GB

中国国家标准汇编

517

GB 27927~27944

（2011年制定）

中国标准出版社

中 国 国 家 标 准 汇 编

517

GB 27927～27944

（2011 年制定）

中国标准出版社　编

中国标准出版社

北　京

图书在版编目(CIP)数据

中国国家标准汇编:2011 年制定.517:
GB 27927～27944/中国标准出版社编.—北京:中国
标准出版社,2012
ISBN 978-7-5066-6984-9

Ⅰ.①中… Ⅱ.①中… Ⅲ.①国家标准-汇编-中国
-2011 Ⅳ.①T-652.1

中国版本图书馆 CIP 数据核字(2012)第 197123 号

中国标准出版社出版发行
北京市朝阳区和平里西街甲 2 号(100013)
北京市西城区三里河北街 16 号(100045)

网址 www.spc.net.cn
总编室:(010)64275323 发行中心:(010)51780235
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

开本 880×1230 1/16 印张 34.75 字数 952 千字
2012 年 9 月第一版 2012 年 9 月第一次印刷

*

定价 220.00 元

出 版 说 明

1.《中国国家标准汇编》是一部大型综合性国家标准全集。自1983年起，按国家标准顺序号以精装本、平装本两种装帧形式陆续分册汇编出版。它在一定程度上反映了我国建国以来标准化事业发展的基本情况和主要成就，是各级标准化管理机构，工矿企事业单位，农林牧副渔系统，科研、设计、教学等部门必不可少的工具书。

2.《中国国家标准汇编》收入我国每年正式发布的全部国家标准，分为“制定”卷和“修订”卷两种编辑版本。

“制定”卷收入上一年度我国发布的、新制定的国家标准，顺延前年度标准编号分成若干分册，封面和书脊上注明“20××年制定”字样及分册号，分册号一直连续。各分册中的标准是按照标准编号顺序连续排列的，如有标准顺序号缺号的，除特殊情况注明外，暂为空号。

“修订”卷收入上一年度我国发布的、被修订的国家标准，视篇幅分设若干分册，但与“制定”卷分册号无关联，仅在封面和书脊上注明“20××年修订-1，-2，-3，……”字样。“修订”卷各分册中的标准，仍按标准编号顺序排列（但不连续）；如有遗漏的，均在当年最后一分册中补齐。需提请读者注意的是，个别非顺延前年度标准编号的新制定的国家标准没有收入在“制定”卷中，而是收入在“修订”卷中。

读者配套购买《中国国家标准汇编》“制定”卷和“修订”卷则可收齐由我社出版的上一年度我国制定和修订的全部国家标准。

3. 由于读者需求的变化，自1996年起，《中国国家标准汇编》仅出版精装本。

4. 2011年我国制修订国家标准共1 989项。本分册为“2011年制定”卷第517分册，收入国家标准GB 27927～27944的最新版本。

中国标准出版社

2012年8月

目　　录

ICS 35.240.40

中华人民共和国国家标准

GB/T 27927—2011

银行业务和相关金融服务 三重数据加密算法操作模式 实施指南

Banking and related financial services—Triple DEA-Modes of operation—Implementation guidelines

(ISO/TR 19038:2005,MOD)

2011-12-30 发布　　2012-05-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

前　言

本标准修改采用 ISO/TR 19038:2005《银行业务和相关金融服务　三重数据加密算法操作模式实施指南》(英文版)。

本标准根据 ISO/TR 19038:2005 重新起草,与 ISO/TR 19038:2005 的技术性差异为:

a) 将标准中的"TDEA"按照我国习惯修改为"三重数据加密算法"(在本文中简称"3-DEA")(标准正文中部分需要区分之处保留"三重 DEA"的说法);

b) 为便于使用者理解标准正文,增加一条术语:"错误传播"(见 3.20);

c) 在 5.5 中为无编号、无标题的表编号为:表 1DEA 功能块执行时间表,以下表号顺延。

d) 在 6.6.1.1 中,将与 7.4 中 TCFB 惟一的不同之处是,反馈到移位函数的数据块是 O_i 而不是 C_i"修改为"与 6.4 中 TCFB 惟一的不同之处是,反馈到移位函数的数据块是 O_i 而不是 C_i"(勘误);

