PCT

世界知识产权组织
国际局

按照专利合作条约(PCT)所公布的国际申请

(51) 国际专利分类号[6]:
H04L 9/00

A1

(11) 国际公布号: WO97/12459

(43) 国际公布日: 1997年4月3日(03.04.97)

(21) 国际申请号: PCT/CN95/00077

(22) 国际申请日: 1995年9月26日(26.09.95)

(71) (72) 申请人及发明人: 林仙坎(LIN, Xiankan) [CN/CN]; 中国福建省福州市华林路203号, 邮政编码:350003, Fujian (CN)。

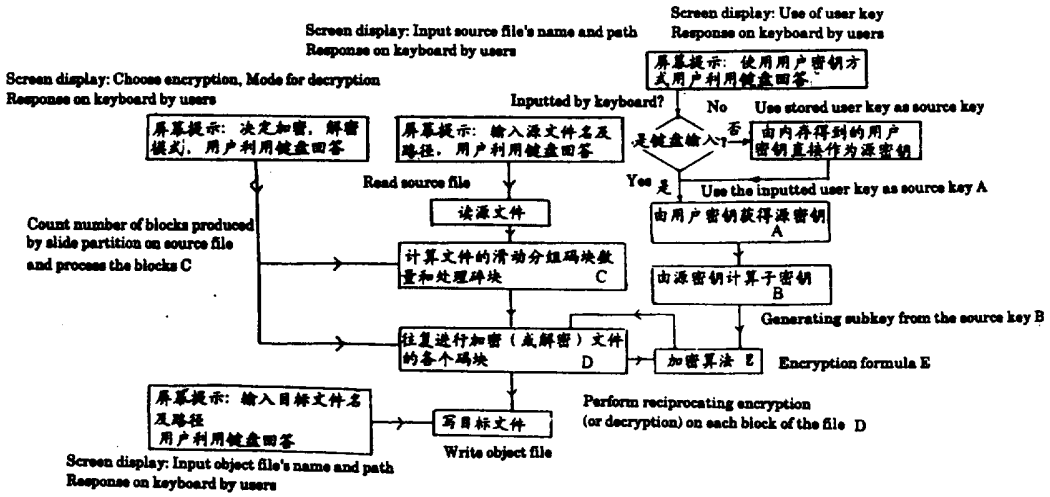
(74) 代理人:柳沈知识产权律师事务所(LIU, SHEN & ASSOCIATES); 中国北京市朝阳区北辰东路8号汇宾大厦A0601, 邮政编码:100101, Bei-jing (CN)。

(81) 指定国:
AM, AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LT, LU, LV, MD, MG, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TT, UA, UG, US, UZ, VN, ARIPO专利(KE, MW, SD, SZ, UG), 欧洲专利(AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI专利(BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG)

本国际公布:
包括国际检索报告。

(54) Title: A METHOD FOR ENCRYPTION OF FILE

(54) 发明名称: 一种文件加密处理方法



(57) Abstract

A method for encryption of file, comprising the steps of performing slide partition on source file block-by-block, each block being 128 bits; generating source key from user key by complementing the user key or by subjecting the user key to pseudo-random number processing; generating subkey from the source key through the use of compression permutation and logic shift; enciphering the blocks through the use of initial permutation, multiplicative conversion and inverse initial permutation, the multiplicative conversion using a cryptographic function including operations of extended conversion, exclusive OR of the subkey, box substitution and E conversion. The method is suitable for generating such digital information as voice and image etc. The executable file thus generated is provided to user in the form of software or being stored in memory, such as ROM and PROM, or being integrated into chips of various specifications, and is highly security and easy to use.

(57) 摘要

一种文件的加密处理以及方法，它是通过对源文件进行滑动分组，每组128比特，及碎块处理，对用户密钥的补充，伪随机数处理，压缩置换，逻辑移位产生出子密钥;对源文件的各码块经初始置换，乘积变换，逆初始置换，加密函数的使用，扩展变换，异或子密钥运算，密盒替代，变换E等途径进行数据加密。适用于文本、声音、图像等数字信号的加密处理。由此产生的可执行文件以软件形式或固化于各类ROM、PROM及做成LSI等各种规格的芯片之上提供给用户，保密性强，使用方便。

以下内容仅供参考

在按照PCT所公布的国际申请小册子首页上所采用的PCT成员国国家代码如下:

AL	阿尔巴尼亚	CM	喀麦隆	IS	冰岛	MG	马达加斯加	SI	斯洛文尼亚
AM	亚美尼亚	CN	中国	IT	意大利	MK	前南斯拉夫马其顿共和国	SK	斯洛伐克
AT	奥地利	CU	古巴	JP	日本			SN	塞内加尔
AU	澳大利亚	CZ	捷克共和国	KE	肯尼亚	ML	马里	SZ	斯威士兰
AZ	阿塞拜疆	DE	德国	KG	吉尔吉斯斯坦	MN	蒙古	TD	乍得
BA	波斯尼亚-黑塞哥维那	DK	丹麦	KP	朝鲜民主主义人民共和国	MR	毛里塔尼亚	TG	多哥
		EE	爱沙尼亚			MW	马拉维	TJ	塔吉克斯坦
BB	巴巴多斯	ES	西班牙	KR	韩国	MX	墨西哥	TM	土库曼斯坦
BE	比利时	FI	芬兰	KZ	哈萨克斯坦	NE	尼日尔	TR	土耳其
BF	布基纳法索	FR	法国	LC	圣卢西亚	NL	荷兰	TT	特立尼达和多巴哥
BG	保加利亚	GA	加蓬	LI	列支敦士登	NO	挪威		
BJ	贝宁	GB	英国	LK	斯里兰卡	NZ	新西兰	UA	乌克兰
BR	巴西	GE	格鲁吉亚	LR	利比里亚	PL	波兰	UG	乌干达
BY	白俄罗斯	GH	加纳	LS	莱索托	PT	葡萄牙	US	美国
CA	加拿大	GN	几内亚	LT	立陶宛	RO	罗马尼亚	UZ	乌兹别克斯坦
CF	中非共和国	GR	希腊	LU	卢森堡	RU	俄罗斯联邦	VN	越南
CG	刚果	HU	匈牙利	LV	拉脱维亚	SD	苏丹	YU	南斯拉夫
CH	瑞士	IE	爱尔兰	MC	摩纳哥	SE	瑞典		
CI	科特迪瓦	IL	以色列	MD	莫尔多瓦	SG	新加坡		

一种文件加密处理方法

所属技术领域

本发明涉及密码技术中的文件加密处理技术，更确切的涉及一种适用于数据处理中的文件加密(解密)处理方法。

背景技术

由于信息是一种资源，所以她就存在着安全保护的必要性。在计算机存贮和计算机通讯系统中，信息是用“0”和“1”的不同组合来构成的，也就是说，所有的信息在计算机中都是用数据来表示的。为了数据的安全，产生了许多数据加密的技术方案。其中，数据加密标准DES(Data Encryption Standard)算法是目前通用的数据加密法。然而这种算法有以下几个缺点：(1)它的密钥量为2^{56}。在出现了高速计算机的今天，这个密钥量显得小了些。因为破译者可以运用穷举法在高速计算机上来取得密钥。这对于那些比较重要的信息，需要保存较长时间的密文和对不同的加密对象采用同样的密钥是很不利的。(2)它的基础之一是由称为S_Box的替代密盒完成的压缩替换。替代密盒中有8个替代表，在某些替代表中，在相同的列号而行号不同的位置上有着相同的元素值；而且相同的行号、列号在不同的替代表中却有着相同的元素值。这样的元素多于76对。(3)它的变换E是一种对称型的替代，这就使得DES的研究者可以把S_Box和变换E分割开来进行分析，这就便于破译密文。

在DES算法的实际应用中，曾经采用了密码块编链法CBC(Cipher Block Chaining)，这种方法有二个缺点：(1)当改变源文件的任意一比特时，并不能使目标文件的每一比特都有变化的可能。(2)需要对初始变量IV(Initial Variable)进行加密传送。

发明目的

本发明的目的是要提供一种数据处理中的文件加密的处理方法，使得在计算机存贮系统和计算机通讯系统中，实施以分离软件形似或固化于各类ROM、PROM或作为操作系统内容之一存在于硬盘之中的该方法对任意格式一定长度的数据文件进行加密(或解密)。

技术方案

为实现上述本发明的目的，本发明技术方案如下：

在常规的计算机及其外围设备所构成的系统中，在操作系统控制下，针对用户指定的目标文件进行加密（或解密）工作，步骤如下：

首先由用户确定：加密（或解密）的工作模式；源文件名及其路径；目标文件名及其路径；用户密钥。

根据用户上述输入，在内存中记录工作模式（加密或解密）。

根据用户确定的用户密钥，当其由键盘输入取得时，共有ASCII码值由20H到7EH的95个码值被用作用户密钥，其字节长度可在1-16之间变化，当其长度小于16字节时，把其补足到16字节，继而对键盘输入的用户密钥每字节的高4位进行伪随机数处理，如此形成16字节长的源密钥；而当用户确定的用户密钥是从内存中取得时，就直接把16字节长的用户密钥作为源密钥。

根据所得到的源密钥通过压缩置换及逻辑移位等变换计算而得到子密钥。

上述由键盘键入的用户密钥补足为16字节长的步骤为：

把补充的密钥字节量作为循环数，把用户密钥的首字节作为第一噪声源，末字节作为第二噪声源，在循环体中，先将第一噪声源乘以第二噪声源，其乘积除以10，如果其商的低8位等于零，则把商的高8位作为补充密钥，如果其商的低8位不等于零，则把商的低8位作为补充密钥，然后把补充密钥作为第二噪声源，如果循环没结束又回到循环体的开始，执行循环体中的操作，如循环结束，则把补充密钥的首字节逻辑乘1FH。

上述对由键盘输入的用户密钥每字节的高4位进行伪随机数处理的步骤如下：

把键盘输入的用户密钥的字节长度作为循环数，把键盘输入的用户密钥的首字节作为第一噪声源，末字节作为第二噪声源，（如果有补充密钥的话，则把补充密钥的末字节作为第二噪声源）。在循环体中，先将第一噪声源乘以第二噪声源，上述的乘积除以10，如果其商的低8位等于零，则把商的高8位作为第二噪声源，如果其商的低8位不等于零，则把商的低8位作为第二噪声源；然后执行下面的操作，如果第二噪声源的高4位等于零，则把密钥的高4位异或第二噪声源的低4位，如果第二噪声源的高4位不等于零，则把密钥的高4位异或第二噪声源的高4位；将上述结果中的第二噪声源作为下一个循环的输入进行循环，如循环没结束，又回到循环体的开始，执行循环体中的操作，直至循环结束形成

16字节长的源密钥;

上述由源密钥通过压缩置换及逻辑移位等变换而计算子密钥的步骤如下:

由源密钥计算子密钥，16字节的源密钥共有128比特，先将这128比特从首部开始依位置顺序编号为1,2,3,...,127,128，经过压缩置换1成为C_0D_0，再经逻辑移位成为C_iD_i(i=1,32)，经压缩置换2后输出，其中C_iD_i(i=1,32)的产生由函数LM_i与C_{i-1}，D_{i-1}分别决定即由下式所示:

$C_i=LM_i(C_{i-1})$ (i=1,32)

$D_i=LM_i(D_{i-1})$ (i=1,32)

其中函数LM_i表示逻辑移位，见图8。

压缩置换1见图7所示，把源密钥的第115位作为C_0D_0的第1位，把源密钥的第99位作为C_0D_0的第2位，依此类推，形成了112比特长的C_0D_0;

