TECHNICAL REPORT

ISO/TR 19038

First edition
2005-06-15

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

Banque et autres services financiers — Triple DEA — Modes d'opération — Lignes directrices pour la mise en œuvre

Reference number
ISO/TR 19038:2005(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In exceptional circumstances, when a technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide by a simple majority vote of its participating members to publish a Technical Report. A Technical Report is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/TR 19038 was prepared by Technical Committee ISO/TC 68, *Financial services*, Subcommittee SC 2, *Security management and general banking operations*.

Introduction

In order to significantly strengthen DEA (Data Encryption Algorithm) and extend its useful lifetime, the use of Triple Data Encryption Algorithm (TDEA) modes of operation has been recommended. These TDEA modes of operation not only provide greatly increased cryptographic protection, but because they are based on DEA, the TDEA learning curve for users and vendors is reduced. Since certain TDEA modes of operation can be made backward compatible with existing DEA modes of operation, the financial community may leverage its investment in standard DEA technology by using TDEA to extend its secure lifetime.

Each mode of operation provides different benefits and has different characteristics. The selection, implementation and use of a particular mode of operation is dependent upon the security requirements, risk acceptance posture, and operational needs of the financial institution and are beyond the scope of this Technical Report. This Technical Report is necessary to provide the basis for interoperability between different parties using any of the TDEA modes specified herein, provided that they use the same mode of operation and share the same secret cryptographic key(s).

This Technical Report does not replace the Data Encryption Algorithm Standard nor the Triple Data Encryption Algorithm specified in ISO/IEC 18033. DEA is the basis for the TDEA modes of operation. TDEA provides increased security in keeping with advances in computing technology and cryptanalytic techniques. TDEA may be implemented in hardware, software or a combination of hardware and software.

This Technical Report provides implementation guidelines for the modes of operation specified in ISO/IEC 10116.

It is the responsibility of the financial institution to put overall security procedures in place with the necessary controls to ensure that the process is implemented in a secure manner. Furthermore, the process should be audited to ensure compliance with the procedures.

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

1 Scope

This Technical Report provides the user with technical support and details for the safe and efficient implementation of the Triple Data Encryption Algorithm (TDEA) modes of operation for the enhanced cryptographic protection of digital data. The modes of operation described herein are specified for both enciphering and deciphering operations. The modes described in this Technical Report are implementations of the block cipher modes of operation specified in ISO/IEC 10116 using the Triple DEA algorithm (TDEA) specified in ISO/IEC 18033-3.

The TDEA modes of operation may be used in both wholesale and retail financial applications. The use of this Technical Report provides the basis for the interoperability of products and facilitates the development of application standards that use the TDEA modes of operation. This Technical Report is intended for use with other ISO standards using DEA.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 10116, *Information technology — Security techniques — Modes of operation for an n-bit block cipher*

ISO/IEC 18033-3, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*

ISO/IEC 9797-1, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
birthday phenomenon
phenomenon whereby at least two people out of a relatively small group of n people will likely share the same birthday

EXAMPLE: when $n = 23$, the probability is over ½. Generally, if one randomly picks up a number from m possible numbers with replacement, the probability to get at least one coincidence in n experiments ($n < m$) is approximated by:

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

In the above experiment, the expected number of trials before a coincidence is found is approximately $(\pi m/2)^{1/2}$. It implies that for a 64-bit block encryption operation with a fixed key, if one has a text dictionary of 2^{32} plaintext/ciphertext pairs and

2^{32} blocks of ciphertext produced from random input, then it should be expected that one block of unknown ciphertext will be found in the dictionary (see [11]).

3.2
block
binary string

EXAMPLE: a plaintext or a ciphertext, is segmented with a given length. Each segment is called a block. A plaintext (ciphertext) is encrypted (decrypted) block by block from left to right. In this Technical Report, for TCBC, TCBC-I, TOFB, TOFB-I modes, the plaintext and ciphertext are segmented into 64-bit blocks, while for TCFB and TCFB-P modes, the encryption and decryption support 1-bit, 8-bit and 64-bit plaintext and ciphertext block sizes.

