2)若m_1和m_2在同一列，则c_1和c_2分别是m_1和m_2下边的字母(第一行视为在第五行的下边)；

(3)若m_1和m_2位于不同的行和列，则c_1和c_2是以m_1和m_2为顶点组成的长方形中的另两个顶点。其中c_1和m_1，c_2和m_2分别在同一行；

(4)若$m_1=m_2$，则在m_1和m_2之间插进一个无效字母。例如可取为X；

(5)若明文信息共有奇数个字母，则在明文末尾加上一个无效字母；

(6)字母I和J看成是一个字母。

例：明文为Computer，用Playfair法加密。

明文 CO MP UT ER

密文 OD TH MU GH

代数加密法 代数加密法首先规定用于明文字母的二进制数字序列或等效数字序列。在用查表法完成从字母到数字的变换以后，再用代数运算方法完成加密和解密。

下面介绍Vernam法、方程法和矩阵法。

Vernam加密法 Vernam加密法是为电传机编码发明的。它使用模2运算。

例：

明文	0	1	0	0	0	1
密钥	1	1	0	1	1	1
密文	1	0	0	1	1	0

如用M代表明文、C代表密文、K代表密钥，则加密过程可写成：

$$C=M\oplus K$$

解密过程为

$$M=C\oplus K$$

例：明文为define，密钥为System，用Vernam法加密如下：

二进制明文：010100,010101,010110,011001,100101,010101

二进制密钥：110010,111000,110010,110011,010101,100100

二进制密文：100110,101101,100100,101010,110000,110001

字母形式密文：O) M $ /

Vernam加密，解密，需要一张如表12.1-3所示的代码表。

表 12.1-3 字符的二进制编码

字 母	八进制码	二 进 制 码	字 母	八进制码	二进制码
0	00	000000	X	40	100000
1	01	000001	J	41	100001
2	02	000010	K	42	100010
3	03	000011	L	43	100011
4	04	000100	M	44	100100
5	05	000101	N	45	100101
6	06	000110	O	46	100110
7	07	000111	P	47	100111
8	10	001000	Q	50	101000
9	11	001001	R	51	101001
#	12	001010	$	52	101010
@	13	001011	*	53	101011
?	14	001100	—	54	101100
:	15	001101	)	55	101101
>	16	001110	;	56	101110
⩾	17	001111	⩽	57	101111
+	20	010000	Blank	60	110000
A	21	010001	/	61	110001
B	22	010010	S	62	110010
C	23	010011	T	63	110011
D	24	010100	U	64	110100
E	25	010101	V	65	110101
F	26	010110	W	66	110110
G	27	010111	X	67	110111
H	30	011000	Y	70	111000
I	31	011001	Z	71	111001
.	32	011010	,	72	111010
[	33	011011	%	73	111011
&	34	011100	≠	74	111100
(	35	011101	=	75	111101
<	36	011110	]	76	111110
←	37	011111	"	77	111111

方程加密法(Hill 法,四元代替法) 以联立方程为基础的加密法是Hill 发明的。用x 代表明文字母,y 代表密文字母。其数字根据下列任意建立的字母表来定。

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

规定加密序列以四个明文字母为一组,所以加密算法可用四元方程组表示。因此此法又称四元代替法,加密时用下列加密方程:

$$Y_1=8X_1+6X_2+9X_3+5X_4 \mod 26$$

$$Y_2=6X_1+9X_2+5X_3+10X_4 \mod 26$$

$$Y_3=5X_1+8X_2+4X_3+9X_4 \mod 26$$

$$Y_4=10X_1+6X_2+11X_3+4X_4 \mod 26$$

根据加密方程,给出解密方程如下:

$$X_1=23Y_1+20Y_2+5Y_3+1Y_4 \mod 26$$
$$X_2=2Y_1+11Y_2+18Y_3+1Y_4 \mod 26$$
$$X_3=2Y_1+20Y_2+6Y_3+25Y_4 \mod 26$$
$$X_4=25Y_1+2Y_2+22Y_3+25Y_4 \mod 26$$

例:给明文HELP 加密。

首先将明文变换成一组数

H $X_1=5$

E $X_2=9$

L $X_3=22$

P $X_4=21$

用加密算法对方程组加密:

$$Y_1=8X_1+6X_2+9X_3+5X_4 \mod 26$$
$$=8\times5+6\times9+9\times22+5\times21 \mod 26$$
$$=7$$
$$Y_2=6X_1+9X_2+5X_3+10X_4 \mod 26$$
$$=6\times5+9\times9+5\times22+10\times21 \mod 26$$
$$=15$$
$$Y_3=5X_1+8X_2+4X_3+9X_4 \mod 26$$
$$=5\times5+8\times9+4\times22+9\times21 \mod 26$$
$$=10$$
$$Y_4=10X_1+6X_2+11X_3+4X_4 \mod 26$$
$$=10\times5+6\times9+11\times22+4\times21 \mod 26$$
$$=14$$