压缩置换2见图9所示，把C_iD_i的第14位作为K_i的第1位，把C_iD_i的第27位作为K_i的第2位，依此类推，形成了96比特长的子密钥K_i；在形成每一个子密钥K_i(i=1,32)时，压缩置换2都是相同的，只是对应的C_iD_i各不相同。

根据用户所确定的源文件及路径名，将源文件读入内存，分别对其进行滑动分组、计算滑动分组码块数量、处理碎块。

上述滑动分组步骤如下:

对源文件进行滑动分组，处理方法是把前一组码块的加密(或解密)结果的后面M个(M为整数，可取1至4之一)字节作为后一码块的前M个字节，在正向滑动操作模式下，这样的一组一组的码块经加密(或解密)后，产生了同样组数的新的码块，然后又以逆向方式对前述的新的码块组成的数字序列进行滑动分组，即从新的数据系列的尾部以逆向滑动操作模式开始进行滑动分组，处理方法是把前一组码块的加密(或解密)结果的后面M个字节作为后一码块的前M个字节，这样的一组一组的码块经加密(或解密)后，就产生了对应于源文件的目标文件，即密文(或明文)。

上述计算滑动分组码块数量的步骤如下:

计算码块数量和碎块长度的方法是先取文件的字节长度除以(16-M)，如加密则把(商+1)作为商，然后把((16-M)-余数)作为碎块字节长度，把商给码块数量;如不加密，则直接把商给码块数量。

上述处理碎块步骤如下:

处理碎块即把滑动分组剩下的一些明文信息进行处理，其方法是增

加一些信息使之凑齐一组数据，所增加的信息必须包含有一个特殊信息即碎块长度，使之在解密时，据此把新增加的信息截断，完整地恢复原明文的面貌，其余的新增信息用伪随机数填充，其做法是把(碎块长度-1)作为循环数，循环数等于零，直接将碎块长度送至碎块区；循环数不等于零，则把源密钥的首字节作为第一噪声源，把源密钥的末字节作为第二噪声源，在循环体中，先将第一噪声源乘以第二噪声源，上述的乘积除以10，如果其商的低8位等于零，则把商的高8位作为第二噪声源，如果其商的低8位不等于零，则把商的低8位作为第二噪声源；然后把第二噪声源送到碎块区，如循环未结束，则又返回到循环体的开始，执行循环体中的操作，循环结束则把碎块长度送至碎块区；

经上述处理后，对所得的源文件各码块进行加密（或解密）处理，

对加密(或解密)采取了往复进行的形式，其方法是第一次由源文件头开始依次对各滑动分组码块进行加密(或解密)，第二次则从文件尾部开始，逆向进行；首先是把码块数量作为循环数，把源数据地址指针和目标数据地址指针均指向文件缓冲区首地址，在循环体中，先执行加密算法，然后把源数据地址指针、目标数据地址指针均增加(16-M)，循环末结束则又返回到循环体的开始，执行循环体中的操作，循环结束就得到了一个新的数字序列。然后对这个新的数字序列进行逆向方式的加密（或解密），把码块数量作为循环数，把源数据地址指针和目标数据地址指针均指向新的数字序列末第16字节处，在循环体中，先执行加密算法，然后把源数据地址指针、目标数据地址指针均减少(16-M)，如循环未结束则回到循环体的开始，执行循环体中的操作，如循环已经结束就得到了源文件所对应的密文（或明文）。任务完成后，返回操作系统；

所述加密算法由初始置换，乘积变换，逆初始置换所组成，输入128比特的明文(密文)和长度为12字节的子密钥32个， 其输出是128比特的密文(明文)；

初始置换的方案如图16是把输入数据的第122位作为初始置换结果的第1位，把输入数据的第114位作为初始置换结果的第2位，依此类推，获得经初始置换后的128比特的输出数据。

乘积变换是一个不断迭代的过程，共进行32次，初始置换的输出作为第一次迭代的输入，以后的操作就是把前一次迭代的输出作为后一次迭代的输入，第32次迭代的结果作为逆初始置换的输入；在图15中，用O表示每一次迭代输出(或输入)数据的奇数字节， E表示偶数字节，F表

示加密函数，加密时，对第i次的迭代使用了子密钥K_i，并且$O_i=E_{i-1}$，$E_i=F(E_{i-1}\oplus O_{i-1})$ (i=1,32)，解密时，对第i次的迭代使用了子密钥K_{33-i}，并且$E_i=O_{i-1}$，$O_i=F(O_{i-1})\oplus E_{i-1}$ (i=1,32)；

逆初始置换的方案如图17，把乘积变换的最后结果的第80位作为逆初始置换结果的第1位，把乘积变换的最后结果的第16位作为逆初始置换结果的第2位，依此类推，获得逆初始置 换后的128比特的输出数据。

所述加密函数F是算法的核心，它是由扩展变换，异或子密钥运算，密盒替代，变换E所组成对于输入64比特的数据，先经过扩展变换成96比特的数据，再把扩展变换的结果和96比特的子密钥进行异或作用，得到异或的结果为96比特的数据，又经密盒替代成64比特的数据，最后经过变换E，输出64比特数据；

所述扩展变换图19表示了扩展变换的规则，它将64比特的输入数据变成96比特的输出数据，将输入序列的第64位作为输出序列的第1位，将输入序列的第1位作为输出序列的第2位，依此类推，进行操作。

所述密盒替代是一种压缩替换，本发明的每一个密盒中有16个密表，每一个密表分成为4行×16列。把输入的96比特数据依次平均分成16组，每组6比特，每一组的替代依次对应一个密表，在6比特的输入数据中，头尾2比特组成行号，中间4比特组成列号，依此行号、列号在对应的密表中提取出元素值作为输出，各组的输出依次组合在一起，成为密盒替代的输出数据64比特；

可以有一个密盒的16个密表如图20，图21所示，如果把图20，图21所示的16个密表中的任意2个密表的位置对调，则又组成了一个新的密盒；如果把图20，图21所示的列号相同的任意2个列的位置同时对调(或是把前述的新的密盒的列号相同的任意2个列的位置同时对调)，则也组成了一个新的密盒。依此类推，可以知道本发明提出了一个密盒群，共有$(16!)^2$个密盒。

所述变换E是一种置乱，它利用了伪随机数和另一数（称为RA）进行异或作用得到的数仍是伪随机数，伪随机数与RA的产生都应尽量与变换E的输入数据有关，伪随机数序列的产生依公式

$X_{i+2}=(X_i \cdot X_{i+1}) \text{ MOD } M$ 当$X_{i+2}\neq 1$时

X_{i+2}=小于M的最大素数 当$X_{i+2}=1$时

其中，M为素数，$X_0\neq 0,M$；$X_1\neq 0,1,M$；$i=0,1,\cdots,(n-2)$，n为自然数。

由密盒替代所得到的64比特的数据作为本过程的输入，对变换E的

操作可以是这样的：首先把64比特的输入数据依次赋予$SX_i(i=0,7)$，SX_i的长度是一个字节；令变量S为一个字节长，据公式$S=(\sum_{i=0}^{7}SX_i) MOD\ 256$，求出S；如果$\sum_{i=0}^{7}SX_i=0$，则令$SX_0=241$，$SX_1=239$。然后从$SX_i$的首部开始依次搜索第一次出现的非0、非251值的字节，如果找到了，就把该字节作为第一噪声源，如未找到，则把241作为第一噪声源；再从SXi的尾部开始逆序搜索第一次出现的非0，非1，非251值的字节，如找到了，就把该字节作为第二噪声源，如未找到，则把239作为第二噪声源。把8作为循环数，且令变量i = 0，在循环体中，第一阶段操作是把第一噪声源乘以第二噪声源，把其乘积除以251，得到余数R，把 $(R\oplus S\oplus SX_i)$ 的值给SX_i，第二阶段是把本次循环的第二噪声源作为下一个循环的第一噪声源，把余数R作为下一个循环的第二噪声源，（如果R=1，则把239作为第二噪声源）。接着把变量i增加1，如循环未结束，则又回到循环体的开始，执行循环体中的操作，如果循环结束，则把$SX_i(i=0,7)$作为加密函数F的结果输出。

变换E的操作还可以是这样的：如图22所示，把64比特的输入数据依次赋予$SX_i(i=0,3)$，SX_i的长度是一个字，相应于上述的变换E的操作，相应的改动之处可以根据以下的事实：(1)在无符号的整数中，一个字节的最大值为255，一个字的最大值为65535；(2)在一个字节的范围内，素数从大到小的排列依次是：251，241，239，233，...；在一个字的范围内，相应的排列是：65521，65519，65497，65479，...。

图面说明

下面结合附图通过实施例以清楚地说明本发明的具体内容。

图1．本发明的总体硬件示意图

图2．文件加密处理方法概图

图3．由用户密钥获得源密钥的程序图

图4．补充密钥的方法程序图

图5．对用户密钥的高4位进行处理的方法程序图

图6．由源密钥产生子密钥的方法程序图

图7. 压缩置换1的方法图
图8. 逻辑移位函数构图
图9. 压缩置换2的方法图
图10.正向滑动分组示意图
图11.逆向滑动分组示意图
图12.计算码块数量和碎块长度的程序图
图13.处理碎块的方法程序图
图14.对源文件进行加密(或解密)的程序图
图15.数据加密算法的阶梯图
图16.初始置换方法图
图17.逆初始置换方法图
图18.加密函数的逻辑图
图19.扩展变换方法图
图20.密盒中的前8个密表图
图21.密盒中的后8个密表图
图22.变换E的程序图

实现发明的优选实施例

本发明的文件加密处理方法应用于这样的硬件环境：包括计算机存贮系统，计算机通讯系统，中央处理器、内存贮器、键盘、显示器、磁盘驱动器、打印机、通讯接口、软盘，它们之间用控制总线、地址总线、数据总线连接起来，如图1所示，其中：

内存块A(图1)存放加密命令文件，内存块B(图1)存放加密(或解密)对象，即源文件和目标文件，内存块A的起始地址由操作系统决定，内存块B位于计算机内存的高端，在加密命令完成加密(或解密)工作后，内存块B受操作系统控制；

内存块A设有存放加密(或解密)操作模式信息的一个字节物理单元，用户的加密（或解密）请求决定了该物理单元的内容(图1中未标出)；又设有一个字的物理单元，用于存放操作系统信息，它表明系统是属于中文操作系统，还是英文操作系统，还是别的语言的操作系统(图1中未标出)；

根据本发明的实施例中完成加密(或解密)工作的逻辑关系如图2所示．根据屏幕提示，用户分别回答如下四个问题：加密(或解密)的工作

模式，源文件名及其路径，目标文件名及其路径，使用用户密钥的方式；

当用户由键盘上确定了加密(或解密)的模式之后，内存块A中存放加密(或解密)模式信息的物理单元的内容也就跟着确定下来了；

当用户输入正确的源文件名及其路径之后，即可依据该源文件的长度和内存资源的使用情况决定内存块B的大小和起始地址，然后把源文件读至内存块B中去；对内存块B中的源文件进行滑动分组，计算出滑动分组码块数量和处理碎块，然后往复对源文件的各码块执行加密算法；

当把内存块B中的源文件的全部内容进行加密(或解密)之后，就把其中的密文(或明文)写入目标文件中；

当用户密钥由键盘取得时，可以有95个码值被用作用户密钥，其ASCII码值由20H到7EH；用户密钥的字节长度可在1～16之间变化，然后由用户密钥获得源密钥；

由用户密钥获得源密钥，当用户密钥长度小于16字节时，要把密钥进行补充，补足到16字节长，而且对由键盘上得到的用户密钥每字节的高4位进行伪随机数处理；经过上述的过程，形成了16字节长的源密钥(上述如图3 所示)；