3.3
bundle
collection of elements comprising a TDEA (K) key

NOTE A bundle may consist of two elements (k_1,k_2) or three elements (k_1,k_2,k_3).

3.4
ciphertext
encrypted (enciphered) data

3.5
clock cycle
time unit used in this Technical Report to define the time period for executing DEA operation once by one DEA functional block

3.6
cryptographic initialization
process of entering the initialization vector(s) into the TDEA to initialize the algorithm prior to the commencement of encryption or decryption

3.7
cryptographic key
key
parameter that determines the transformation from plaintext to ciphertext and vice versa

NOTE A DEA key is a 64-bit parameter consisting of 56 independent bits and 8 parity bits.

3.8
cryptoperiod
time span during which a specific (bundle of) key(s) is authorized for use

3.9
data encryption algorithm
DEA
algorithm specified in ISO/IEC 18033-3

NOTE The term “single DEA” implies DEA, whereas TDEA implies triple DEA as defined in this Technical Report.

3.10
DEA encryption operation
enciphering of 64-bit blocks by DEA with a key K

3.11
DEA decryption operation
deciphering of 64-bit blocks by DEA with a key K

3.12
DEA functional block
that which performs either a DEA encryption operation or a DEA decryption operation with a specified key

NOTE In this Technical Report, each DEA functional block is represented by DEA_j.

3.13
decryption
process of transforming ciphertext into plaintext

3.14
encryption
process of transforming plaintext into ciphertext

3.15
exclusive-OR
bit-by-bit modulo 2 addition of binary vectors of equal length

3.16
initialization vector
binary vector used as the input to initialize the algorithm for the encryption of a plaintext block sequence to increase security by introducing additional cryptographic variance and to synchronize cryptographic equipment

NOTE The initialization vector need not be secret.

3.17
key
see **3.7** cryptographic key

3.18
plaintext
intelligible data that has meaning and can be read or acted upon without the application of decryption

NOTE Also known as cleartext.

3.19
propagation delay
delay between the presentation of a plaintext block to a TDEA mode and the availability of the resulting ciphertext block

3.20
re-synchronization
synchronization, after being lost because of the addition or deletion of bits in one or more ciphertext blocks

EXAMPLE: if the additions or deletions can be detected, and if the appropriate number of bits can be deleted or added to the ciphertext so that the block boundaries are re-established correctly starting at block C_i such that the succeeding decrypted plaintext is correct from block P_{i+r} for some r, then we say that it is re-synchronized at C_{i+r}.

3.21
self-synchronization
automatic re-synchronization

EXAMPLE: the TCBC mode exhibits self-synchronization in the sense that if an error (including the loss of one or more entire blocks) occurs in ciphertext block C_i but no further error occurs, then C_{i+2} and succeeding ciphertext blocks are correctly decrypted to P_{i+2} and succeeding plaintext blocks (see [11] and [12]).

3.22
synchronization
where, for a plaintext with blocks P_1, P_2, … P_n if it is encrypted as a ciphertext with blocks C_1, C_2, … C_n, then for any i, $1 \leqslant i \leqslant n$, P_1, P_2, … P_i can be correctly decrypted from C_1, C_2, … C_i.

NOTE If some error occurs in the transmission of the ciphertext or if some bits are added or lost from the ciphertext, then synchronization is lost.

4 Symbols and abbreviations

C_i i-th ciphertext block consisting of k bits, where k = 1, 8, 64.

$C^{(j)}$ j-th ciphertext substream in TCBC-I mode.

$C_{j,i}$ i-th block in j-th ciphertext substream.

CBC Cipher block chaining.

CFB Cipher feedback.

D_{K_j} A DEA decryption operation with key "K_j".

DEA The data encryption algorithm specified in ISO/IEC 18033-3.

DEA_j j-th DEA functional block.

E_{K_j} A DEA encryption operation with key "K_j".

ECB Electronic codebook.

I_i i-th input block of encryption operation consisting of 64 bits in TCFB, TCFB-P, TOFB, and TOFB-I modes of operation.

i Index of blocks.