译成字母,密文为UQZY。解密时用解密方程组计算即可。

矩阵加密法 矩阵加密法可以用下面的矩阵算法求密文,同样也可以用公式来解密。

加密矩阵算法:

$$Y_1=\left\{\begin{bmatrix}3&6&2\\16&23&8\\2&16&13\end{bmatrix}X_1(\mathrm{mod}26)+\begin{bmatrix}2&6&14\\8&24&4\\14&16&20\end{bmatrix}X_2(\mathrm{mod}26)+\begin{bmatrix}18&6&6\\24&20&22\\2&2&16\end{bmatrix}\right\}(\mathrm{mod}26)$$

$$Y_2=\left\{\begin{bmatrix}18&14&22\\20&4&10\\22&20&24\end{bmatrix}X_1(\mathrm{mod}26)+\begin{bmatrix}15&16&20\\4&13&2\\20&8&11\end{bmatrix}X_2(\mathrm{mod}26)+\begin{bmatrix}2&16&14\\8&12&4\\18&8&20\end{bmatrix}\right\}(\mathrm{mod}26)$$

将明文AIR SEA ATTACK AT DAWN 加密。

$$X_1=\begin{bmatrix}A&I&R\\S&E&A\\A&T&T\end{bmatrix}=\begin{bmatrix}4&17&23\\19&9&4\\4&12&12\end{bmatrix}$$

$$X_2=\begin{bmatrix}A&C&K\\A&T&D\\A&W&N\end{bmatrix}=\begin{bmatrix}4&25&0\\4&12&2\\4&18&24\end{bmatrix}$$

上面的字母变成数字的过程和方程加密法一样。

$$Y_1=\left\{\begin{bmatrix}3&6&2\\16&23&8\\2&16&13\end{bmatrix}\begin{bmatrix}4&17&23\\19&9&4\\4&12&12\end{bmatrix}(\text{mod}26)+\begin{bmatrix}2&6&14\\8&24&4\\14&16&20\end{bmatrix}\begin{bmatrix}4&25&0\\4&12&2\\4&18&24\end{bmatrix}(\text{mod}26)\right.$$
$$\left.+\begin{bmatrix}18&6&6\\24&20&22\\2&2&16\end{bmatrix}\right\}(\text{mod}26)=\begin{bmatrix}6&15&3\\25&11&20\\20&16&14\end{bmatrix}=\begin{bmatrix}O&Q&J\\C&V&F\\F&G&Y\end{bmatrix}$$

$$Y_2=\left\{\begin{bmatrix}18&14&22\\20&4&10\\22&20&24\end{bmatrix}\begin{bmatrix}4&17&23\\9&9&4\\4&12&12\end{bmatrix}(\text{mod}26)+\begin{bmatrix}15&16&20\\4&13&2\\20&8&11\end{bmatrix}\begin{bmatrix}4&25&0\\4&12&2\\4&18&24\end{bmatrix}(\text{mod}26)\right.$$
$$\left.+\begin{bmatrix}2&16&14\\8&12&4\\18&8&20\end{bmatrix}\right\}(\text{mod}\ 26)=\begin{bmatrix}8&1&12\\20&20&24\\10&6&4\end{bmatrix}=\begin{bmatrix}B&X&T\\F&F&N\\Z&O&A\end{bmatrix}$$

密文为:OQJC VFFG YBXT FFNZ OA

密码体制评价 可用以下五个方面来评价和比较不同的密码体制:

(1)保密强度:所需要的安全程度与数据的重要性有关。保密强度大的系统,开销往往较大。

(2)密钥的长度:密钥太短,就会降低保密强度。然而,密钥太长又不便于传送、保管和记忆。密钥必须经常更换,每次更换新密钥时,通信双方传送新密钥的通道必须保密和绝对安全。

(3)算法的复杂性:以人工方式加密与解密时,过程不能太复杂,否则容易出错。使用计算机或专用线路,复杂性也要有一定限制,否则开销过大。

(4)差错的播散性:不希望由于一点差错而使整个通信失败,特别是在实时性强的应用情况下更是这样。

(5)加密后信息长度的增加程度:有的加密方法使信息长度增加。如故意加入一些无含义的字符,企图改变语言的统计规律,以迷惑敌方。信息长度的增加将导致通信效率的降低。

12.1.3 数据加密标准算法(DES 算法)