把补充的密钥字节量作为循环数，把用户密钥的首字节作为第一噪声源，末字节作为第二噪声源，在循环体中，先将第一噪声源乘以第二噪声源，其乘积除以10，如果其商的低8位等于零，则把商的高8位作为补充密钥，如果其商的低8位不等于零，则把商的低8位作为补充密钥，然后把补充密钥作为第二噪声源，如果循环没结束又回到循环体的开始，执行循环体中的操作，如循环结束，则把补充密钥的首字节逻辑乘1FH，(上述如图4所示)；

把用户密钥的字节长度作为循环数，把用户密钥的首字节作为第一噪声源，末字节作为第二噪声源，如果有补充密钥的话，则把补充密钥的末字节作为第二噪声源。在循环体中，先将第一噪声源乘以第二噪声源，上述的乘积除以10，如果其商的低8位等于零，则把商的高8位作为第二噪声源，如果其商的低8位不等于零，则把商的低8位作为第二噪声源；然后执行下面的操作，如果第二噪声源的高4位等于零，则把密钥的高4位异或第二噪声源的低4位，如果第二噪声源的高4位不等于零，则把密钥的高4位异或第二噪声源的高4位；将上述结果中的第二噪声源作为下一个循环的输入进行循环，如循环没结束，又回到循环体的开始，执行循环体中的操作，如循环结束则进入计算子密钥的步骤(上述如图5

所示);

当用户密钥是从内存中取得时，就直接把16字节长的用户密钥作为源密钥;

由源密钥计算子密钥，16字节的源密钥共有128比特，先将这128比特从首部开始依位置顺序编号为1,2,3,...,127,128，经过压缩置换1成为C_0D_0，再经逻辑移位成为C_iD_i(i=1,32)，压缩置换2后输出，(如图6所示)，其中图6所示的C_iD_i(i=1,32)的产生由函数LM_i与C_{i-1}，D_{i-1}分别决定即由下式所示:

$C_i=LM_i(C_{i-1})$ (i=1,32)

$D_i=LM_i(D_{i-1})$ (i=1,32)

其中函数LM_i表示逻辑移位，见图8;

压缩置换1见图7所示，把源密钥的第115位作为C_0D_0的第1位，把源密钥的第99位作为C_0D_0的第2位，依此类推，形成了112比特长的C_0D_0;

压缩置换2见图9所示，把C_iD_i的第14位作为K_i的第1位把C_iD_i的第27位作为K_i的第2位，依此类推，形成了96比特长的子密钥K_i；在形成每一个子密钥K_i(i=1,32)时，压缩置换2都是相同的，只是对应的C_iD_i各不相同;

对源文件进行滑动分组，优选地，把前一组码块的加密(或解密)结果的后面二个字节作为后一码块的前二个字节，其正向滑动操作模式如图10所示，N为自然数；这样的一组一组的码块经加密(或解密)后，产生了同样组数的新的码块，然后又以逆向方式对前述的新的码块组成的数字序列进行滑动分组，即从新的数据系列的尾部开始进行滑动分组，如图11所示，其中N为自然数;处理方法是把前一组码块的加密（或解密）结果的后面二个字节作为后一码块的前二个字节，这样的一组一组的码块经加密(或解密)后，就产生了对应于源文件的目标文件，即密文（或明文）。

计算码块数量和碎块长度的方法是先取文件的字节长度除以14，如加密则把(商+1)作为商，然后把(14-余数)作为碎块字节长度，把商给码块数量；如不加密，则直接把商给码块数量，见图12,

处理碎块即把滑动分组剩下的一些明文信息进行处理，其方法是增加一些信息使之凑齐一组数据，所增加的信息必须包含有一个特殊信息即碎块长度，使之在解密时，据此把新增加的信息截断，完整地恢复原明文的面貌，其余的新增信息用伪随机数填充，其做法是把(碎块长度-

1)作为循环数，循环数等于零，直接将碎块长度送至碎块区；循环数不等于零，则把源密钥的首字节作为第一噪声源，把源密钥的末字节作为第二噪声源，在循环体中，先将第一噪声源乘以第二噪声源，上述的乘积除以10，如果其商的低8位等于零，则把商的高8位作为第二噪声源，如果其商的低8位不等于零，则把商的低8位作为第二噪声源；然后把第二噪声源送到碎块区，如循环未结束，则又返回到循环体的开始，执行循环体中的操作，循环结束则把碎块长度送至碎块区，如图13所示；

对加密(或解密)采取了往复进行的形式，其方法是第一次由源文件头开始依次对各滑动分组码块进行加密(或解密)，第二次则从文件尾部开始，逆向进行；首先是把码块数量作为循环数，把源数据地址指针和目标数据地址指针均指向文件缓冲区首地址，在循环体中，先执行加密算法，然后把源数据地址指针、目标数据地址指针均增加14，循环未结束则又返回到循环体的开始，执行循环体中的操作，循环结束就得到了一个新的数字序列。然后对这个新的数字序列进行逆向方式的加密（或解密），把码块数量作为循环数，把源数据地址指针和目标数据地址指针均指向新的数字序列末第16字节处，在循环体中，先执行加密算法，然后把源数据地址指针、目标数据地址指针均减少14，如循环未结束则回到循环体的开始，执行循环体中的操作，如循环已经结束就得到了源文件所对应的密文（或明文）。任务完成后，返回操作系统，具体见图14所示；

数据加密算法的阶梯图如图15，由初始置换，乘积变换，逆初始置换所组成，输入128比特的明文(密文)和长度为12字节的子密钥32个，其输出是128比特的密文(明文)，如图15所示；

初始置换的方案如图16，把输入数据的第122位作为初始置换结果的第1位，把输入数据的第114位作为初始置换结果的第2位，依此类推，获得经初始置换后的128比特的输出数据。

乘积变换是一个不断迭代的过程，共进行32次，初始置换的输出作为第一次迭代的输入，以后的操作就是把前一次迭代的输出作为后一次迭代的输入，第32次迭代的结果作为逆初始置换的输入；在图15中，用O表示每一次迭代输出(或输入)数据的奇数字节，E表示偶数字节，F表示加密函数，加密时，对第i次的迭代使用了子密钥K_i，并且$O_i=E_{i-1}$，$E_i=F(E_{i-1})\oplus O_{i-1}(i=1,32)$，解密时，对第i次的迭代使用了子密钥$K_{33-i}$并且$E_i=O_{i-1}$，$O_i=F(O_{i-1})\oplus E_{i-1}$ $(i=1,32)$；

逆初始置换的方案如图17，把乘积变换的最后结果的第80位作为逆初始置换结果的第1位把乘积变换的最后结果的第16位作为逆初始置换结果的第2位，依此类推，获得逆初始置换后的128比特的输出数据。

加密函数F是算法的核心，它是由扩展变换，异或子密钥运算，密盒替代，变换E所组成，如图18所示，对于输入64比特的数据，先经过扩展变换成96比特的数据，再把扩展变换的结果和96比特的子密钥进行异或作用，得到异或的结果为96比特的数据，又经密盒替代成64比特的数据，最后经过变换E，输出64比特数据；

图19表示了扩展变换的规则，它将64比特的输入数据变成96比特的输出数据，将输入序列的第64位作为输出序列的第1位，将输入序列的第1位作为输出序列的第2位，依此类推，进行操作。

密盒替代是一种压缩替换，本实施例的每一个密盒中有16个密表，每一个密表分成为4行×16列。有一个密盒的16个密表如图20，图21所示，如果把图20，图21所示的16个密表中的任意2个密表的位置对调，则又组成了一个新的密盒；如果把图20，图21所示的列号相同的任意2个列的位置同时对调，(或是把前述的新的密盒做到号相同的任意2个列的位置同时对调)则也组成了一个新的密盒。依此类推，可以知道本发明提出了一个密盒群，共有$(16!)^2$个密盒群。把输入的96比特数据依次平均分成16组，每组6比特，每一组的替代依次对应一个密表，在6比特的输入数据中，头尾2比特组成行号，中间4比特组成列号，依此行号、列号在对应的密表中提取出元素值作为输出，各组的输出依次组合在一起，成为密盒替代的输出数据64比特；

所述变换E是一种置乱，它利用了伪随机数和另一数（称为RA）进行异或作用得到的数仍是伪随机数，伪随机数与RA的产生都应尽量与变换E的输入数据有关，伪随机数序列的产生依公式

$X_{i+2}=(X_i \bullet X_{i+1}) \text{MOD } M$ 当$X_{i+2}\neq 1$时

$X_{i+2}=$小于M的最大素数 当$X_{i+2}=1$时

其中，M为素数，$X_0\neq 0,M$；$X_1\neq 0,1,M$；$i=0,1,\cdots,(n-2)$，n为自然数。

由密盒替代所得到的64比特的数据作为本过程的输入，对变换E的操作可以是这样的：首先把64比特的输入数据依次赋予$SX_i(i=0,7)$，SX_i的长度是一个字节；令变量S为一个字节长，据公式$S=\left(\sum_{i=0}^{7} SX_i\right) \text{MOD } 256$,

求出S；如果$\sum_{i=0}^{7} SX_i = 0$，则令$SX_0 = 241$，$SX_1 = 239$。然后从SX_i的首部开始依次搜索第一次出现的非0非251值的字节，如果找到了，就把该字节作为第一噪声源，如未找到，则把241作为第一噪声源；再从SX_i的尾部开始逆序搜索第一次出现的非0，非1，非251值的字节，如找到了，就把该字节作为第二噪声源，如未找到，则把239作为第二噪声源。把8作为循环数，且令变量i = 0，在循环体中，第一阶段操作是把第一噪声源乘以第二噪声源，把其乘积除以251，得到余数R，把(R⊕S⊕SX_i)的值给SX_i，第二阶段是把本次循环的第二噪声源作为下一个循环的第一噪声源，把余数R作为下一个循环的第二噪声源，(如果R=1，则把239作为第二噪声源)。接着把变量i增加1，如循环未结束，则又回到循环体的开始，执行循环体中的操作，如果循环结束，则把SX_i(i=0,7)作为加密函数F的结果输出。

变换E的操作还可以是这样的：如图22所示，把64比特的输入数据依次赋予SX_i(i=0,3)，SX_i的长度是一个字，相应于上述的变换E的操作，相应的改动值之处可以根据以下的事实：(1)在无符号的整数中，一个字节的最大值为255，一个字的最大值为65535；(2)在一个字节的范围内，素数从大到小的排列依次是：251，241，239，233，...；在一个字的范围内，相应的排列是：65521，65519，65497，65479，...。

根据以上所说明的文件加密处理方法，在以上所述本发明的实施例中，还可以优选地：以软件形式(如经编程、编译、连接等工序而形成为操作系统的外部加密命令文件，或带有后缀“EXE”的可执行文件)或固化于各类ROM，PROM做成LSI芯片中。同样优选地，在计算机运行中，可以不必在程序中为数据文件开辟一个专门的数据区，而向操作系统申请一块位于高端地址的内存贮器，如图1中所示的内存块B，用来放置数据文件，以能够充分使用硬件条件下最大有效内存(按照目前操作系统提供的技术，一次可以加密1兆字节长度的数据文件，即可以加密近50万字的一本中文书籍)。反之，解密亦然。在编程时，可优选地使用汇编语言。

如果用户认为必要的话，还可以把第一次加密所产生的目标文件作为第二次加密的源文件，依此类推，可以进行多次的加密，加密进行了多少次，解密也要进行相同的次数，就可以恢复早先的明文。