IV Initialization vector.

j Index of functional blocks, index of keys, and index of plaintext substreams (ciphertext substreams) in TCBC-I.

h A given counter value of a clock cycle. It is for describing the actions of each DEA functional block at $t = h - 1$, $t = h$, and $t = h + 1$. In the interleaved or pipelined mode, h is used to describe at clock cycle $t = 3(h - 1) + j$, j = 1, 2, 3, the simultaneous actions of three functional blocks. In the interleaved mode, h is used as an index of blocks for tripartition of a plaintext.

k Size of blocks, a parameter for shifting functions S_k, k = 1, 8, 64.

K Cryptographic key.

n Number of blocks in a plaintext.

O_i i-th output block of encryption operation consisting of 64 bits in TCFB, TCFB-P, TOFB, and TOFB-I modes of operation.

$\{O_i\}_k$ Leftmost k bits of O_i, k =1, 8, 64. When k = 64, $\{O_i\}_k = O_i$.

OFB Output feedback.

P_i i-th plaintext block consisting of k bits, where k = 1, 8, 64.

$P^{(j)}$ j-th plaintext substream in TCBC-I mode.

$P_{j,i}$ i-th plaintext block in j-th plaintext substream.

S_k "k-Shifting" function, defined as follows:

Given a 64-bit block I = (i_1, i_2, …, i_{64}) and a k-bit block C = (c_1, c_2, … c_k) where k = 1, 8, 64, the shifting function S_k(I | C) produces a 64-bit block:

$S_k(\mathrm{I} \mid \mathrm{C}) = \{i_{k+1}, i_{k+2}, ..., i_{64}, c_1, c_2, ... c_k\}$

where the bits of I have been shifted left by k places, discarding i_1, i_2, ... i_k and placing the k bits of C in the rightmost k places of I. When k = 64, S_k(I | C) = C.

t Counter of clock cycle starting from 1.

TCBC TDEA cipher block chaining.

TCBC-I TDEA cipher block chaining-interleaved.

TCFB TDEA cipher feedback.

TCFB-P TDEA cipher feedback-pipelined.

TDEA Triple data encryption algorithm.

TECB TDEA electronic codebook.

TOFB TDEA output feedback.

TOFB-I TDEA output feedback-interleaved.

X⊕Y "Exclusive-or" operation of X and Y.

X || Y Concatenation of X and Y.

|X| Length of binary string X.

5 Specifications

5.1 TDEA encryption/decryption operation

In this Technical Report, each TDEA encryption/decryption operation is a compound operation of DEA encryption and decryption operations as specified in ISO/IEC 18033-3. The following operations are to be used in this Technical Report.

a) TDEA encryption operation: the transformation of a 64-bit block I into a 64-bit block O that is defined as follows:

$$\mathrm{O} = \mathrm{E}_{\mathrm{K}3}(\mathrm{D}_{\mathrm{K}2}(\mathrm{E}_{\mathrm{K}1}(\mathrm{I}))).$$

b) TDEA decryption operation: the transformation of a 64-bit block I into a 64-bit block O that is defined as follows:

$$\mathrm{O} = \mathrm{D}_{\mathrm{K}1}(\mathrm{E}_{\mathrm{K}2}(\mathrm{D}_{\mathrm{K}3}(\mathrm{I}))).$$

5.2 Keying options

This Technical Report uses the following keying options for the TDEA key.

a) Keying Option 1: K1, K2 and K3 are independent keys;

b) Keying Option 2: K1 and K2 are independent keys and K3 = K1;

c) Keying Option 3: K1 = K2 = K3.

NOTE Keying option 3 is not recommended as its use reduces the strength of the TDEA operation to that of DEA.

5.3 TDEA modes of operation

This Technical Report discusses:

a) TDEA Electronic Codebook Mode (TECB);

b) TDEA Cipher Block Chaining Mode (TCBC);

c) TDEA Cipher Block Chaining Mode — Interleaved (TCBC-I);

d) TDEA Cipher Feedback Mode (TCFB);

e) TDEA Cipher Feedback Mode — Pipelined (TCFB-P);

f) TDEA Output Feedback Mode (TOFB);

g) TDEA Output Feedback Mode — Interleaved (TOFB-I).