乘积密码 乘积密码包括代替和移位两个步骤。如图12.1-2 所示为ADFGVX 乘积密码,它是在第二次世界大战中德军所使用的密码。

这种密码是由标有A,D,F,G,V,X 六个字母的行和列的方格构成的,图中随机填写A 至Z 这26 个字母和0 至9 十个数字。

加密时,第一步,将每个明文字母用它所在位置的纵横座标字母代替。第二步,将中间结果逐行地填写在一个矩形方格内,再按密钥字DEUTSCH 的各字母在字母表中的顺序逐列地取出。

解密时,先将密文按照同样的密钥字(DEUTSCH)的顺序逐列地填入方格内,然后逐行地取出,并将这个中间报文的各对字母作为纵横坐标,在标有ADFGVX 的方格中查找出对应的明文字母,从而得到明文。

第二次世界大战期间的密码研究实践表明,利用代替和移位交替变换所形成的乘积密码,可以获得保密强度很强的加密算法。DES 算法就是基于这个思想实现的。

	A	D	F	G	V	X
A	K	Z	W	R	1	F
D	9	B	6	C	L	5
F	Q	7	J	P	G	X
G	E	V	Y	3	A	N
V	8	O	D	H	0	2
X	U	4	I	S	T	M

明文：
P R O D U C T
C I P H E R S
中间报文(代替)
FG AG VD VF XA DG XV
DG XF FG VG GA AG XG

D E U T S C H
2 3 7 6 5 1 4

密钥
各密钥字母排列次序

F	G	A	G	V	D	V
F	X	A	D	G	X	V
D	G	X	F	F	G	V
G	G	A	A	G	X	G

密文：
DXGX FFDG GXGG VVVG
VGFG GDFA AAXA

图12.1-2 乘积密码例

DES算法简述 1968年至1975年间研究高保密强度的乘积密码时，由Feiste设计的分组乘积密码用LUCIFER密码系统实现了。不久，由W.L.Tuchman博士领导的小组，在LUCIFER密码的基础上研究出一种新的密码算法。这种算法是在密钥的控制下进行16圈代替和固定置换变换所组成。由美国国家标准局批准定为联邦数据加密标准，于1977年7月15日生效。

DES算法是在56比特密钥的控制下，将64比特明文数据块变成64比特的密文数据块。加密过程要进行16次迭代。每次都采用乘积码加密方式，称为密码函数。提供的密钥为64比特，其中有8位为奇偶校验位。从56比特密钥中，选出含48比特的不同子集供不同的圈使用。它们分别记为K(1)，K(2)，…，K(16)。解密时，将密钥序号颠倒过来使用，即第1圈用K(16)，第二圈用K(15)，以下类推。

可以将DES算法看成是一个有64比特输入和输出的，由密钥控制的代替盒，称为S盒。若使用64比特的代替盒，可使明文到密文的变换总数达到2的64次方种可能。在DES算法中，采用了6比特输入，4比特输出的较小的代替盒S_1，S_2，…，S_8。

经过多次返复的代替和置换使密码强度得以增强。

加密用E表示，解密用D表示。

加密算法：$E_k(x)=y$，表示明文x在密钥k的作用下，经过加密变换，得到密文y。

解密算法：$D_k(y)=x$，表示密文y在密钥k的作用下，经过解密变换，得到明文x。

由上述两式可以看出，加密和解密时用同一个密钥，因此*DES*密码体制又称之为对称密钥体制。

在*DES*算法中明文、密文和密钥之间存在着互补关系，可用方程表示如下。

$$E_k(x)=E_k(\bar{x})$$

DES为分组乘积密码，其密钥总长度为64比特，其中包括8比特奇偶校验位，它可以将64比特明文变换成64比特密文，当然也可以将密文变成明文。

数据加密标准算法的加密步骤如图12.1-3所示。

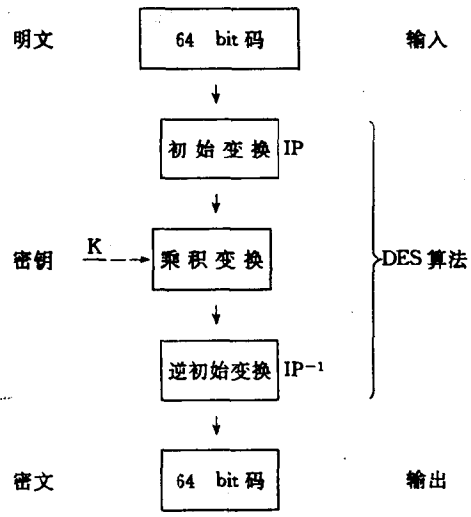


图12.1-3 DES加密过程框图

(1)初始变换.这是一种移位操作,用IP表示.移位时不用密钥,仅对64比特明文进行变换.它可以用置换群定义如下:

$$IP=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & \cdots & 61 & 62 & 63 & 64\\ 58 & 50 & 42 & 34 & 26 & \cdots & 31 & 23 & 15 & 7\end{pmatrix}$$

为了方便,用表12.1-4表示.

