天津市科协专著基金
TAST Fund For Academic Publications

魏仲山 编著

金卡安全技术

天津大学出版社

前　言

金卡是指全民信用卡。1993 年 6 月江泽民主席指出："要用 10 年左右的时间，在 3 亿人口中推广信用卡、现金卡，实现支付手段的革命性变化，跨入电子货币时代。"现在我们面临的任务是，能在 21 世纪初的中国让 3 亿人民应当持有安全、通用、简便和经济的全民信用卡。当前在我国市场上牡丹卡、长城卡、金穗卡、维萨(VISA)和万事达(MASTER)卡、太平洋卡等多卡并存，互不通用。在我国经济由粗放型向集约型过渡之际，为实现各卡通用，就要采取"跨(银)行"交易方法。跨行交易是指受理的金融终端并不属发卡行管辖，此时，通信网络一般为公用网络。显然，跨行比本行范围内作交易的技术问题更为复杂，安全风险也更大。

金卡安全是信用卡应用的永恒主题。金卡安全涉及到持卡人(卡主)、信用卡本身、作受理的金融终端(自动柜员机或销售点终端)、通信网络和发卡银行内部诸多环节的安全问题。从统计资料可以看出，由于磁卡具有易于涂改和仿制的固有弊端，1991 年仅亚太地区损失就达 1.25 亿美元，其中伪卡作案占信用卡犯罪案例总数的 70%。另一方面，无论在国外或国内，凡大案要案多出自内部、知情人或内外勾结，这些都是安全上脆弱点所在，必须在管理、技术上采取防范对策和措施。

实际使用时，信用卡授权取决于 PIN(个人标识号)，本质上它为卡主的电子签名。为保证卡主的真实性，PIN 需要绝对保密。金卡系统除非确认卡主提供的 PIN，能与信用卡上客户帐号相符，否则拒绝作这笔电子转帐交易。PIN 和信用卡相分离的作用在于，一旦信用卡丢失或被窃，拾者或窃贼无法利用它，因为他不知与该卡相应的 PIN。但是，信用卡为磁卡，就易于读出卡上信息或仿制成

伪卡。利用大批伪卡于受理终端，案犯是能设法猜出PIN的。一旦猜出，伪卡作案就会得逞。所以，使用磁卡和PIN就有伪卡泛滥的隐患存在。对此，为验证卡主真实身份，可采取在受理终端设置鉴定卡主出示的指纹，或视网膜脉管图像的扫描设备，以取代鉴定PIN，从而制止伪卡作案。另外尚有辨认卡主人体特征的其它办法可供参用。但是，凡是这类方法旨在判别卡主身份的真伪，是针对防范伪卡作案的"单打一"安全措施。除验证卡主身份外，也可以从信用卡自身作改进，用智能(IC)卡取代磁卡。IC卡较磁卡的一大优点是，卡内信息密封而难伪造，这从根本上杜绝伪卡出笼。不仅如此，IC卡还能提高金卡系统其它环节的安全度，尤其是制止伪受理终端作案。IC卡还具备一卡多用的前景。由此可见，IC卡具有一举多得的综合保护机制和经济效果。在21世纪来临之际，IC卡取代磁卡而作为金卡的主体势在必行。

一般来说，一个信息系统的安全度，体现为反泄密、反窜改和反破坏的能力。除信息存储和处理过程外，信息在传输过程中受到的安全威胁最大。安全威胁手段大体上可分为被动攻击和主动攻击两类。被动攻击旨在破坏信息机密性，主动攻击旨在破坏信息真实性和完整性。就机密密集型而言，以军用计算机为代表的国家安全领域用于封闭环境。对此，为保密而把致泄密的被动攻击作为主要对象置于首位。它也是以保密为主导原则的传统安全模式。与此不同，就财富密集型而言，以金融系统为代表的商用安全领域用于开放环境。此时对客户是开放的，所使用公用网络是开放的，这种环境下机密并不能全保得住。为保证金融信息真实性与完整性把致假冒或窜改的主动攻击置于首位。防主动攻击比防被动攻击更难，后者不易发觉但易制止，前者虽能发觉但难制止。后者靠加密技术和方法能够奏效，前者的威胁则来自机、网、库、卡诸多层次，这主要靠鉴定技术和方法，以及多层次综合保护机制和措施。

为金卡安全所用的各种鉴定技术和方法，是以密码算法为基

础的。同样采用磁卡(或IC卡)的金卡系统,因为鉴定技术和方法不同而有不同安全度。尤其因为密码算法不同而安全度有明显差异。由此可见,密码算法不仅是鉴定技术和方法的依据,也是影响整个金卡系统安全度的主要因素。