e) 为便于理解,在 B.3.2 的标题中将"stream cipher"翻译为"伪随机向量序列$\{O_i\}$"。

为便于使用,本标准还做了下列编辑性修改:

a) 将原文中的"本技术报告"改为"本标准";

b) 删除 ISO/TR 19038:2005 的前言,修改了 ISO/TR 19038:2005 的引言。

本标准的附录 A、附录 B、附录 C 为资料性附录。

本标准由中国人民银行提出。

本标准由全国金融标准化技术委员会(SAC/TC 180)归口。

本标准负责起草单位:中国金融电子化公司。

本标准参加起草单位:中国人民银行、中国工商银行、中国银行、交通银行、中国银联股份有限公司、华北计算技术研究所、北京工商大学、中国人民银行太原中心支行。

本标准主要起草人:王平娃、陆书春、李曙光、吕毅、杨颖莉、刘运、刘志军、林中、张启瑞、刘先、仲志晖、李彦智、周亦鹏、钱湘隆、李劲松、赵志兰、贾树辉、景芸、马小琼、张龙龙。

引　言

为加强 DEA(数据加密算法)的强度和延长其生命周期,推荐使用三重数据加密算法(3-DEA)运算模式。3-DEA 的操作模式大大加强了密码保护的强度,由于这些算法基于 DEA,因此,用户和厂商可以较快熟悉它们。由于 3-DEA 操作模式能向下兼容已有的 DEA 操作模式,金融机构可使用 3-DEA 延长 DEA 的安全生命周期,保护对标准 DEA 技术的投资。

每种操作模式均有其优势和特性。对特定操作模式的选择、实施和使用取决于金融机构的安全要求、风险接受度和操作要求,这些不在本标准范围之内。如果参与方使用相同操作模式和共享保密密钥,那么本标准需要给使用本文所规定的 3-DEA 操作模式的各方提供互操作的基础根据。

本标准并不替代 DEA 算法标准和 ISO/IEC 18033 中规定的 3-DEA 算法。DEA 是 3-DEA 操作模式的基础。3-DEA 使用了先进的计算技术和密码分析技术,提供了更高的安全性。3-DEA 可用硬件、软件或软硬件混合实现。

本标准提供了 ISO/IEC 10116 中规定的操作模式的实施指南。

金融机构有责任建立全面的安全流程,其中包含必要的控制措施以确保上述过程以安全的方式实施,并且应对实施过程进行审计以确认该过程符合安全流程。

银行业务和相关金融服务
三重数据加密算法操作模式
实施指南

1 范围

本标准给用户提供了为增强数据加密保护而安全有效地实施 3-DEA 操作模式的技术支持和详细资料。本处描述的 3-DEA 操作模式用于加密运算和解密运算。本标准所描述的模式是使用 ISO/IEC 18033-3 中规定的 3-DEA 运算的分组密码操作模式(在 ISO/IEC 10116 中规定)的实现。

3-DEA 操作模式可用于金融批发业务和金融零售业务的应用系统。本标准为产品的互用性和使用 3-DEA 操作模式的应用标准的开发提供了基础。本标准将和其他使用 DEA 的 ISO 标准一起使用。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

ISO/IEC 9797-1 信息技术 安全技术 用块密码算法作密码校验函数的数据完整性机制

ISO/IEC 10116 信息技术 安全技术 n 位块密码算法的操作方式

ISO/IEC 18033-3 信息技术 安全技术 加密算法 第3部分:分组运算器

3 术语和定义

下列术语和定义适用于本文件。

3.1

生日现象 birthday phenomenon

一个有 n 个成员的相对较小的小组中至少两个人可能拥有共同生日的现象。

示例:当 $n=23$,该概率超过 1/2。如果一个人从 m 个可相互替代的可能数字随机地挑出一个,在 n 个实验对象中($n<m$),至少出现一对相同值的概率由以下公式估算出:

$$p=1-E^{-n^2/2m}$$

在以上实验中,试验的期望数在被发现相同值之前大约是$(\pi m/2)^{1/2}$。其表明对于使用混合密钥的 64 比特分组加密运算,如果一个人拥有 2^{32} 明文/密文对和 2^{32} 个由随机输入产生的密文块的文本字典,那么应该认为未知密码文本块将可从该字典中搜索到(见参考文献[11])。

