INTERNATIONAL STANDARD

ISO/IEC 18033-3

Second edition
2010-12-15

Information technology — Security techniques — Encryption algorithms —

Part 3: Block ciphers

Technologies de l'information — Techniques de sécurité — Algorithmes de chiffrement

Partie 3: Chiffrement par blocs

Reference number
ISO/IEC 18033-3:2010(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.

COPYRIGHT PROTECTED DOCUMENT

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) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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

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

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

ISO/IEC 18033-3 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 18033-3:2005), which has been technically revised. It also incorporates the Technical Corrigenda ISO/IEC 18033-3:2005/Cor.1:2006, ISO/IEC 18033-3:2005/Cor.2:2007 and ISO/IEC 18033-3:2005/Cor.3:2008.

ISO/IEC 18033 consists of the following parts, under the general title *Information technology — Security techniques — Encryption algorithms*:

— *Part 1: General*

— *Part 2: Asymmetric ciphers*

— *Part 3: Block ciphers*

— *Part 4: Stream ciphers*

Information technology — Security techniques — Encryption algorithms —

Part 3: Block ciphers

1 Scope

This part of ISO/IEC 18033 specifies block ciphers. A block cipher maps blocks of *n* bits to blocks of *n* bits, under the control of a key of *k* bits. A total of seven different block ciphers are defined. They are categorized in Table 1.

Table 1 — Block ciphers specified

Block length	Algorithm name (see #)		Key length
64 bits	TDEA	(4.2)	128 or 192 bits
	MISTY1	(4.3)	128 bits
	CAST-128	(4.4)	
	HIGHT	(4.5)	
128 bits	AES	(5.2)	128, 192 or 256 bits
	Camellia	(5.3)	
	SEED	(5.4)	128 bits

The algorithms specified in this part of ISO/IEC 18033 have been assigned object identifiers in accordance with ISO/IEC 9834. The list of assigned object identifiers is given in Annex B. Any changes to the specification of the algorithms resulting in a change of functional behaviour will result in a change of the object identifier assigned to the algorithm.

2 Terms and definitions

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

2.1
block
string of bits of defined length

NOTE In this part of ISO/IEC 18033, the block length is either 64 or 128 bits.

[ISO/IEC 18033-1:2005]

2.2
block cipher
symmetric encipherment system with the property that the encryption algorithm operates on a block of plaintext, i.e. a string of bits of a defined length, to yield a block of ciphertext

[ISO/IEC 18033-1:2005]

2.3
ciphertext
data which has been transformed to hide its information content

[ISO/IEC 9798-1:1997]

2.4
key
sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment)

NOTE In all the ciphers specified in this part of ISO/IEC 18033, keys consist of a sequence of bits.

[ISO/IEC 11770-1:1996]

2.5
***n*-bit block cipher**
block cipher with the property that plaintext blocks and ciphertext blocks are *n* bits in length

[ISO/IEC 10116:2006]

2.6
plaintext
unenciphered information

[ISO/IEC 9797-1:1999]

3 Symbols

n	plaintext/ciphertext bit length for a block cipher
E_K	encryption function with key K
D_K	decryption function with key K
Nr	the number of rounds for the AES algorithm, which is 10, 12 or 14 for the choices of key length 128, 192 or 256 bits respectively
$\oplus$	the bit-wise logical exclusive-OR operation on bit-strings, i.e., if A, B are strings of the same length then $A \oplus B$ is the string equal to the bit-wise logical exclusive-OR of A and B
$\otimes$	multiplication of two polynomials (each with degree < 4) modulo $x^4 + 1$
$\wedge$	the bit-wise logical AND operation on bit-strings, i.e., if A, B are strings of the same length then $A \wedge B$ is the string equal to the bit-wise logical AND of A and B
$\vee$	the bit-wise logical OR operation on bit-strings, i.e., if A, B are strings of the same length then $A \vee B$ is the string equal to the bit-wise logical OR of A and B
||	concatenation of bit strings
•	finite field multiplication
$<<<_i$	the left circular rotation of the operand by i bits
$>>>_i$	the right circular rotation of the operand by i bits