迄今为止,世界上现行的有单钥和双钥制两种密码。单钥制(或对称制)以美国IBM首创的DES(数据加密标准)为代表。在DES中加密和解密使用同一密钥为加密和解密数据,DES采用同一非线性积函数(或称组合函数)。该算法本身为公开的但有强加密度,其基本点是密钥需要绝对保密。由于在使用中需要传输密钥,所以密钥管理复杂。双钥制(或非对称制)以美国MIT三个创始人命名的RSA为代表。它在加密时使用公开的公钥,解密时使用保密的私钥。双钥制也称为公钥制。在使用中并不需要传输密钥,这不仅使密钥管理大为简化,也因此提高了安全度。RSA算法为加密和解密数据用一对非素数模互逆离散幂函数。算法本身是公开的,而算法安全度则靠大数因子分解难来保证。RSA会比DES有更高安全度。RSA公钥数签是利用报文发送端所保密的私钥,对所签发报文作数字签名。因不知私钥,报文接收端只能用相应公钥核实签发报文,则不存在窜改冒充而构成伪报文的任何可能性。RSA公钥数签既安全又简便,是取代商业纸面契约和票据的重大创举。只有IC卡具备使用公钥数签的条件,而磁卡就不具备使用条件。RSA-IC卡比DES-IC卡具有更高安全度。但是,RSA比DES的运算速度慢,所以研制开发高速RSA芯片成为当务之急。

本书共分10章。前4章为技术基础:第1和2章讨论DES及其应用;第3章讨论单钥制密钥管理;第4章介绍公钥密码基础知识,以及RSA密码。后6章为技术应用:在第5和6章讨论了PIN管理和安全威胁,金卡安全技术归结为身份鉴定方法和报文鉴定方法;第7章讨论前者而第8章讨论后者;第9章提出金卡安全的

18项技术指标；第10章讨论实际应用，以跨行交易为起点，分析研究了磁卡、IC卡共6个技术方案，并作比较。正如统计所示，在国内外凡大案要案多出自内部、知情人或内外勾结，为此又讨论了金卡安全审计的一些问题。

本书由天津市科协自然科学学术专著基金资助出版。天津市科协给予了大力支持和鼓励，在此表示感谢。由于作者水平所限，望读者批评指正。

作者

1996年10月

目　录

上篇　技术基础

下篇　技术应用

上 篇 技术基础

第一章 数据加密标准(DES)

相传早在我国春秋战国时期(约公元前473年),吴越交战中,城池久攻不下,后因城防图失窃而战败灭国。这里说的"城防图失窃"也就是"信息遭泄密"。可见保密会涉及到战争胜败和国家存亡,有何等重要,千百年来这种观念世代相传。为达到保密目的而采用的加密手段一直视为一种高深莫测的神秘技巧。

本世纪40年代电子计算机问世。60年代计算机技术迅猛发展,大量重要的数据汇集于计算机数据库,并在通信网络内传输。在这种场合下,存储于计算机的数据遭窃取、窜改和复制屡有发生。计算机网络的实体防护最为薄弱,数据在传输过程中受到安全威胁尤为突出。因此,撇开存储数据的载体和通信渠道,利用加密方法直接对数据加密,成为当今公认的最为奏效的保密手段。

第一节 必要性和可行性

在工程应用上,为何需要有一种数据加密标准?这是因为在使用中应为各家厂商制造的加密系统提供兼容性。对使用保密通信的用户,只需购置一对加密解密设备安装于通信线路两端,并置入相应密钥就行,谈不上需要一个加密标准。颁布一个公认的标准,反而不利于保密自身。当通信范围只涉及到有统一管辖权的企事业组织,用加密方法保护所通信传输的数据,不会出现什么麻烦。

即使在组织管理上有一些麻烦，也易于在具体实现中作协调而取得一致。迄今为止，一个企事业组织内部作保密通信，多在租用线路的专用通信网络上实施。在这种场合下，无必要有数据加密标准。

在不同企事业组织间作保密通信，并非轻而易举。因为各企事业所选用加密解密设备来自不同制造厂家而有所不同。各种密码设备的这种不兼容性，不但无法作保密通信，也影响作其它通信。本世纪 80 年代以后，国际间商贸往来和繁荣促使计算机通信互联网络出现。国际标准化组织(ISO)为开放系统互连(OSI)颁布了七层通信网络协议，这是异种机间通信协议。然而，通信协议各层和加密之间的关系，又为加密实施带来新的限制。1989 年，ISO 颁布了 ISO OSI 网络安全体系结构。为了实现各种设备间兼容和网络保密通信，有必要制订一个工程上广为应用的数据加密标准。