3.2

块;分组 block

二进制串 binary string

示例:分割成给定的长度的明文或密文,每个片断称作一个块(分组)。明文(密文)从左向右逐块加密(解密)。在本标准中,对于 TCBC、TCBC-I、TOFB 和 TOFB-I 模式,明文和密文分割成 64 比特的块,然而对于 TCFB 和 TCFB-P 模式,支持 1 位、8 位及 64 比特明文和密文块的加密和解密。

3.3

密钥组 bundle

组成一个完整 3-DEA(K)密钥的元素组。

注：密钥组可由 2 个元素($K1$,$K2$)或者 3 个元素($K1$,$K2$,$K3$)组成。

3.4

密文 ciphertext

加密过的数据。

3.5

时钟周期 clock cycle

本标准中使用的时间单元，定义为一个 DEA 功能块执行一次 DEA 运算的时长。

3.6

密码算法初始化 cryptographic initialization

在开始加密或者解密之前，输入初始化向量到 3-DEA 中对算法进行初始化的过程。

3.7

密钥 cryptographic key

决定从明文到密文的转换的参数，反之亦然。

注：DEA 密钥是由 56 个独立位和 8 个奇偶位组成的 64 比特参数。

3.8

密钥周期 cryptoperiod

特定密钥(或密钥集)授权使用的有效期限。

3.9

数据加密算法 data encryption algorithm;DEA

ISO/IEC 18033-3 中规定的算法。

注：术语"单一 DEA"(single DEA)指 DEA，然而 3-DEA 指本标准中规定的三重 DEA(3-DEA)。

3.10

DEA 加密运算 DEA encryption operation

DEA 使用密钥 K 加密 64 比特数据块。

3.11

DEA 解密运算 DEA decryption operation

DEA 使用密钥 K 解密 64 比特数据块。

3.12

DEA 功能块 DEA functional block

指使用特定密钥执行 DEA 加密运算或 DEA 解密运算的块。

注：本标准中，每个 DEA 功能块由 DEA_j 表示。

3.13

解密 decryption

把密文转换成明文的过程。

3.14

加密 encryption

把明文转换成密文的过程。

3.15

异或运算 exclusive-OR

等长位二进制向量的逐位模 2 加运算。

3.16

初始向量　initialization vector

通过引入附加的密码变量并使得密码设备同步而对明文块序列的密码算法的初始化引入的二进制向量，以提高数据加密的安全性。

注：向量初值无需保密。

3.17

密钥　key

见 3.7 密钥。

3.18

明文　plaintext

包含一定涵义，且无需解密即可阅读或操作的可读数据。

注：也称之为明文(cleartext)。

3.19

传播延迟　propagation delay

给 3-DEA 模式提供的明文块与形成可用的密文块之间的延迟。

3.20

错误传播　error propagation

一个明文(密文)块中的错误比特经过加密(解密)运算后，不仅导致相应密文(明文)块中出现错误，而且导致其他密文(明文)块中出现错误。

3.21

再同步　re-synchronization

由于一个或多个密文块中比特位的增加或删除，失去同步状态后的再同步。

示例：如果能侦测到比特位的增加或删除，并且能删除或增加适当数目的比特位到密文，以便由块 C_i 开始重新建立块边界，使得随后解密的明文仍正确地来自包含 r 的块 P_{i+r}，那么，我们就认为是 C_{i+r} 的再同步。

3.22

自同步　self-synchronization

自动的再同步。

示例：TCBC 模式展示了自动同步，即如果密文 C_i 发生了包括丢失一个或多个完整块的错误，但是错误不再发生，那么，C_{i+2} 和随后的密文块正确地解密到 P_{i+2} 和随后的明文块(见[11]和[12])。

3.23

同步　synchronization

指对于包括 P_1、P_2、……、P_n 的明文，如果其加密成为 C_1、C_2、……、C_n 等密文块，那么，对于任何 i，$1 \leqslant i \leqslant n$，$P_1$、$P_2$、……、$P_i$ 能正确地从 C_1、C_2、……、C_i 解密得出。

注：如果密文转换中出现错误，或者，密文增加或丢失了某些比特位，那么，同步丢失。

4　符号和缩略语

C_i	第 i 个密文块，由 k 比特组成，$k=1$、8 或 64。
$C^{(j)}$	TCBC-I 模式中的第 j 个密文子串。
$C_{j,i}$	第 j 个密文子串中的第 i 个密文块。
CBC	密码分组链接(Cipher block chaining)。
CFB	密码反馈(Cipher feed back)。
D_{K_j}	使用密钥 K_j 的 DEA 解密运算。