表12.1-4 初始变换IP表

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

(2)乘积变换.是一种复杂的与密钥有关的代替和移位变换.它采用分组的方式来增加代替和移位变换的可能状态.

(3)逆初始变换.也是一种移位操作,用IP^{-1}表示.它和IP互逆.可用如下置换群定义:

$$IP^{-1}=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & \cdots & 61 & 62 & 63 & 64\\ 40 & 8 & 48 & 16 & 56 & \cdots & 49 & 17 & 57 & 25\end{pmatrix}$$

可用表12.1-5表示.

在乘积变换步骤中,代替是在密钥控制下进行的,而移位是按固定顺序进行的.代替是由明(密)文、密钥及其圈数和S盒决定的.

表12.1-5 逆初始变换IP^{-1}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

初始变换 见DES算法简述。

逆初始变换 见DES算法简述。

乘积变换 见DES算法简述。

选择运算E 输入32比特数据产生48位输出。可用表12.1-6表示。

表12.1-6 选择运算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

由表12.1-6可以看出，第1，2列和第5，6列分别是一样的。即第1，4，5，8，9，12，13，16，17，20，21，24，25，28，29各位的数字复用一次。因而输入32位数，可产生48位的输出。

S盒 S盒由S_1，S_2，S_3，S_4，S_5，S_6，S_7，$S_8$8个盒组成。每个盒S_i有6位输入，4位输出(都是二进制位，即比特)。八个S盒的输出组成32位输出。表12.1-7给出了选择函数S_1到S_8的矩阵。

S_1到S_8选择函数组输入是一个48位码组，用B_1 B_2 B_3 B_4 B_5 B_6 B_7 B_8表示。每个B_i(i=1，2，…，8)包含6位。S_1用于B_1，S_2用于B_2，以下类推。若S为一选择函数，B_i是自变量，则选择函数的输出记为$S_i(B_i)$。$S_i(B_i)$计算过程如下：

(1)B_i的第一位和最后一位代表0～3的二进制数，记作m，行数。

(2)B_i的中间4位代表从0～15的二进制数，记作n，列数。

(3)采用从零开始标号的S_i矩阵，把位于矩阵第m行第n列的数作为一个四位二进制数码组。

(4)第(3)步的结果是选择函数S_i的输出。

整个选择函数组的输出是由$S_1(B_1)$ $S_2(B_2)$ $S_3(B_3)$ $S_4(B_4)$ $S_5(B_5)$ $S_6(B_6)$ $S_7(B_7)$ $S_8(B_8)$组成的二进制串。

表 12.1-7 选择函数S_1到S_8的矩阵

S_1

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

S_2

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

S_3

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

S_4

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

S_5

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

S_6

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

S_7

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

S_8

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

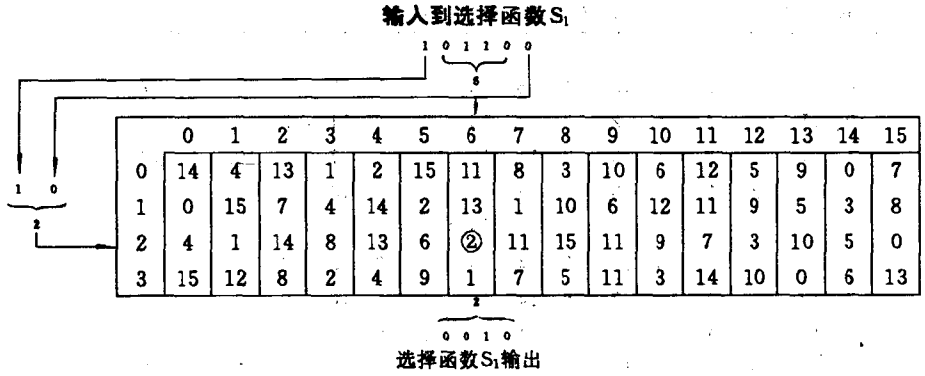


图12.1-5 使用选择函数S_1的例子

图12.1-5为选择函数S_1应用实例。输给选择函数S_1的是二进制数101100。输入的第一位和最后一位分别是1和0，即为2。表示第2行。输入的中间4位是0110，它是6，表示第6列。位于S1矩阵第2行第6列处的数是2，即二进制的0010，这就是在输入条件下选择函数S1的选择输出。