有一个公认的标准，则公开的知识就不可避免。显然，这与保密的传统观念背道而驰。多少年来人们力图把加密方法的具体实现作为机密。然而，在数据加密标准算法本身必然公开的基础上，它的基本要求是：

①它必须使所加密的数据具有高保密度。

②它必须有完整说明，资料易于理解。

③该算法的安全并非建立于算法本身的保密。因为算法是公开的。

④它必须能为所有制造商和用户使用。

⑤它必须适应各种应用环境。

⑥在电子设施(硬件或固化成芯片)上它必须是经济的和高效的。

⑦它必须经得起持久的实际验证。

⑧它必须和国际有关标准相兼容。

根据这些基本要求，数据加密标准的算法不作保密。为保证所

加密数据的高保密度，它的基点应着眼于该算法本身的加密强度，以及对密钥的保密上。

为找到强加密算法，可追溯到本世纪第一次世界大战期间德国军队使用过的 ADFGVX 乘积密码，如图 1-1(a)所示。这种乘积

		A	D	F	G	V	X
代换字母表	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	Ø	2
	X	U	4	I	S	T	M

密钥字	D	E	U	T	S	C	H
密文读出次序	2	3	7	6	5	1	4

置换表	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

(a)

明　　文　M:PRODUCTCIPHERS

中间密文　c:fgagvdvfxadgxvdgxffgvggaagxg

密 钥 字　k:DEUTSCH(2376514)

密　　文　C:DXGXFFDGGXGGVVVGVGFGGDFAAAXA

(b)

图 1-1　ADFGVX　乘积密码

密码是由代换和置换(即移位)两种类型构成的组合密码。代换密码由 6×6 阶矩阵所表述的字母表实现。明文为 A,…,Z,26 个字母和∅,1,2,3,4,5,6,7,8,9,十个数字共 36 个字符随机插入该矩阵内。密文共为 6 个字母(即 ADFGVX)分别作为矩阵的行和列。一个明文字符对应于矩阵的行和列相应位置上的二个密文字母。

例如，明文 P 在矩阵内为 F 行 G 列上，所以经字母表代换后为 fg。加密第一步是利用代换字母表把明文变换成中间密文。加密第二步把中间密文经置换读出。读出次序取决于密钥字给定的字母次序。因为密文字母总共才 6 个，在置换过程中倒来倒去，很难找出字母频度分布规律而破译。图 1-1(b)为一个实际例子。明文 PRODUCTCIPHERS，第一步用代换字母表生成中间密文，第二步用任选的密钥字，此处取用 DEUTSCH(这个德文字的含义“德语”，它的字母次序为 C 为 1，D 为 2，E 为 3，以此类推，构成中间密文读出次序为 2376514。密钥字为保密的，利用它表征读出次序就便于记忆而不必写下来)表示读出次序，把中间密文变换成密文。在图 1-1(a)内以密钥字数分组按行生成中间密文的置换表，再利用密钥字次序按列读出即生成密文。在使用中每次加密可选用不同密钥字以达到不易破译的目的。

第二次世界大战期间对密码学的研究证明，交替使用代换和置换所生成乘积密码有很强加密度。ADFGVX 密码的创新在于首先使用乘积密码，不足之处是只使用一次代换和置换交替。另外，代换字母表并不随密钥变化而更动。

本世纪 60 年代后，大规模集成电路技术飞速发展，在单个芯片上实现高复杂度密码算法已成现实，这是多少年来手工算法所无法实现的梦想。1968 至 1975 年，某企业研制开发成了 Lucifer 系统使用积密码。在此基础上 IBM 改进 Lucifer 后推出新密码算法，它是 16 轮密钥控制下交替运算的积密码。它的特点是实现高复杂度的非线性变换，具有很强的加密度。

在数据加密技术发展史上，IBM 加密算法成为一个重要里程碑。70 年代后，无论政府机构还是工商业界都迫切需要数据保密。1977 年美国国家标准局(NBS)正式批准此加密算法为美国数据加密标准(DES)。1980 年美国国家标准协会(ANSI)正式采纳它为美国商用加密算法。