DEA　ISO/IEC 18033-3 中规定的数据加密算法(data encryption algorithm)。

DEA_j　第 j 个 DEA 功能块。

E_{K_j}　使用密钥 K_j 的 DEA 加密运算。

ECB　电子密码本(Electronic codebook)。

I_i　加密运算第 i 个输入块,包括 TCFB、TCFB-P、TOFB 和 TOFB-I 操作模式中的 64 比特。

i　块索引。

IV　初始向量(Initialization vector)。

j　TCBC-I 中的功能块索引、密钥索引和明文子串(密文子串)索引。

h　时钟周期给定的计数数值。其用于描述每个 DEA 功能块的操作,通过采取 $t=h-1$、$t=h$ 和 $t=h+1$ 的形式。在交错或者流水模式中,h 以时钟周期 $t=3(h-1)+j$,$j=1,2,3$ 的方式,用于描述三个功能块的同时操作行为。在交错模式中,h 用作把明文划作三部分的块的索引。

k　块的长度,用作转换函数 S_k 的参数,$k=1$、8、64。

K　密钥。

n　明文中块的数量。

O_i　加密运算中第 i 个输出块,包括 TCFB、TCFB-P、TOFB 和 TOFB-I 操作模式中的 64 比特。

$\{O_i\}_k$　O_i 加最左边的 k 比特,$k=1$、8、64。当 $K=64$ 时,$\{O_i\}_k=O_i$。

OFB　输出反馈(Output feedback)。

P_i　第 i 个明文块,包括 k 位,$k=1$、8、64。

$P^{(j)}$　TCBC-1 模式中的第 j 个明文支流。

$P_{j,i}$　第 j 个明文支流中的第 i 个密文块。

S_k　"k 转换"函数,定义如下:

假设 64 比特分组 $I=(i_1,i_2,\cdots\cdots,i_{64})$ 和 k 比特块 $C=(C_1,C_2,\cdots\cdots,C_k)$,$k=1,8,64$,那么,$k$ 转换函数 $S_k(I|C)$ 产生一个 64 比特块:

$$S_k(I|C)=\{i_{k+1},i_{k+2},\cdots\cdots,i_{61},c_1,c_2,\cdots\cdots,c_k\}$$

这里 I 的比特数被向左移动 k 比特,丢弃 $i_1,i_2,\cdots\cdots,i_k$ 并且把 C 的 k 比特放在 I 的最右边 k 个位置。当 $k=64$ 时,$S_k(I|C)=C$。