加密命令包括可以用在中文操作系统，也可以用在英文操作系统中，或其他语言的操作系统中。

在计算机存贮系统和计算机通讯系统中，本发明可以适用于包括文本文件、表格文件、图形文件、图像文件、库函数文件乃至可执行文件等。

本发明提出的数据加密法还可以用在实时的通讯系统中，包括用于图像数字讯号，声音数字讯号的加密与解密。也可以用在无线电通讯中。

本发明提出的数据文件加密处理方法包括可以用在微型计算机上，也可以用在小型计算机上。

本发明提出的数据文件加密处理方法包括适用于单用户操作系统，也适用于多用户操作系统。

有益效果

本发明与目前国内、外的 DES 算法及其变种相比，有以下几个有益的技术效果：

1. 密钥量大为2^{112}，且由键盘取得的密钥长度可变。

2. 本发明提出了一个密盒群，共有$(16!)^2$个密盒。在每一个替代密盒中，有16个密表；相同的行号、列号在16个密表中的元素各不相同；在16个密表中，同一列上的各元素值不同，同一行上的各元素也不相同。所以，每一次的密盒替代是贯彻了“一次一密”体制的。

3. 把变换E与伪随机数联系起来，使变换E成了“黑盒子”。在加密函数中，它与替代密盒连接而成为一体。采用这种技术方案，使用本算法在理论上是不可破译的。

4. 对数据文件使用了往复式的滑动分组编链法。它有二个好处：(1)改变源文件中的任一比特值，都会使目标文件中的任一比特都有发生变化的可能。(2)不需要密码块编链法CBC中的初始变量IV，使得本发明便于和公开密钥体制进行衔接。(3)更难破译。

5. 对用户密钥码值的高4位分别进行与伪随机数字序列的异或运算，可以使人的行为习惯不会在密文中表现出来，增加了破译困难。

6. 在本发明中，可优选地把操作对象即数据文件放置在计算机内存的高端，这样就可充分利用内存，对一定长度的数据文件进行加密（或解密），而且还能形成操作系统的外部加密命令，增强了文件管理类型命令的功能，丰富了操作系统的内容。

7. 相对于那些码块较短的算法来说，本发明由于加密的各个码块的长度为16字节，就容易使官文值在0～255上的分布得更理想。

上面以本发明优选实施例对本发明给予了说明，可以理解在不脱离本发明后附权利要求的精神下，本领域的技术人员可以做出多种改进与变形。

权利要求书

1. 一种文件加密处理方法，在常规的计算机及其外围设备所构成的系统中（包括计算机存贮系统，计算机通讯系统，中央处理器、内存贮器、键盘、显示器、磁盘驱动器、打印机、通讯接口、软盘，它们之间用控制总线、地址总线、数据总线连接起来），在操作系统控制下，针对用户指定的目标文件进行加密（或解密）工作，步骤如下：

(1) 由用户确定：加密（或解密）的工作模式；源文件名及其路径；目标文件名及其路径；用户密钥；

(2) 根据用户上述输入，在内存中记录工作模式（加密或解密）；

(3) 根据用户确定的用户密钥，当其是从内存中取得时，就直接把16字节长的用户密钥作为源密钥；

(4) 根据用户确定的用户密钥，当其由键盘输入取得时，共有ASCII码值由20H到7EH的95个码值被用作用户密钥，其字节长度可在1-16之间变化，当其长度小于16字节时，把其补足到16字节其过程为：

把补充的密钥字节量作为循环数，把用户密钥的首字节作为第一噪声源，末字节作为第二噪声源，在循环体中，先将第一噪声源乘以第二噪声源，其乘积除以10，如果其商的低8位等于零，则把商的高8位作为补充密钥，如果其商的低8位不等于零，则把商的低8位作为补充密钥，然后把补充密钥作为第二噪声源，如果循环没结束又回到循环体的开始，执行循环体中的操作，如循环结束，则把补充密钥的首字节逻辑乘1FH；

继而对键盘输入的用户密钥每字节的高4位进行伪随机数处理，其过程为：

把键盘输入的用户密钥的字节长度作为循环数，把键盘输入的用户密钥的首字节作为第一噪声源，末字节作为第二噪声源，（如果有补充密钥的话，则把补充密钥的末字节作为第二噪声源），在循环体中，先将第一噪声源乘以第二噪声源，上述的乘积除以10，如果其商的低8位等于零，则把商的高8位作为第二噪声源，如果其商的低8位不等于零，则把商的低8位作为第二噪声源；然后执行下面的操作，如果第二噪声源的高4位等于零，则把密钥的高4位异或第二噪声源的低4位，如果第二噪声源的高4位不等于零，则把密钥的高4位异或第二噪声源的高4位；将上述结果中的第二噪声源作为下一个循环的输入进行循环，如循环没结束，又回到循环体的开始，执行循环体中的操作，直至循环结束，如

此形成16字节长的源密钥;

(5) 根据所得到的源密钥通过压缩置换及逻辑移位等变换计算而得到子密钥，其过程如下:

由源密钥计算子密钥，16字节的源密钥共有128比特，先将这128比特从首部开始依位置顺序编号为1,2,3,...,127,128，经过压缩置换1成为C_0D_0，再经逻辑移位成为C_iD_i(i=1,32)，经压缩置换2后输出，其中C_iD_i(i=1,32)的产生由函数LM_i与C_{i-1}，D_{i-1}分别决定，即由下式所示:

$C_i=LM_i(C_{i-1})$ (i=1,32)

$D_i=LM_i(D_{i-1})$ (i=1,32)

其中函数LM_i表示逻辑移位，如下表所示:

第 i 次迭代	LMi (循环左移位数)	第 i 次迭代	LMi (循环左移位数)
1	1	17	1
2	1	18	1
3	2	19	2
4	2	20	2
5	2	21	2
6	2	22	2
7	2	23	2
8	2	24	2
9	1	25	1
10	2	26	2
11	2	27	2
12	2	28	2
13	2	29	2
14	2	30	2
15	2	31	2
16	1	32	1

压缩置换1如下表所示，把源密钥的第115位作为C_0D_0的第1位，把源密钥的第99位作为C_0D_0的第2位，依此类推，形成了112比特长的C_0D_0;

115	99	83	67	51	35	19	3
117	101	85	69	53	37	21	5
119	103	87	71	55	39	23	7
123	107	91	75	59	43	27	11
125	109	93	77	61	45	29	13
127	111	95	79	63	47	31	15
114	98	82	66	50	34	18	2
128	112	96	80	64	48	32	16
126	110	94	78	62	46	30	14
124	108	92	76	60	44	28	12
122	106	90	74	58	42	26	10
120	104	88	72	56	40	24	8
118	102	86	70	54	38	22	6
116	100	84	68	52	36	20	4

压缩置换2如下表所示，把C_iD_i的第14位作为K_i的第1位，把C_iD_i的第27位作为K_i的第2位，依此类推，形成了96比特长的子密钥K_i；在形成每一个子密钥K_i(i=1,32)时，压缩置换2都是相同的，只是对应的C_iD_i各不相同；

14	27	31	1	6	101	93	80
4	94	43	26	67	59	15	97
23	57	36	75	50	109	39	9
49	106	69	7	32	72	86	52
102	66	28	78	112	11	38	60
91	8	87	47	81	62	17	103
54	96	16	88	34	110	84	42
73	58	85	21	99	51	2	79
45	111	46	89	56	10	74	68
55	5	106	37	70	95	48	22
13	19	77	104	24	40	90	63
30	108	33	64	20	98	41	82

(6) 根据用户所确定的源文件及路径名，将源文件读入内存；

(7) 对源文件进行滑动分组，步骤如下：

把前一组码块的加密(或解密)结果的后面二个字节作为后一码块的前二个字节，在正向滑动操作模式下，这样的一组一组的码块经加密(或解密)后，产生了同样组数的新的码块，然后又以逆向方式对前述的新的码块组成的数字序列进行滑动分组，即从新的数据系列的尾部开始进行滑动分组，处理方法是把前一组码块的加密(或解密)结果的后面二个字节作为后一码块的前二个字节，这样的一组一组的码块经加密(或解密)后，就产生了对应于源文件的目标文件，即密文（或明文）；

(8) 对源文件计算滑动分组码块数量和碎块长度，其步骤如下：

先取文件的字节长度除以14，如加密，则把(商+1)作为商，然后把(14-余数)作为碎块字节长度，把商给码块数量；如不加密，则直接把商给码块数量；

(9) 对源文件处理碎块，其步骤如下：

对于滑动分组剩下的一些明文信息增加一些信息使之凑齐一组数据，所增加的信息必须包含有一个特殊信息即碎块长度，使之在解密时，据此把新增加的信息截断，完整地恢复原明文的面貌，其余的新增信息用伪随机数填充，其做法是把(碎块长度-1)作为循环数，循环数等于零，直接将碎块长度送至碎块区；循环数不等于零，则把源密钥的首字节作为第一噪声源，把源密钥的末字节作为第二噪声源，在循环体中，先将第一噪声源乘以第二噪声源，上述的乘积除以10，如果其商的低8位等于零，则把商的高8位作为第二噪声源，如果其商的低8位不等于零，则把商的低8位作为第二噪声源；然后把第二噪声源送到碎块区，如循环未结束，则又返回到循环体的开始，执行循环体中的操作，循环结束则把碎块长度送至碎块区；

(10)对所得的源文件各码块进行加密（或解密）处理，采取了往复进行的形式，其步骤如下：第一次由源文件头开始依次对各滑动分组码块进行加密(或解密)，第二次则从文件尾部开始，逆向进行；首先是把码块数量作为循环数，把源数据地址指针和目标数据地址指针均指向文件缓冲区首地址，在循环体中，先执行加密算法，然后把源数据地址指针、目标数据地址指针均增加14，循环未结束则又返回到循环体的开始，执行循环体中的操作，循环结束就得到了一个新的数字序列，然后对这

个新的数字序列进行逆向方式的加密（或解密），把码块数量作为循环数，把源数据地址指针和目标数据地址指针均指向新的数字序列末第16字节处，在循环体中，先执行加密算法，然后把源数据地址指针、目标数据地址指针均减少14，如循环未结束则回到循环体的开始，执行循环体中的操作，如循环已经结束就得到了源文件所对应的密文（或明文），任务完成后，返回操作系统；

所述加密算法由初始置换，乘积变换，逆初始置换所组成，输入128比特的明文(密文)和长度为12字节的子密钥32个，其输出是128比特的密文(明文)；

初始置换的方案如下表所示，把输入数据的第122位作为初始置换结果的第1位，把输入数据的第114位作为初始置换结果的第2位，依此类推，获得经初始置换后的128比特的输出数据；

122	114	106	98	90	82	74	66	58	50	42	34	26	18	10	2
124	116	108	100	92	84	76	68	60	52	44	36	28	20	12	4
126	118	110	102	94	86	78	70	62	54	46	38	30	22	14	6
128	120	112	104	96	88	80	72	64	56	48	40	32	24	16	8
121	113	105	97	89	81	73	65	57	49	41	33	25	17	9	1
123	115	107	99	91	83	75	67	59	51	43	35	27	19	11	3
125	117	109	101	93	85	77	69	61	53	45	37	29	21	13	5
127	119	111	103	95	87	79	71	63	55	47	39	31	23	15	7

乘积变换是一个不断迭代的过程，共进行32次，初始置换的输出作为第一次迭代的输入，以后的操作就是把前一次迭代的输出作为后一次迭代的输入，第32次迭代的结果作为逆初始置换的输入；在图15中，用O表示每一次迭代输出(或输入)数据的奇数字节，E表示偶数字节，F表示加密函数，加密时，对第i次的迭代使用了子密钥K_i，并且$O_i=E_{i-1}$，