本世纪 80 年代以后，开放系统互连直至国际通信网络，对传输数据的加密保护要求越来越迫切。1980 年经英国建议，国际标准化组织信息处理系统技术委员会(ISO/TC 97)着手数据加密标准国际化工作。1984 年成立数据加密技术分技术委员会(ISO/TC 97/SC 20)。1985 年形成“数据加密算法 DEA-1”和“64 比特块密码算法运算方式”两个国际标准草案。事实上，前者除了没有规定密钥块 8,16,32,40,48,56,64 比特的作用外，其余和美国 DES 相同。

1986 年 ISO/TC 97 决定放弃数据加密标准国际化的工作，并宣布以后不再制定数据加密国际标准，代之以对加密算法作登记。提出开放系统互连安全体系结构(1989 年正式颁布文件 ISO 7498/2,1991 年 CCITT 相应颁布 X.800)。随着互连通信网络开放性大趋势，虽然不会再出现数据加密国际标准，但是美国 DES 仍值得作为数据加密标准的典型，迄今为止，已得到最广泛的应用。

第二节　DES 原理和逻辑结构

Shannon 指出，两个简单却不可互换的运算求积所得的函数，即混合函数会有强加密度。根据 Shannon 提出的原则，把各种不同类型函数组合以获取混合变换。混合变换是把有含义的明文信息随机且均匀分布到全部可能出现的密文信息集合上。譬如，移位后接着交替作一串代换和简单线性运算，可构成混合变换。Lucifer 密码就是依照了这种混合变换的思路。

为弄清用混合变换实现积密码的原理，假设数据块为 12 比特，如图 1-2 所示。实际使用的加密数据块会比 12 比特位要多。此密码交替使用代换 S_i 和置换 P_i，以积函数形式表述为：

$$C=Ek(M)=S_t \cdot P_{t-1} \cdot \cdots \cdot S_2 \cdot P_1 \cdot S_1(M)$$

式中 M 为明文数据块;C 为密文数据块。每次 S_i 均为密钥 k 的函数。代换 S_i 分解为若干子代换 $S_{i1},\cdots,S_{i4}$ 以便于实现成为各子块。置换 P_i 把各子块(S 盒)上比特位全部搅乱。代换和置换过程交替进行。可以设想,在密钥控制下,每一比特位明文 m 随机散射成密文各位 c。这样的混合变换应具有非线性变换的特性,所以,Lucifer 密码也可看成 t 个密码函数的混合,即:

$$C=f_1 \cdot f_2 \cdot \cdots \cdot f_t$$

式中下标量为奇或偶数,分别代表交替代换或置换密码函数。混合函数的强加密度在于它的非线性变换,但它仍具有为密码所必备的双射函数(即一对一映射)的性质。

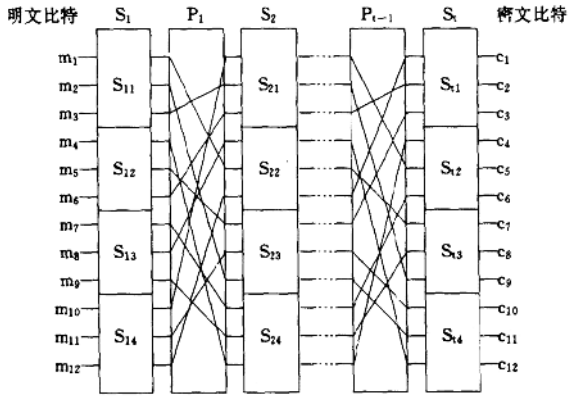

图 1-2 积密码原理

DES 原理以 Lucifer 密码为基础,它的逻辑结构如图 1-3 所示。此图用于块加密,明文和密文块均为 64 比特。它具备加密解密的两种运算功能。在加密运算过程中,密钥块控制下输入明文块

求得密文块输出。在解密运算过程中，利用同一密钥块，输入的是密文块，输出求得明文块。在此两种运算过程中，密钥块均为64比特输入。其实密钥块本身为56比特，其中每7比特附有1比特奇校验位，或称密钥块输入为8字节，每一字节(8比特)内含有一校验位。