t　从 1 开始的时钟周期的计数器。

TCBC　3-DEA 密码分组链接(TDEA cipher block chaining)。

TCBC-I　3-DEA 交错密码分组链接(TDEA cipher block chaining-interleaved)。

TCFB　3-DEA 密码反馈(TDEA cipher feed back)。

TCFB-P　3-DEA 密码管道式反馈(TDEA cipher feedback-pipelined)。

3-DEA　三重 DEA(Triple data encryption algorithm)。

TECB　3-DEA 电子密码本(TDEA electronic algorithm)。

TOFB　3-DEA 输出反馈(TDEA output feed back)。

TOFB-I　3-DEA 输出管道式反馈(TDEA output feedback-interleaved)。

$X\oplus Y$　X 和 Y 的异或运算。

$X||Y$　X 和 Y 的链接。

$|X|$　位串 X 的长度。

5 规范

5.1 3-DEA 加密/解密运算

本标准中，每个 3-DEA 加密/解密运算均遵守 ISO/IEC 18033-3 中的规定，为 DEA 加密和解密运算的复合运算。以下运算将适用于本标准。

a) 3-DEA 加密运算：把 64 比特分组 I(输入)转换成 64 比特分组 O(输出)，定义如下：

$O=E_{K3}(D_{K2}(E_{K1}(I)))$；

b) 3-DEA 解密运算：把 64 比特分组 I 转换成 64 比特分组 O，定义如下：

$O=E_{K1}(D_{K2}(E_{K3}(I)))$。

5.2 密钥选项

本标准在 3-DEA 密钥方面使用以下密钥选项：

a) 密钥选项 1：K1、K2 和 K3 是相互独立的密钥；

b) 密钥选项 2：K1 和 K2 是相互独立的密钥，K3＝K1；

c) 密钥选项 3：K1＝K2＝K3。

注：不推荐密钥选项 3，因为它将 3-DEA 的安全强度降低到了 DEA 的安全强度。

5.3 3-DEA 操作模式

本标准讨论了以下操作模式：

a) 3-DEA 电子密码本模式(TECB)；

b) 3-DEA 密码分组链接模式(TCBC)；

c) 3-DEA 密码分组链接模式-交错(TCBC-I)；

d) 3-DEA 密码反馈模式(TCFB)；

e) 3-DEA 密码反馈模式-管道(TCFB-P)；

f) 3-DEA 输出反馈模式(TOFB)；

g) 3-DEA 输出反馈模式-交错(TOFB-I)。

这些就是 ISO/IEC 10116 中规定的 ECB、CBC 和 CFB 操作模式的实施方式。在应用中，高效的 3-DEA 加密/解密运算很重要，或者传播延迟必须最小化，因此，本标准也提供了最新交错模式(针对 TCBC 和 TOFB)和管道模式(针对 TCFB)。

5.4 向后兼容性

在本标准中，如果在 3-DEA 操作中使用恰当的密钥选项，3-DEA 操作模式能够向后兼容到单个 DEA 的相应操作模式。

a) 使用单一 DEA 操作模式加密得到的密文能正确地通过 3-DEA 相应的操作模式加以解密；

b) 使用 3-DEA 操作模式加密得到的密文能正确地通过单一 DEA 相应的操作模式加以解密。

使用密钥选项 3 时，TECB、TCBC、TCFB 和 TOFB 模式均分别向后兼容 ECB、CBC、CFB 和 OFB 的单一 DEA 操作模式。宜注意：向后兼容到 DEA 把 3-DEA 的操作模式的安全性降低到单一 DEA 的相应操作模式的程度。

5.5 DEA 功能块执行时间表

在本标准中，一个时钟周期定义为执行 $E_K(I)$ 或 $D_K(I)$ 的 DEA 功能块的时钟周期。在 DEA 功能块执行时间表中，$O=E_{K3}(D_{K2}(E_{K1}(I)))$ 划分为三个操作。每个操作由一个功能块在一个时钟周期内完成。表 1 是在执行 $E_{K3}(D_{K2}(E_{K1}(I)))$ 时三个 DEA 功能块的执行时间次序。

表 1 DEA 功能块执行时间表

	Input	DEA_1	DEA_2	DEA_3	Output
$t=1$	I	$E_{K1}(I)$			
$t=2$			$D_{K2}(E_{K1}(I))$		
$t=3$				$E_{K3}(D_{K2}(E_{K1}(I)))$	O

5.6 提高运算效率并将传播最小化

如 5.5 所示，有效的 3-DEA 输出块 O 仅在输入块 I 之后产生，已经传播经过了三个单独的 DEA 功能块。也就是说，获得输出花费了三个时钟周期。在每个时钟周期内，只有一个 DEA 功能块在进行数据加密/解密。该配置方式具有最低的运算效率和最长的传播延迟。

为了提高运算效率并将传播最小化，可使用本标准提供的交错模式和管道模式。它们分别是 TCBC-I、TCFB-P 和 TOFB-I 模式。在交错模式中，明文序列分割成三个明文子序列。加密能同步进行。在管道模式中，通过三个时钟周期，用三个 IV 发起加密运算，以至于在发起之后，三个 DEA 功能块能并行处理数据。交错和管道配置方式用于配有多个 DEA 处理器的系统。