$E_i=F(E_{i-1})\oplus O_{i-1}$ (i=1,32)，解密时，对第i次的迭代使用了子密钥K_{33-i}
并且$E_i=O_{i-1}$, $O_i=F(O_{i-1})\oplus E_{i-1}$ (i=1,32)；

逆初始置换的方案如下表所示，把乘积变换的最后结果的第80位作为逆初始置换结果的第1位把乘积变换的最后结果的第16位作为逆初始置换结果的第2位，依此类推，获得逆初始置 换后的128比特的输出数据。

80	16	96	32	112	48	128	64	79	15	95	31	111	47	127	63
78	14	94	30	110	46	126	62	77	13	93	29	109	45	125	61
76	12	92	28	108	44	124	60	75	11	91	27	107	43	123	59
74	10	90	26	106	42	122	58	73	9	89	25	105	41	121	57
72	8	88	24	104	40	120	56	71	7	87	23	103	39	119	55
70	6	86	22	102	38	118	54	69	5	85	21	101	37	117	53
68	4	84	20	100	36	116	52	67	3	83	19	99	35	115	51
66	2	82	18	98	34	114	50	65	1	81	17	97	33	113	49

所述加密函数F是算法的核心，它是由扩展变换， 异或子密钥运算，密盒替代，变换E所组成，对于输入64比特的数据，先经过扩展变换成96比特的数据，再把扩展变换的结果和96比特的子密钥进行异或作用，得到异或的结果为96比特的数据，又经密盒替代成64比特的数据，最后经过变换E，输出64比特数据；

所述扩展变换如下表所示，表示了扩展变换的规则，它将64比特的输入数据变成96比特的输出数据，将输入序列的第64位作为输出序列的第1位， 将输入序列的第1位作为输出序列的第2位，依此类推，进行操作；

64	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	33
32	33	34	35	36	37	36	37
38	39	40	41	40	41	42	43
44	45	44	45	46	47	48	49
48	49	50	51	52	53	52	53
54	55	56	57	56	57	58	59
60	61	60	61	62	63	64	1

所述密盒替代是一种压缩替换，本发明的每一个密盒中有16个密表，每一个密表分成为4行×16列，　把输入的96比特数据依次平均分成16组，每组6比特，每一组的替代依次对应一个密表，在6比特的输入数据中，头尾2比特组成行号，中间4比特组成列号，依此行号、列号在对应的密表中提取出元素值作为输出，各组的输出依次组合在一起，成为密盒替代的输出数据64比特；

所述变换E是一种置乱，它利用了伪随机数和另一数进行异或作用得到的数仍是伪随机数。

2. 如权利要求1所述的文件加密处理方法，其中所述的密盒替代中可以有一个密盒的16个密表如下表A、表B所示；

如果把表A、表B所示的16个密表中的任意2个密表的位置对调，则又组成了一个新的密盒；　如果把表A、表B所示的列号相同的任意2个列的位置同时对调（或是把前述的新的密盒的列号相同的任意二个列的位置同时对调），则也组成了一个新的密盒，依此类推，可以知道本发明提出了一个密盒群，共有 $(16!)^2$ 个密盒；

		列															
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S0	行0	15	1	5	6	10	9	4	12	8	11	2	7	3	0	13	14
	1	6	5	15	10	9	4	1	2	0	7	13	12	11	14	8	3
	号2	8	6	14	1	3	7	9	0	12	10	5	4	2	11	15	13
	3	1	2	0	8	11	5	10	13	9	14	6	15	4	7	3	12
S1		10	2	7	8	4	6	15	5	9	0	1	13	14	12	3	11
		15	6	2	9	12	3	0	8	7	5	11	10	4	13	14	1
		9	0	15	4	2	10	1	3	13	11	6	5	7	14	8	12
		0	14	6	7	15	13	9	10	8	1	3	4	11	2	12	5
S2		14	10	8	7	3	5	2	6	15	9	0	4	12	11	1	13
		7	4	1	8	15	0	5	10	3	6	12	11	9	2	13	14
		1	7	6	12	5	9	11	8	10	2	14	3	4	13	0	15
		10	15	2	0	12	14	1	11	7	8	13	6	5	4	9	3
S3		13	0	10	5	9	8	14	3	11	1	15	12	6	7	2	4
		8	7	0	1	11	15	4	9	5	13	10	14	3	12	6	2
		2	1	5	3	4	11	12	7	15	9	13	10	8	0	14	6
		11	5	4	2	3	12	0	14	6	15	8	13	10	9	7	1
S4		7	9	6	4	2	13	5	11	12	10	14	1	15	3	0	8
		3	2	5	7	14	1	8	0	6	4	15	9	13	10	11	12
		10	15	4	2	7	12	0	5	14	8	9	11	6	1	13	3
		9	6	15	5	13	10	4	1	3	11	7	14	2	12	8	0
S5		3	11	9	2	8	12	13	4	7	5	10	6	1	15	14	0
		9	8	6	3	10	14	7	1	4	2	0	15	12	11	5	13
		11	14	7	0	1	13	10	2	5	6	1	9	15	4	3	8
		8	7	14	4	0	11	3	15	12	10	5	2	6	1	13	9
S6		8	4	15	9	5	10	3	1	2	12	13	0	11	14	7	6
		5	14	9	12	8	11	6	13	1	10	4	7	2	0	3	15
		14	10	3	13	12	8	5	6	11	4	7	15	9	2	1	0
		4	3	10	15	1	9	11	12	5	2	14	8	13	6	0	7
S7		4	3	2	10	12	15	6	9	1	8	7	14	0	13	11	5
		14	12	8	11	1	13	9	3	10	0	6	5	7	15	2	4
		0	9	13	6	11	14	8	15	4	3	1	7	12	10	5	2
		3	13	1	9	6	0	7	8	2	12	10	11	14	5	4	15

表 A

		列号															
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S8	行0	6	5	14	0	15	11	8	7	10	13	12	2	4	1	9	3
	1	0	11	7	6	3	5	14	12	15	9	2	13	1	4	10	8
	号2	13	2	1	5	6	15	3	14	9	7	10	8	0	12	4	11
	3	2	4	3	1	10	7	12	5	13	0	11	9	15	8	6	14
S9		0	13	12	11	6	7	1	8	14	3	9	15	2	5	4	10
		11	3	14	5	2	12	10	4	13	1	8	6	15	9	0	7
		5	8	0	14	10	6	15	9	3	12	2	1	13	7	11	4
		13	0	11	10	14	4	8	2	1	9	12	7	3	15	5	6
S10		2	8	4	12	7	14	0	13	5	15	11	3	9	6	10	1
		1	10	3	4	13	6	11	15	12	8	9	2	14	5	7	0
		12	5	9	11	8	0	2	4	1	14	15	13	10	3	6	7
		7	9	12	3	5	15	13	0	10	6	4	1	8	14	2	11
S11		5	12	11	3	14	1	7	0	13	2	8	9	10	4	6	15
		10	9	4	15	0	2	13	14	8	3	5	1	6	7	12	11
		3	13	8	10	9	5	4	1	2	15	0	12	11	6	7	14
		12	8	13	11	2	6	5	9	4	7	15	0	1	3	14	10
S12		12	15	0	1	11	4	9	2	3	14	6	5	13	10	8	7
		4	13	10	0	7	9	12	6	2	11	14	3	8	1	15	5
		7	3	12	15	13	1	6	11	8	0	4	2	14	5	9	10
		15	1	9	6	4	8	14	3	11	5	2	12	7	0	10	13
S13		9	6	1	15	13	2	10	14	0	4	3	11	7	8	5	12
		2	0	11	13	6	10	15	7	14	12	1	8	5	3	4	9
		15	11	2	7	0	4	13	10	6	1	8	14	3	9	12	5
		5	12	8	14	7	3	6	4	15	13	0	10	9	11	1	2
S14		1	7	13	14	0	3	11	15	4	6	5	10	8	2	12	9
		13	15	12	2	5	8	3	11	9	14	7	4	0	6	1	10
		6	4	11	9	15	2	14	12	7	13	3	0	5	8	10	1
		14	11	7	13	8	1	2	6	0	3	9	5	12	10	15	4
S15		11	14	3	13	1	0	12	10	6	7	4	8	5	9	15	2
		12	1	13	14	4	7	2	5	11	15	3	0	10	8	9	6
		4	12	10	8	14	3	7	13	0	5	11	6	1	15	2	9
		6	10	5	12	9	2	15	7	14	4	1	3	0	13	11	8

表 B

3.如权利要求1所述的文件加密处理方法，其中所述的伪随机数序列的产生依公式：

$X_{i+2}=(X_i \cdot X_{i+1}) MOD\ M$ 当$X_{i+2}\neq 1$时

$X_{i+2}=$小于M的最大素数 当$X_{i+2}=1$时

其中，M为素数，$X_0\neq 0,M$；$X_1\neq 0,1,M$；$i=0,1,\cdots,(n-2)$，n为自然数。

4.如权利要求3所述的文件加密处理方法，其中由密盒替代所得到的64比特的数据作为本过程的输入，对变换E的操作可以是这样的：

首先把64比特的输入数据依次赋予$SX_i(i=0,7)$，SX_i的长度是一个字节；令变量S为一个字节长，据公式$S=(\sum_{i=0}^{7} SX_i) MOD\ 256$，求出S；如果$\sum_{i=0}^{7} SX_i=0$，则令$SX_0=241$，$SX_1=239$。然后从$SX_1$的首部开始依次搜索第一次出现的非0，非251值的字节，如果找到了，就把该字节作为第一噪声源，如未找到，则把241作为第一噪声源；再从SXi的尾部开始逆序搜索第一次出现的非0，非1，非251值的字节，如找到了，就把该字节作为第二噪声源，如未找到，则把239作为第二噪声源。把8作为循环数，且令变量i = 0，在循环体中，第一阶段操作是把第一噪声源乘以第二噪声源，把其乘积除以251，得到余数R，把 $(R\oplus S\oplus SX_i)$ 的值给SX_i，第二阶段是把本次循环的第二噪声源作为下一个循环的第一噪声源，把余数R作为下一个循环的第二噪声源，（如果R=1，则把239作为第二噪声源）。接着把变量i增加1，如循环未结束，则又回到循环体的开始，执行循环体中的操作，如果循环结束，则把$SX_i(i=0,7)$作为加密函数F的结果输出；

变换E的操作还可以是这样的：把64比特的输入数据依次赋予SX_i $(i=0,3)$，SX_i的长度是一个字，相应于上述的变换E的操作，相应的改动之处可以根据以下的事实：(1)在无符号的整数中，一个字节的最大值为255，一个字的最大值为65535；(2)在一个字节的范围内，素数从大到小的排列依次是：251，241，239，233，...；在一个字的范围内，相应的排列是：65521，65519，65497，65479，...；

5. 如权利要求1所述的文件加密处理方法，其中所述将用户确定的源文件读入内存时，可以向操作系统中申请一块位于高端地址的内存来放置源文件和目标文件。

6. 一种文件加密处理方法及其软盘，其特征在于它的应用范围，有

(1).由该方法形成的加密(或解密)命令文件(或带后缀“EXE”型的可执行文件)可以写在包括软盘，硬盘上，也可以形成具有加密功能的指令组，将其写在只读存贮器ROM或程序只读存贮器PROM所形成的LSI芯片上；