These are triple DEA implementations of the ECB, CBC, CFB, and OFB modes of operation specified in ISO/IEC 10116. For applications in which high TDEA encryption/decryption throughput is important or in which propagation delay must be minimized, the new interleaved (for TCBC and TOFB) and pipelined (for TCFB) modes are provided.

5.4 Backward compatibility

In this Technical Report, a TDEA mode of operation is backward compatible with its single DEA counterpart if, with a proper keying option for TDEA operation,

a) an encrypted plaintext computed using a single DEA mode of operation can be decrypted correctly by a corresponding TDEA mode of operation;

b) an encrypted plaintext computed using a TDEA mode of operation can be decrypted correctly by a corresponding single DEA mode of operation.

When using Keying Option 3, TECB, TCBC, TCFB and TOFB modes are backward compatible with single DEA modes of operation ECB, CBC, CFB, OFB respectively. It should be noted that backward compatibility with single DEA reduces the security of the TDEA mode to that of the single DEA mode.

5.5 Schedule of DEA functional blocks

In this Technical Report, one clock cycle is defined as the time period for a DEA functional block to perform $E_K(I)$ or $D_K(I)$. In a schedule of DEA functional blocks, $O = E_{K3}(D_{K2}(E_{K1}(I)))$ is broken down into three actions. Each action is finished in one clock cycle by a functional block. The following table shows the schedule for three DEA functional blocks in performing $E_{K3}(D_{K2}(E_{K1}(I)))$.

	Input	DEA_1	DEA_2	DEA_3	Output
$t = 1$	I	$\mathrm{E}_{K1}(\mathrm{I})$			
$t = 2$			$\mathrm{D}_{K2}(\mathrm{E}_{K1}(\mathrm{I}))$		
$t = 3$				$\mathrm{E}_{K3}(\mathrm{D}_{K2}(\mathrm{E}_{K1}(\mathrm{I})))$	O

5.6 Improving throughput and minimizing propagation

As is shown in 5.5, a valid TDEA output block, O, is produced only after the input block, I, has propagated through the three individual DEA functional blocks. That is, it takes three clock cycles to get the output. Within each clock cycle, only one DEA functional block is actively encrypting/decrypting data. This configuration provides the slowest throughput speed and greatest propagation delay.

In order to improve the throughput and minimize the propagation, interleaved and pipelined modes of operation are provided. They are TCBC-I, TCFB-P, and TOFB-I modes. In an interleaved mode, the plaintext sequence is split into three subsequences of plaintext. The encryption can be done simultaneously. In a pipelined mode, the encryption is initiated with three IVs at three clock cycles so that after initialization, the three DEA functional blocks can process the data simultaneously. The interleaved and pipelined configurations are intended for systems equipped with multiple DEA processors.

In a mode of operation, which is interleaved or pipelined, a schedule defines simultaneous actions of multiple DEA functional blocks within each clock cycle.

5.7 Keys and initialization vectors

The following specifications for keys and initialization vectors shall be met in implementing the TDEA modes of operation.

a) For all TDEA modes of operation, the three cryptographic keys (K_1, K_2, K_3) define a TDEA key bundle. The bundle and the individual keys shall:

   1) be secret;

   2) be generated randomly;

   3) have integrity whereby each key in the bundle has not been altered in an unauthorized manner since the time it was generated, transmitted, or stored by an authorized source;

   4) be used in the appropriate order as specified by the particular mode;

   5) be considered a fixed quantity in which an individual key cannot be manipulated while leaving the other two keys unchanged;

   6) cannot be unbundled for any purpose.

b) IVs shall meet the following attributes:

   1) for TECB, no IV is used;

   2) for all modes using IV(s), the IV(s) may be public information;

   3) in the cryptoperiod of a given bundle of keys, a new IV or three new IVs shall be generated whenever the encryption process is reinitialized.

c) IVs shall be generated by one of the following methods, which are given in order of preference:

   1) generate randomly or

   2) use values of a monotonically increasing counter such that the values will not be repeated during the cryptoperiod of the keys.

d) When three IVs are required, then generate IV by method 1) or method 2) in item c) such that

   1) $IV_1 = IV$;

   2) $IV_2 = IV_1 + R_1 \bmod 2^{64}$, where R_1 = (5555555555555555);

   3) $IV_3 = IV_1 + R_2 \bmod 2^{64}$, where R_2 = (AAAAAAAAAAAAAAAA).