在交错或者管道模式中，执行时间表定义了在每个时钟周期内多个 DEA 功能块的同步操作。

5.7 密钥和初始向量

在执行 3-DEA 操作模式时应符合以下有关密钥和初始化向量的具体规定。

a) 对于所有的 3-DEA 操作模式，三个密钥(K1，K2，K3)定义了 3-DEA 密钥组。密钥组和单个密钥应：
   1) 保密；
   2) 随机产生；
   3) 从其由授权源产生、传输或者存储时起，保持完整性，以确保密钥组中的每个密钥均不能以未授权方式进行变更；
   4) 以特定操作模式中规定的适当的顺序来使用；
   5) 在 3-DEA 运算及相应的密钥管理过程中，应将整个密钥组看作一个整体，对密钥的相关操作应作用于整个密钥组的每个密钥；
   6) 密钥组不能因为任何目的而拆散。

b) IV 应符合以下特性：
   1) 对于 TECB，不使用 IV；
   2) 对于使用 IV 的所有模式，IV 可为公共信息；
   3) 在给定密钥组的密钥周期内，只要重新发起加密过程，就应产生一个或者三个新的 IV。

c) IV 应通过以下方式之一产生，按照如下优先级顺序采用：
   1) 随机产生；
   2) 由单调递增计数器产生，以便该数值将在密钥的密钥周期内不会重复。

d) 需要三个 IV 时，通过 c)项的方式 1)或方式 2)产生一个 IV，然后：
   1) $IV_1=IV$；
   2) $IV_2=IV_1+R_1 \bmod 2^{64}$，$R_1=(5555555555555555)$；
   3) $IV_3=IV_1+R_2 \bmod 2^{64}$，$R_2=(AAAAAAAAAAAAAAAA)$。

——在以上 IV_2 和 IV_3 的等式中，二进制串或十六进制串转换成整数。运算是整数加法模 2^{64}。运算结果转换回二进制串或十六进制串；

——通过方式 2)，即用单调递增计数器产生 IV 时，IV 值一旦转换成整数，那么应小于 R_1。R_1 当作从(5555555555555555)转换出来的整数。

5.8 输入和输出

以下技术规范适用于 3-DEA 操作模式的输入和输出。

a) 3-DEA 的输入和输出是 64 比特分组。对于 TCFB 和 TCFB-P 模式，明文/密文块大小可为 1 比特、8 比特或者 64 比特。对于 TECB、TCBC、TCBC-I、TOFB 和 TOFB-I，明文/密文需要为其操作提供 64 比特的完整数据块。少于 64 比特的块需要特别处理，该部分内容不在本标准中阐述。

b) 由于中间结果把 3-DEA 的强度降低到 DEA 的水平，任何 3-DEA 操作模式的实施行为宜确保不同 DEA 功能块之间的中间结果不被泄露。因此，为防止针对 3-DEA 运算设备的攻击，设备本身必须加以物理防护，且绝对不能泄露中间结果。