(2).这样的产品适用于包括文本文件，图像文件等的加密(或解密)，也可以用在实时系统中，包括图像数字讯号，或声音数字讯号的实时通讯；

(3).它适用于单用户操作系统，或多用户操作系统，或小型计算机，或微型计算机。

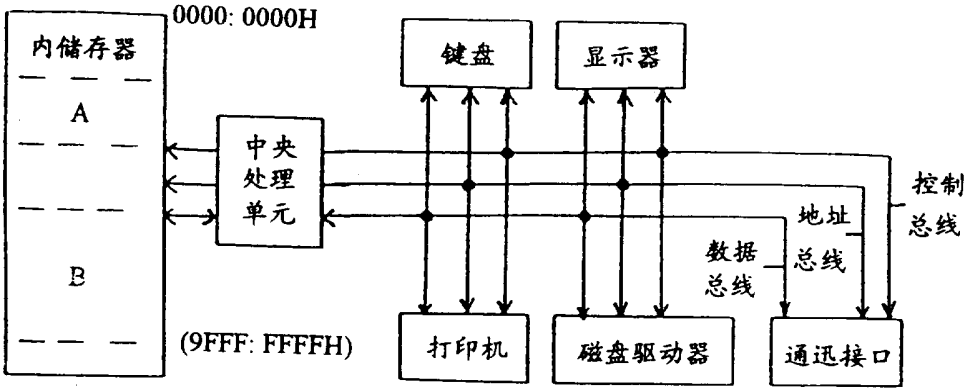

内储存器
A
B
0000: 0000H
(9FFF: FFFFH)
中央处理单元
键盘
显示器
打印机
磁盘驱动器
通迅接口
控制总线
地址总线
数据总线

Fig. 1

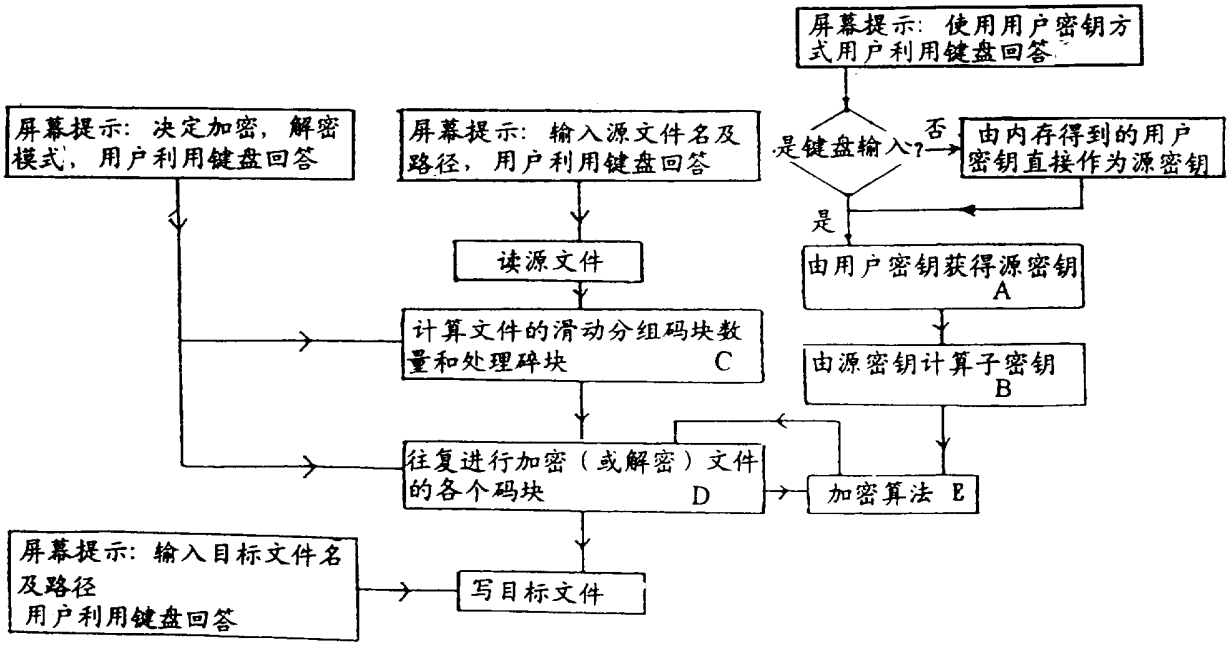

屏幕提示：使用用户密钥方式用户利用键盘回答
屏幕提示：决定加密，解密模式，用户利用键盘回答
屏幕提示：输入源文件名及路径，用户利用键盘回答
是键盘输入?
否
由内存得到的用户密钥直接作为源密钥
是
读源文件
由用户密钥获得源密钥 A
计算文件的滑动分组码块数量和处理碎块 C
由源密钥计算子密钥 B
往复进行加密（或解密）文件的各个码块 D
加密算法 E
屏幕提示：输入目标文件名及路径
用户利用键盘回答
写目标文件

Fig. 2

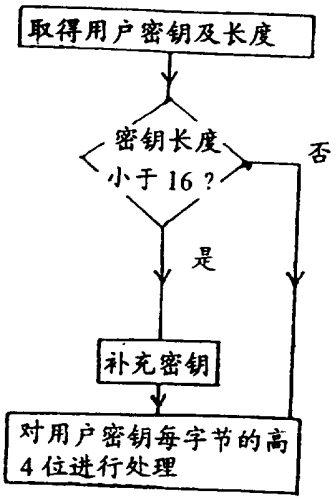


Fig. 3

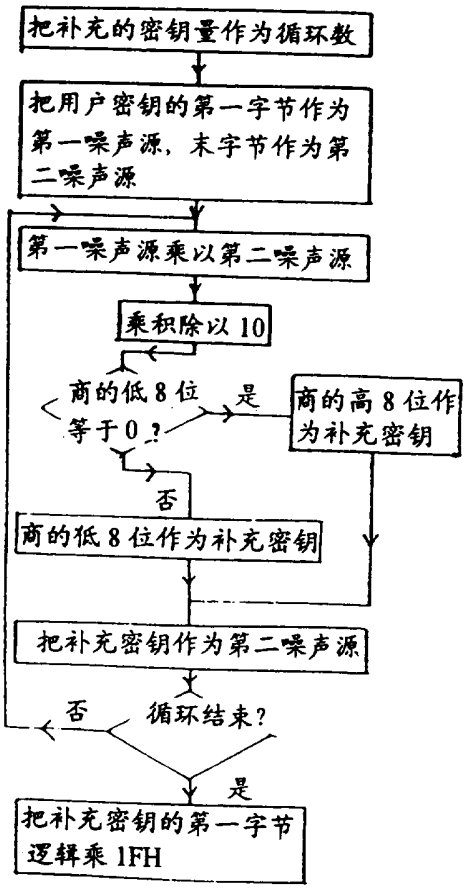


Fig. 4

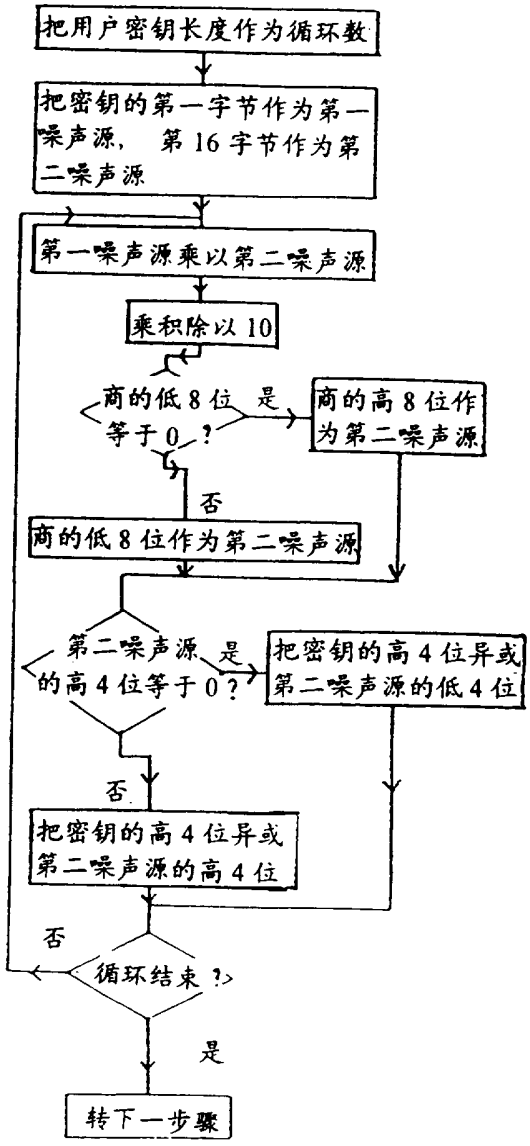


Fig. 5

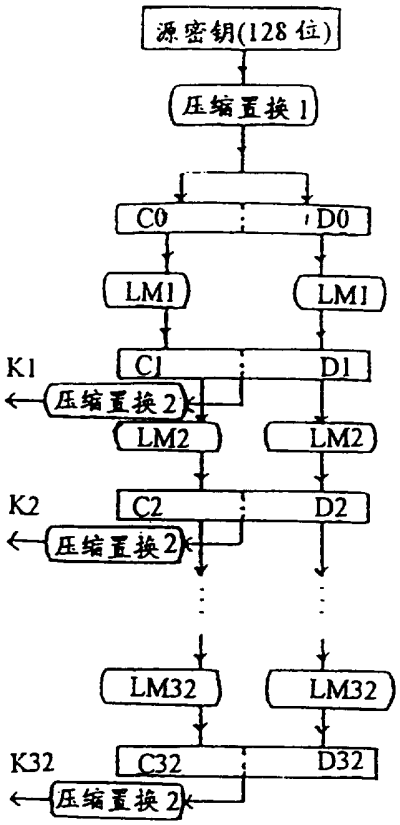


Fig. 6

第 i 次迭代	LMi (循环左移位数)	第 i 次迭代	LMi (循环左移位数)
1	1	17	1
2	1	18	1
3	2	19	2
4	2	20	2
5	2	21	2
6	2	22	2
7	2	23	2
8	2	24	2
9	1	25	1
10	2	26	2
11	2	27	2
12	2	28	2
13	2	29	2
14	2	30	2
15	2	31	2
16	1	32	1

Fig. 8

115	99	83	67	51	35	19	3
117	101	85	69	53	37	21	5
119	103	87	71	55	39	23	7
123	107	91	75	59	43	27	11
125	109	93	77	61	45	29	13
127	111	95	79	63	47	31	15
114	98	82	66	50	34	18	2
128	112	96	80	64	48	32	16
126	110	94	78	62	46	30	14
124	108	92	76	60	44	28	12
122	106	90	74	58	42	26	10
120	104	88	72	56	40	24	8
118	102	86	70	54	38	22	6
116	100	84	68	52	36	20	4

Fig. 7

14	27	31	1	6	101	93	80
4	94	43	26	67	59	15	97
23	57	36	75	50	109	39	9
49	105	69	7	32	72	86	52
102	66	28	78	112	11	38	60
91	8	87	47	81	62	17	103
54	96	16	88	34	110	84	42
73	58	85	21	99	51	2	79
45	111	46	89	56	10	74	68
55	5	106	37	70	95	48	22
13	19	77	104	24	40	90	63
30	108	33	64	20	98	41	82