- In the above equations for IV_2 and IV_3, the binary strings or hexadecimal strings are converted to integers. The operation is integer addition modulo 2^{64}. The operation results shall be converted back to binary strings or hexadecimal strings.

- When the IV is generated by method 2), i.e. values of a monotonically increasing counter are used, the IV value, once converted to an integer, shall be smaller than R_1. R_1 is considered as the integer converted from (5555555555555555).

5.8 Input and output

For the input and output of the TDEA modes of operation, the following specification applies.

a) The input and output of a TDEA operation are 64-bit blocks. For TCFB and TCFB-P modes, the plaintext/ciphertext block size may be 1 bit, 8 bits, or 64 bits. For TECB, TCBC, TCBC-I, TOFB, TOFB-I modes, the plaintext/ciphertext requires complete data blocks of 64 bits for its operation. Blocks of less than 64 bits require special handling, which is not addressed in this Technical Report.

b) As knowledge of intermediate results reduces the strength of the TDEA to that of DEA, implementations of any TDEA mode of operation should ensure that the intermediate results between the different DEA functional blocks are not revealed. Thus to protect against attacks on the device implementing TDEA the device itself must be a physically secure device and must not reveal intermediate results.

c) The initial output data shall be suppressed because it is invalid and may create a security risk if revealed. Each mode of operation shall specify how many bits of output should be suppressed.

6 TDEA modes of operation

6.1 TDEA electronic codebook mode of operation

6.1.1 TECB definition

6.1.1.1 General

Three keying options are defined for TECB mode as described in Section 6.2.

6.1.1.2 TECB encryption

- **Input**: $P_1, P_2, \ldots P_n$; $|P_i| = 64$.

- **Output**: $C_1, C_2, \ldots C_n$; $|C_i| = 64$.

For i = 1, 2, … n, do

1) $C_i = E_{K3}(D_{K2}(E_{K1}(P_i)))$;

2) Output C_i.

The TECB encryption is shown in Figure 1.

Suppose that three DEA functional blocks, DEA_1, DEA_2, and DEA_3, are simultaneously clocked. Let DEA_1 perform the E_{K1} operation, DEA_2 perform the D_{K2} operation and DEA_3 perform the E_{K3} operation. At each clock cycle, each DEA_j performs the specified operation with the input from DEA_{j-1} (or input buffer) and passes the result to DEA_{j+1} (or output buffer). Table 1 shows how three DEA functional blocks are scheduled. At the first two clock cycles, the 128-bit output of the TDEA should be suppressed since valid output is not produced.

Table 1 — Schedule of TECB encryption

Clock	Input	DEA_1	DEA_2	DEA_3	Output
$t = 1$	P_1	$E_{K1}(P_1)$	idle	idle	N/A
$t = 2$	P_2	$E_{K1}(P_2)$	$D_{K2}(E_{K1}(P_1))$	idle	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	$E_{K1}(P_n)$	$D_{K2}(E_{K1}(P_{n-1}))$	$E_{K3}(D_{K2}(E_{K1}(P_{n-2})))$	C_{n-2}
$t = n + 1$	N/A	idle	$D_{K2}(E_{K1}(P_n))$	$E_{K3}(D_{K2}(E_{K1}(P_{n-1})))$	C_{n-1}
$t = n + 2$	N/A	idle	idle	$E_{K3}(D_{K2}(E_{K1}(P_n)))$	C_n

For example:

If the plaintext to be enciphered is “Now is the time for all good men” which when encoded in ASCII is represented in hexadecimal as:

```
X'4E6F772069732074 68652074696D6520 666F7220616C6C20 676F6F64206D656E'
```

is enciphered using TECB mode with Key `X'0123456789ABCDEFFEDCBA9876543210'` the following results.