c) 应禁止将起初的输出数据输出到运算设备之外，因为其无效且如果泄露可产生安全风险。每种操作模式应具体规定多少比特的输出宜加以禁止。

6 3-DEA 操作模式

6.1 3-DEA 操作模式电子密码本

6.1.1 TECB 定义

6.1.1.1 概述

如 6.2 所述，为 TECB 模式定义三个密钥选项。

6.1.1.2 TECB 加密

——输入：P_1、P_2、……、P_n；$|P_i|=64$；

——输出：C_1、C_2、……、C_n；$|C_i|=64$。

For $i=1,2,\cdots\cdots,n$, do

1) $C_i=E_{K3}(D_{K2}(E_{K1}(P_i)))$；

2) 输出 C_i。

TECB 加密如图 1 所示。

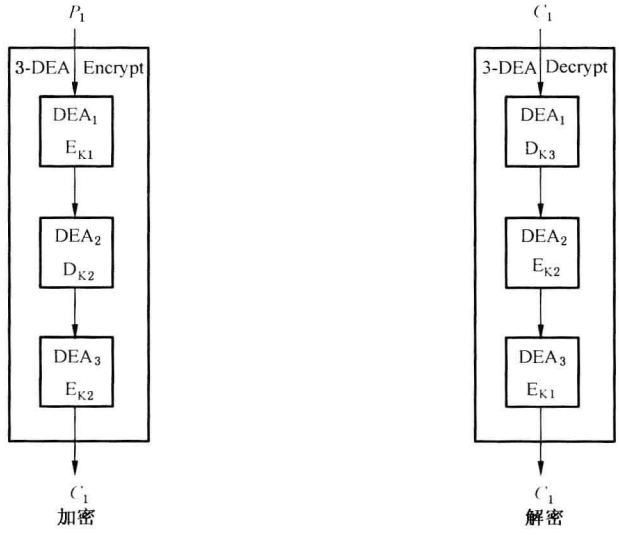

图 1 3-DEA 电子密码本

假设三个 DEA 功能块：DEA_1、DEA_2 和 DEA_3 同步并行运算。DEA_1 执行 E_{K1} 运算，DEA_2 执行 D_{K2} 运算，DEA_3 执行 E_{K3} 运算。在每个时钟周期里，每个 DEA_j 使用来自 DEA_{j-1} 的输入（或者来自输入缓冲区的输入）执行具体运算，把运算结果传给 DEA_{j+1}（或者传给输出缓冲区）。表 2 显示了三个 DEA 功能块是如何按照时间顺序安排的。在起初的两个时钟周期里，3-DEA 的 128 比特输出宜加以禁止，因为其并非有效的输出。

表 2　TECB 加密执行时间表执行时间表

时钟	输入	DEA_1	DEA_2	DEA_3	输出
$t=1$	P_1	$E_{K1}(P_1)$	空闲	空闲	N/A
$t=2$	P_2	$E_{K1}(P_2)$	$D_{K2}(E_{K1}(P_1))$	空闲	N/A
$t=3$	P_3	$E_{K1}(P_3)$	$D_{K2}(E_{K1}(P_2))$	$E_{K3}(D_{K2}(E_{K1}(P_1)))$	C_1
$t=4$	P_4	$E_{K1}(P_4)$	$D_{K2}(E_{K1}(P_3))$	$E_{K3}(D_{K2}(E_{K1}(P_2)))$	C_2
		…	…	…	
$t=h$	P_h	$E_{K1}(P_h)$	$D_{K2}(E_{K1}(P_{h-1}))$	$E_{K3}(D_{K2}(E_{K1}(P_{h-2})))$	C_{h-2}
		…	…	…	
$t=n$	P_n	$E_{K1}(P_n)$	$D_{K2}(E_{K1}(P_{1-1}))$	$E_{K3}(D_{K2}(E_{K1}(P_{n-1})))$	C_{n-2}
$t=n+1$	N/A	空闲	$D_{K2}(E_{K1}(P_4))$	$E_{K3}(D_{K2}(E_{K1}(P_{n-2})))$	C_{n-1}
$t=n+2$	N/A	空闲	空闲	$E_{K3}(D_{K2}(E_{K1}(P_{n-3})))$	C_n

例如：如果待加密的明文是“Now is the time for all good men”，那么其使用 ASCII 编码，采用 16 进制表示为：

X‘4E6F772069732074 68652074696D6520 666F7220616C6C20 676F6F64206D656E’

使用密钥 X‘0123456789ABCDEFFEDCBA9876543210’加密，得到表 3 结果。

表 3　TECB 加密示例

时钟	输入	DEA_1	DEA_2	DEA_3	输出
$t=1$	P_1 4E6F772069732074	$E_{K1}(P_1)$ 3FA40E8A984D4815	空闲	空闲	N/A
$t=2$	P_2 68652074696D6520	$E_{K1}(P_2)$ 6A271787AB8883F9	$D_{K2}(E_{K1}(P_1))$ 0EF020F064194595	空闲	N/A
$t=3$	P_3 666F7220616C6C20	$E_{K1}(P_3)$ 893D51EC4B563B53	$D_{K2}(E_{K1}(P_2))$ 174B332E073DE8AF	$E_{K3}(D_{K2}(E_{K1}(P_1)))$ D80A0D8B2BAE5E4E	C_1 D80A0D8B2BAE5E4E
$t=4$	P_4 676F6F64206D656E	$E_{K1}(P_4)$ 73C1ADB2171F7894	$D_{K2}(E_{K1}(P_3))$ 47B3F7F0E82E1F35	$E_{K3}(D_{K2}(E_{K1}(P_2)))$ 6A0094171ABCFC27	C_2 6A0094171ABCFC27
$t=5$	N/A	空闲	$D_{K2}(E_{K1}(P_4))$ 7A1E4ABD1DA455C6	$E_{K3}(D_{K2}(E_{K1}(P_3)))$ 75D2235A706E232C	C_3 75D2235A706E232C
$t=6$	N/A	空闲	空闲	$E_{K3}(D_{K2}(E_{K1}(P_4)))$ 41B637F9AB83FFD4	C_4 41B637F9AB83FFD4