Fig. 9

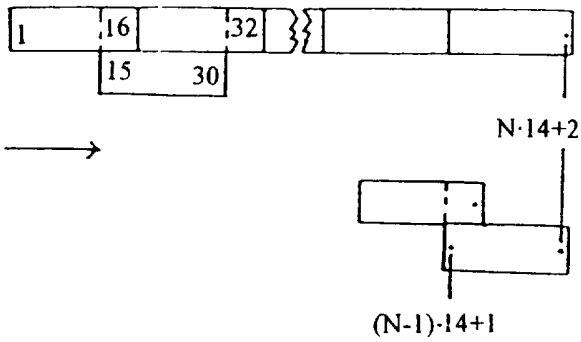


Fig. 10

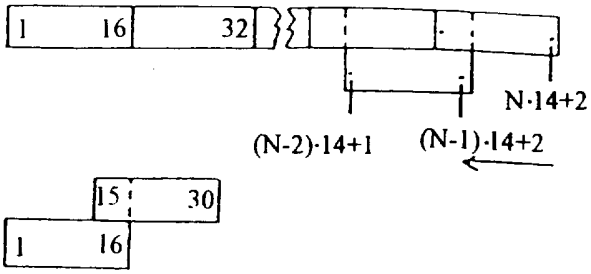


Fig. 11

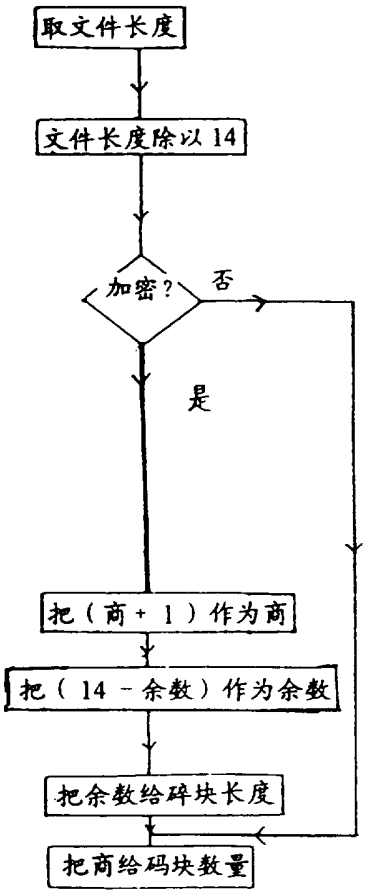


Fig. 12

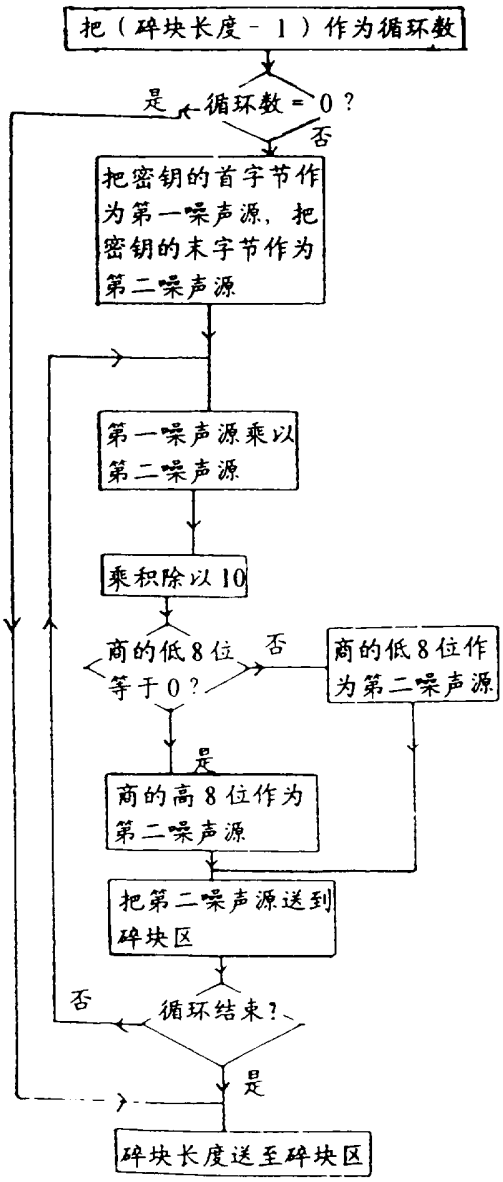


Fig. 13

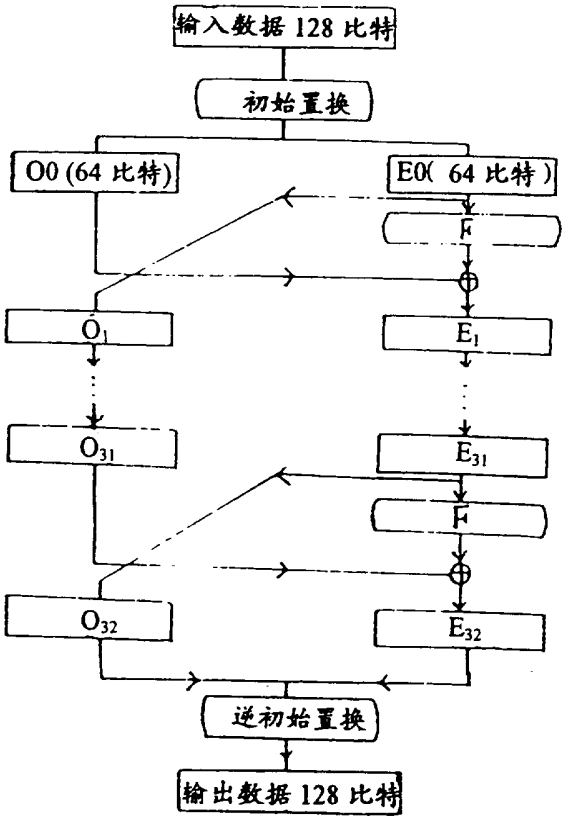


Fig. 15

122	114	106	98	90	82	74	66	58	50	42	34	26	18	10	2
124	116	108	100	92	84	76	68	60	52	44	36	28	20	12	4
126	118	110	102	94	86	78	70	62	54	46	38	30	22	14	6
128	120	112	104	96	88	80	72	64	56	48	40	32	24	16	8
121	113	105	97	89	81	73	65	57	49	41	33	25	17	9	1
123	115	107	99	91	83	75	67	59	51	43	35	27	19	11	3
125	117	109	101	93	85	77	69	61	53	45	37	29	21	13	5
127	119	111	103	95	87	79	71	63	55	47	39	31	23	15	7

Fig. 16

80	16	96	32	112	48	128	64	79	15	95	31	111	47	127	63
78	14	94	30	110	46	126	62	77	13	93	29	109	45	125	61
76	12	92	28	108	44	124	60	75	11	91	27	107	43	123	59
74	10	90	26	106	42	122	58	73	9	89	25	105	41	121	57
72	8	88	24	104	40	120	56	71	7	87	23	103	39	119	55
70	6	86	22	102	38	118	54	69	5	85	21	101	37	117	53
68	4	84	20	100	36	116	52	67	3	83	19	99	35	115	51
66	2	82	18	98	34	114	50	65	1	81	17	97	33	113	49

Fig. 17

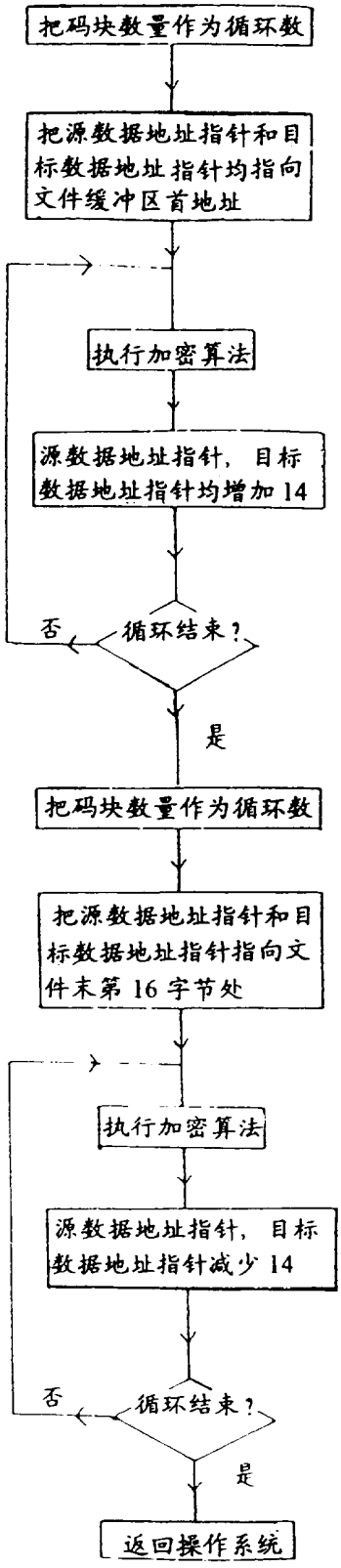


Fig. 14

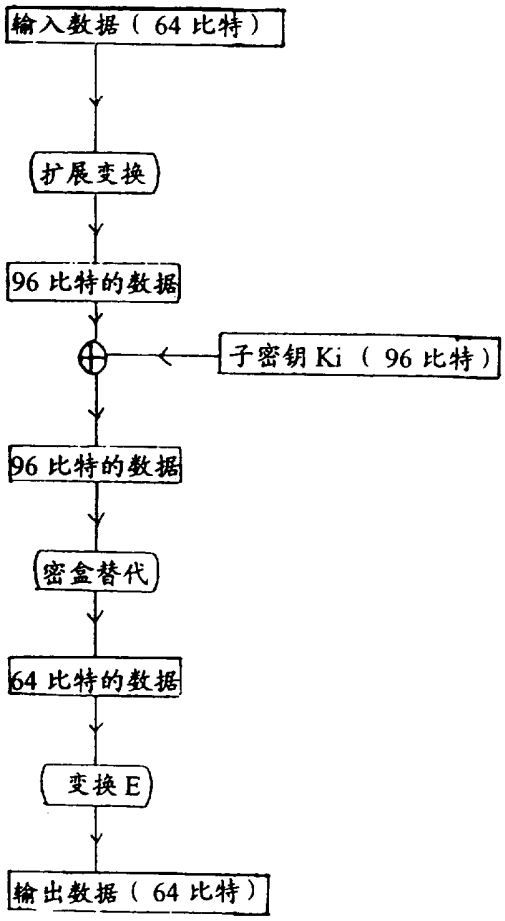


Fig. 18

64	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	33
32	33	34	35	36	37	36	37
38	39	40	41	40	41	42	43
44	45	44	45	46	47	48	49
48	49	50	51	52	53	52	53
54	55	56	57	56	57	58	59
60	61	60	61	62	63	64	1

Fig. 19

		列															
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S0	行0	15	1	5	6	10	9	4	12	8	11	2	7	3	0	13	14
	1	6	5	15	10	9	4	1	2	0	7	13	12	11	14	8	3
	号2	8	6	14	1	3	7	9	0	12	10	5	4	2	11	15	13
	3	1	2	0	8	11	5	10	13	9	14	6	15	4	7	3	12
S1		10	2	7	8	4	6	15	5	9	0	1	13	14	12	3	11
		15	6	2	9	12	3	0	8	7	5	11	10	4	13	14	1
		9	0	15	4	2	10	1	3	13	11	6	5	7	14	8	12
		0	14	6	7	15	13	9	10	8	1	3	4	11	2	12	5
S2		14	10	8	7	3	5	2	6	15	9	0	4	12	11	1	13
		7	4	1	8	15	0	5	10	3	6	12	11	9	2	13	14
		1	7	6	12	5	9	11	8	10	2	14	3	4	13	0	15
		10	15	2	0	12	14	1	11	7	8	13	6	5	4	9	3
S3		13	0	10	5	9	8	14	3	11	1	15	12	6	7	2	4
		8	7	0	1	11	15	4	9	5	13	10	14	3	12	6	2
		2	1	5	3	4	11	12	7	15	9	13	10	8	0	14	6
		11	5	4	2	3	12	0	14	6	15	8	13	10	9	7	1
S4		7	9	6	4	2	13	5	11	12	10	14	1	15	3	0	8
		3	2	5	7	14	1	8	0	6	4	15	9	13	10	11	12
		10	15	4	2	7	12	0	5	14	8	9	11	6	1	13	3
		9	6	15	5	13	10	4	1	3	11	7	14	2	12	8	0
S5		3	11	9	2	8	12	13	4	7	5	10	6	1	15	14	0
		9	8	6	3	10	14	7	1	4	2	0	15	12	11	5	13
		11	14	7	0	1	13	10	2	5	6	1	9	15	4	3	8
		8	7	14	4	0	11	3	15	12	10	5	2	6	1	13	9
S6		8	4	15	9	5	10	3	1	2	12	13	0	11	14	7	6
		5	14	9	12	8	11	6	13	1	10	4	7	2	0	3	15
		14	10	3	13	12	8	5	6	11	4	7	15	9	2	1	0
		4	3	10	15	1	9	11	12	5	2	14	8	13	6	0	7
S7		4	3	2	10	12	15	6	9	1	8	7	14	0	13	11	5
		14	12	8	11	1	13	9	3	10	0	6	5	7	15	2	4
		0	9	13	6	11	14	8	15	4	3	1	7	12	10	5	2
		3	13	1	9	6	0	7	8	2	12	10	11	14	5	4	15