由此可看出选择函数实现了代替法加密。

换位表P 换位表P如表12.1-8所示。它可以用一置换群P表示为：

表12.1-8 换位表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	24

$$P=\begin{pmatrix}1 & 2 & 3 & \cdots & 30 & 31 & 32\\ 16 & 7 & 20 & \cdots & 11 & 4 & 24\end{pmatrix}$$

子密钥换位表PC－1(置换选择1) 在求子密钥时将输入的64位密钥去掉奇偶校验位，经过PC－1换位后分为两个28位码组，记为C_0和D_0，这是计算子密钥的起点。表12.1-9为子密钥换位表PC－1。

表12.1-9 子密钥换位表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

PC－1可以用变换群定义为：

$$(PC-1)=\begin{pmatrix}1 & 2 & 3 & \cdots & 54 & 55 & 56\\ 57 & 49 & 41 & \cdots & 20 & 12 & 4\end{pmatrix}$$

图12.1-6所示，为PC－1在计算密钥时的应用情况。

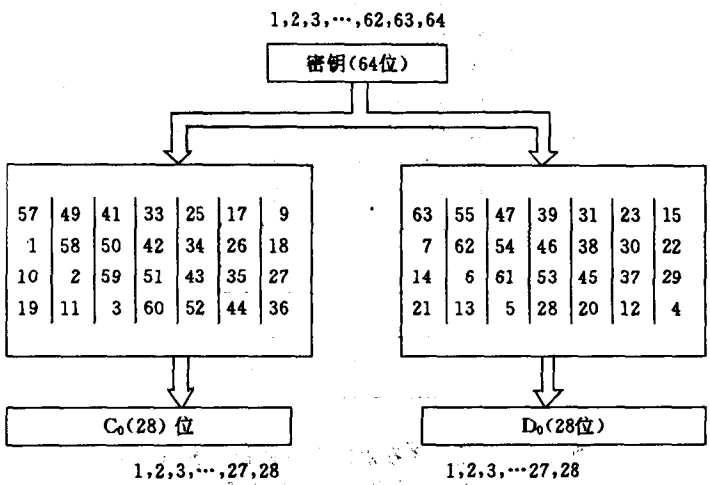


图12.1-6 用于计算C_0和D_0的子密钥换位表PC－1的工作情况

子密钥换位表PC－2(置换选择2) 用于从C_i和D_i的一串码中选出特定位的码作为密钥K_i。C_i和D_i的位数和为56位，被选定的K_i为48位。表12.1-10表示了这个选择及其选后的排列顺序。将C_iD_i串中的第9,18,22,25,35,38,43,54位去掉。

图12.1-7表示了这一变换的过程。

表12.1-10 子密钥变换表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

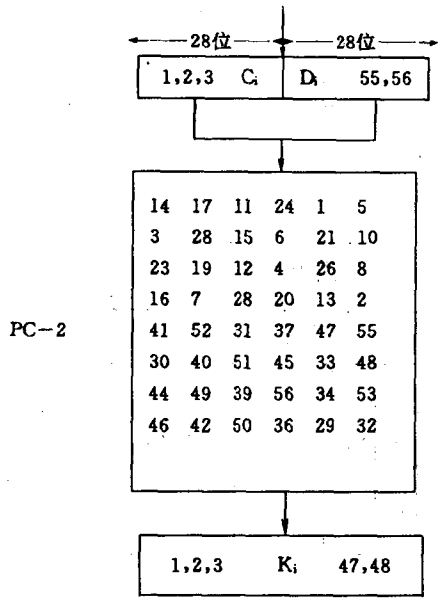


图12.1-7 用于子密钥Ki计算的换位表PC—2

循环移位数表 C_i和D_i的产生是由C_{i-1}和D_{i-1}移位而得到的。其具体规定如表12.1-11所示。

表12.1-11 循环移位数表

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$C_{i-1}D_{i-1}$到C_iD_i之间经历的移位位数	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

DES算法 DES算法包括以下几个部分：

(1)计算密钥，这是产生16个子密钥的过程。

(2)模2加法运算。

(3)加密函数，包括乘积变换中的主要运算。

(4)码组移位产生一"输出前的码组"，作为逆初始置换的输入。

(5)初始置换，它是一个选择表IP。