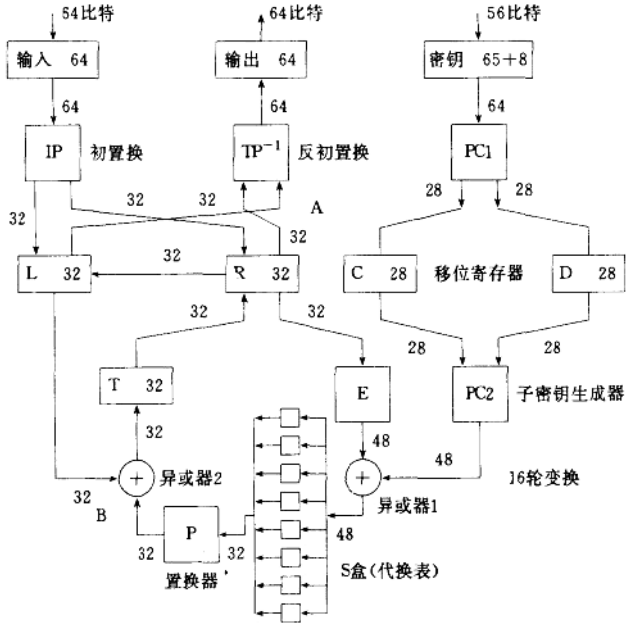

图 1-3 DES 逻辑结构

DES各逻辑部件系置换、代换和异或运算的组合。置换类型各有不同，为以后相应部件所采用。图1-4(a)所示为直接置换，各

比特位只作简单排序移位(无数据扩充)的类型。图 1-4(b)所示为扩充置换,系重复使用输入一些比特位,并把输出场重新排序(有数据扩充)。图 1-4(c)中对置换作选择,删除一些输入比特位,留下各位重新排序(有数据压缩)。

DES 代换运算由 8 个 S 盒实现。每个盒置有不同的代换表(输入为 6 比特,输出为 4 比特)。所以,全部 S 盒输入为 8×6 位,输出为 8×4 位(有数据压缩)。这与 Lucifer 的各 S 盒每个输入输出均为 4 位不同。

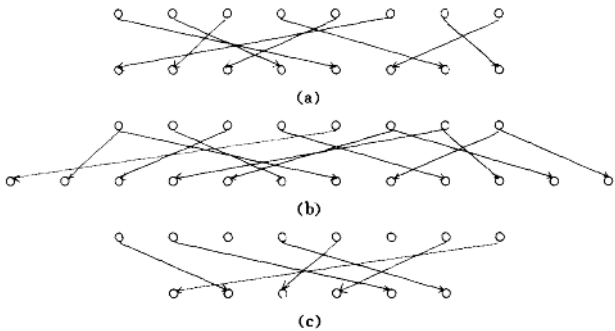

图 1-4　置换类型

DES 加密运算始于数据初始置换(IP),这很有规律性,可看成只是为接纳数据。每次把 8 比特位分别置入 8 个移位寄存器。每次每个寄存器接纳一位,共分 8 次接纳完毕。64 位一旦输入结束,各移位寄存器内数据位有序。初始置换各位如图 1-5 所示。例如,经初始置换后,原明文位 1 现为位 40,明文位为 2 者现为 8。换言之,初始置换后位 1 相应于明文位 58,位 2 相应于明文位 50,以此类推。此置换生成结果似为信息交换所采用的美国标准代码

ASCII，每个字节之尾（第 8 位）表示校验位。在 DES 置换代换运算之前，输入明文块的全部 8 个字节的 8 个校验位。8 个校验位放在一起，并置于数据块一个字节上。尚无论据表明，一开始这种规律性置于加密运算过程会削弱 DES 加密度。这是因为 DES 整个加密运算过程数据发散性很强，所以不致对加密度有影响。由此可见，初始置换只是易于实现，而对加密却无价值。

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

图 1-5　DES 初始置换（IP）

明文块输入初始置换而未作置换代换的加密运算过程之前，此明文块仍可在整个加密运算结尾的输出寄存器读出并复原。此乃初始置换的逆变换（IP^{-1}），称反初（始）置换。

初始置换后，64 位数据块分成 32 位的两个场，送至寄存器 L 和 R。这为 DES 加密主循环运算之始。寄存器 R 把 32 位送至扩充置换器 E。它把其中输入的一半（16 位）重复使用，这样输出就扩充为 48 位。具体实现方法是每一个字节（8 位）中 1、4、5 和 8 位重复使用，扩充置换方法如图 1-6 所示。例如，输出位 1 相应于输入位 32，输出位 2 相应于输入位 1；同时输出位 47 也相应于输入位 32，输出位 48 相应于输入位 1。寄存器 R 内容还向寄存器 L 直接输出 32 位，这将在以后讨论。

扩充置换器 E 的 48 位输出和选定的密钥 48 位组合而作异或