		列号															
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S8	行0	6	5	14	0	15	11	8	7	10	13	12	2	4	1	9	3
	1	0	11	7	6	3	5	14	12	15	9	2	13	1	4	10	8
	号2	13	2	1	5	6	15	3	14	9	7	10	8	0	12	4	11
	3	2	4	3	1	10	7	12	5	13	0	11	9	15	8	6	14
S9		0	13	12	11	6	7	1	8	14	3	9	15	2	5	4	10
		11	3	14	5	2	12	10	4	13	1	8	6	15	9	0	7
		5	8	0	14	10	6	15	9	3	12	2	1	13	7	11	4
		13	0	11	10	14	4	8	2	1	9	12	7	3	15	5	6
S10		2	8	4	12	7	14	0	13	5	15	11	3	9	6	10	1
		1	10	3	4	13	6	11	15	12	8	9	2	14	5	7	0
		12	5	9	11	8	0	2	4	1	14	15	13	10	3	6	7
		7	9	12	3	5	15	13	0	10	6	4	1	8	14	2	11
S11		5	12	11	3	14	1	7	0	13	2	8	9	10	4	6	15
		10	9	4	15	0	2	13	14	8	3	5	1	6	7	12	11
		3	13	8	10	9	5	4	1	2	15	0	12	11	6	7	14
		12	8	13	11	2	6	5	9	4	7	15	0	1	3	14	10
S12		12	15	0	1	11	4	9	2	3	14	6	5	13	10	8	7
		4	13	10	0	7	9	12	6	2	11	14	3	8	1	15	5
		7	3	12	15	13	1	6	11	8	0	4	2	14	5	9	10
		15	1	9	6	4	8	14	3	11	5	2	12	7	0	10	13
S13		9	6	1	15	13	2	10	14	0	4	3	11	7	8	5	12
		2	0	11	13	6	10	15	7	14	12	1	8	5	3	4	9
		15	11	2	7	0	4	13	10	6	1	8	14	3	9	12	5
		5	12	8	14	7	3	6	4	15	13	0	10	9	11	1	2
S14		1	7	13	14	0	3	11	15	4	6	5	10	8	2	12	9
		13	15	12	2	5	8	3	11	9	14	7	4	0	6	1	10
		6	4	11	9	15	2	14	12	7	13	3	0	5	8	10	1
		14	11	7	13	8	1	2	6	0	3	9	5	12	10	15	4
S15		11	14	3	13	1	0	12	10	6	7	4	8	5	9	15	2
		12	1	13	14	4	7	2	5	11	15	3	0	10	8	9	6
		4	12	10	8	14	3	7	13	0	5	11	6	1	15	2	9
		6	10	5	12	9	2	15	7	14	4	1	3	0	13	11	8

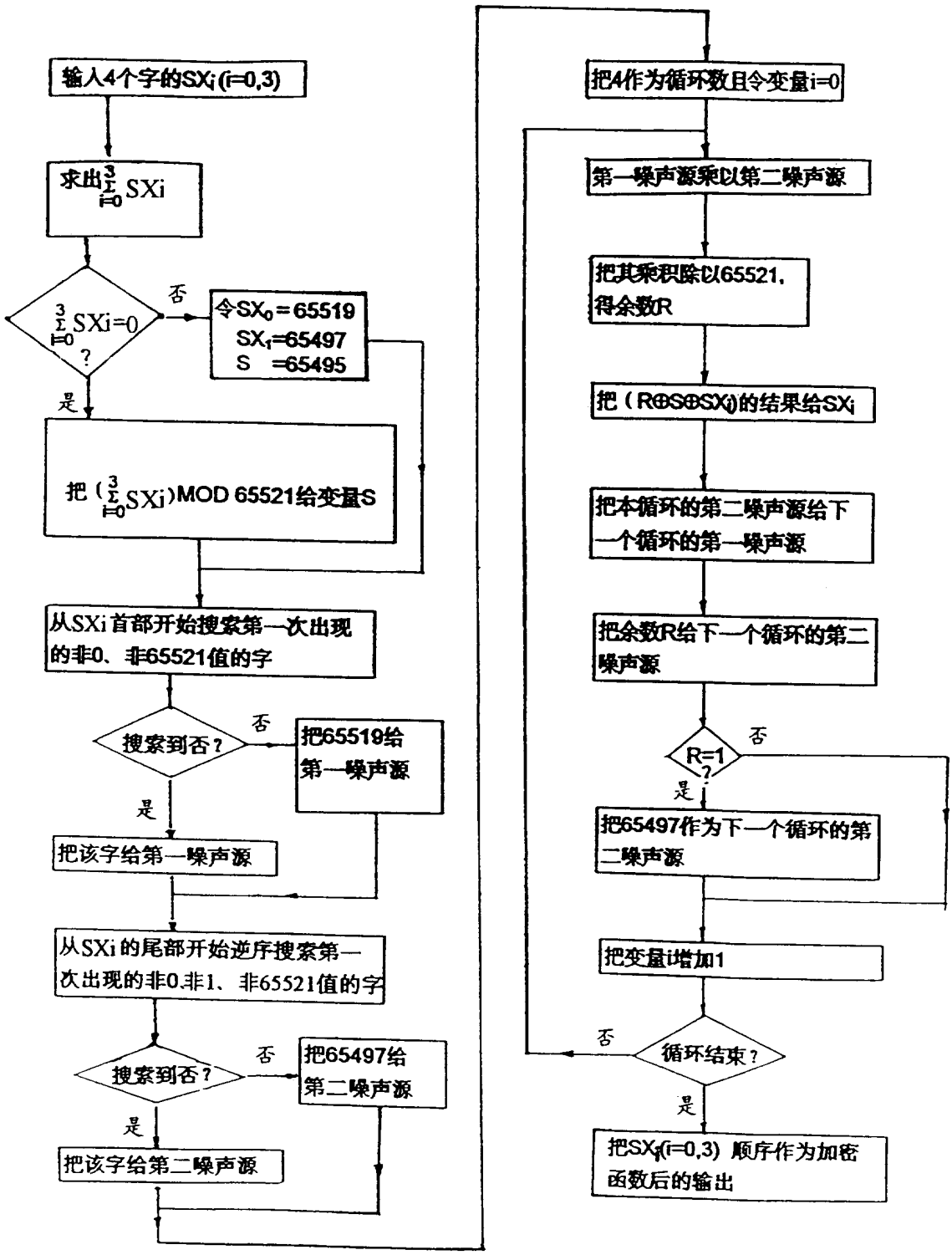


Fig. 22

替换页(细则第26条)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN 95/00077

A. CLASSIFICATION OF SUBJECT MATTER

IPC[6] H04L 9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED H04L G06F

Minimum documentation searched (classification system followed by classification symbols)

H04L 9/00, 9/06, 9/18, 9/20, 9/28, G06F12/00, 12/14, 1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

cryptography, encryption, encipher, block, chain, permutation, substitution, key

C. DOCUMENTENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US,A,5132848(International Business Machines, Armonk, N. Y.)11. Jul. 1995	1-4
A	EP, A2, 0421754 (TELEDYNE INDUSTRIES, INC. 19601 Nordhoff Street Northridge, California 91324(US))04. Oct. 1991	1 1
A	US,A,5103479(Hitachi Ltd. ; Hitachi Control System, Inc. JP)07. Apr. 1992	1 1
A	US, A, 5231662 (Tulip Computers International B. V., Netherlands) 27. Jul. 1993 See all whole clocumeuts	1-4

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claims(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
6. Jun. 1996 (06.06.96)	04 JUL 1996 (04.07.96)
Name and mailing address of the ISA/ Chinese Patent Office, 6 Xitucheng Rd. Jimen Bridge, Haidian District, 100088 Beijing, China Facsimile No. (86-1)2019451	Authorized officer Zhong Qiang Telephone No. (86-10)62093837

Form PCT/ISA/210(second sheet)(July 1992)

国际检索报告

国际申请号
PCT/CN 95/00077

A. **主题的分类** IPC⁶ H04L 9/00

按照国际专利分类表（IPC）或者同时按照国家分类和IPC两种分类

B. **检索领域** H04L G06F

检索的最低限度文献（标明分类体系和分类号）
H04L 9/00, 9/06, 9/18, 9/20, 9/28, G06F 12/00, 12/14, 1/00

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库（数据库的名称和，如果实际可行的，使用的检索词）
cryptography, encryption, encipher, block, chain, permutation, substitution, key

C. **相关文件**

类 型 *	引用文件，必要时，包括相关段落的说明	相关的权利要求编号
A	US, A, 5432848 (International Business Machines, Armonk, N. Y.) 11. 7月. 1995	1--4
A	EP, A2, 0421754 (TELEDYNE INDUSTRIES, INC. 19601 Nordhoff Street Northridge, California 91324 (US)) 04. 10月. 1991	1---4
A	US, A, 5103479 (Hitachi Ltd.; hitachi Control system, Inc. JP) 07. 4月. 1992	1—4
A	US, A, 5231662 (Tulip Computers International B. V. Netherlands) 27. 7月. 1993 看所有文献全文	1—4

☐ 其余文件在C栏的续页中列出。　　☐ 见同族专利附件。

* 引用文件的专用类型：
"A" 明确表示了一般现有技术、不认为是特别相关的文件
"E" 在先文件，但是在国际申请日的同一日或之后公布的
"L" 对优先权要求可能产生怀疑或者用来确定另一篇引用文件的公布日期或其它特殊理由而引用的文件（如详细说明）
"O" 涉及口头公开、使用、展览或其它手段的文件
"P" 在国际申请日之前但迟于所要求的优先权日公布的文件
"T" 在国际申请日或优先权日之后公布的在后文件，它与申请不相抵触，但是引用它是为了理解构成发明基础的理论或原理
"X" 特别相关的文件；当该文件被单独使用时，要求保护的发明不能认为是新颖的或不能认为具有创造性
"Y" 特别相关的文件；当该文件与其它一篇或多篇该类文件结合在一起，这种结合对本领域技术人员是显而易见的，要求保护的发明不能认为具有创造性
"&" 同族专利成员的文件

国际检索实际完成的日期	国际检索报告邮寄日期
06.6月.1996 (06.06.96)	04·7月1996 (04.07.96)
中国专利局 100028 中国北京市海淀区蓟门桥西土城路6号 传真号：(86—1) 2019451	受权官员 钟强 电话号码：(86-10) 62093837