$\overline{x}$	the bitwise complement of *x*
a mod *n*	for integers a and n, (a mod n) denotes the (non-negative) remainder obtained when a is divided by n. Equivalently if $b = a \bmod n$, then b is the unique integer satisfying: (i) $0 \leq b < n$, and (ii) (b-a) is an integer multiple of n
⊞	addition in modular arithmetic, i.e., if *A*, *B* are *t*-bit strings then *A*⊞*B* is defined to equal (*A*+*B* *mod* 2^t)
⊟	subtraction in modular arithmetic, i.e., if *A*, *B* are *t*-bit strings then *A*⊟*B* is defined to equal (*A*-*B* *mod* 2^t)

4 64-bit block ciphers

4.1 Introduction

In this clause, four 64-bit block ciphers are specified; TDEA (or 'Triple DES') in 4.2, MISTY1 in 4.3, CAST-128 in 4.4, and HIGHT in 4.5.

Users authorized to access data that has been enciphered shall have the key that was used to encipher the data in order to decipher it. The algorithm for any cipher in this clause is designed to encipher and decipher blocks of data consisting of 64 bits under control of a 128- (or 192-) bit key. Deciphering shall be accomplished using the same key as for enciphering.

4.2 TDEA

4.2.1 The Triple Data Encryption Algorithm

The Triple Data Encryption Algorithm (TDEA) is a symmetric cipher that can process data blocks of 64 bits, using cipher keys with length of 128 (or 192) bits, of which 112 (or 168) bits can be chosen arbitrarily, and the rest may be used for error detection. The TDEA is commonly known as Triple DES (Data Encryption Standard).

A TDEA encryption/decryption operation is a compound operation of DES encryption and decryption operations, where the DES algorithm is specified in Annex A. A TDEA key consists of three DES keys.

4.2.2 TDEA encryption/decryption

4.2.2.1 Encryption/decryption definitions

The TDEA is defined in terms of DES operations, where E_K is the DES encryption operation for the key *K* and D_K is the DES decryption operation for the key *K*.

4.2.2.2 TDEA encryption

The transformation of a 64-bit block *P* into a 64-bit block *C* is defined as follows:

$$C = E_{K_3}(D_{K_2}(E_{K_1}(P))).$$

4.2.2.3 TDEA decryption

The transformation of a 64-bit block *C* into a 64-bit block *P* is defined as follows:

$$P = D_{K_1}(E_{K_2}(D_{K_3}(C))) .$$

4.2.3 TDEA keying options

This part of ISO/IEC 18033 specifies the following keying options for TDEA. The TDEA key comprises the triple (K_1, K_2, K_3).

1. Keying Option 1: K_1, K_2 and K_3 are different DES keys;
2. Keying Option 2: K_1 and K_2 are different DES keys and $K_3 = K_1$.

NOTE The option that $K_1 = K_2 = K_3$, the single-DES equivalent, is not recommended. Furthermore, the use of keying option 1 is preferred over keying option 2 since it provides additional security at the same performance level (see [3] for further details).

4.3 MISTY1

4.3.1 The MISTY1 algorithm

The MISTY1 algorithm is a symmetric block cipher that can process data blocks of 64 bits, using a cipher key with length of 128 bits.

4.3.2 MISTY1 encryption

The encryption operation is as shown in Figure 1. The transformation of a 64-bit block *P* into a 64-bit block *C* is defined as follows (*KL*, *KO* and *KI* are keys):

(1) $P = L_0 \,||\, R_0$

$KL = KL_1 \,||\, KL_2 \,||\, \ldots \,||\, KL_{10}$

$KO = KO_1 \,||\, KO_2 \,||\, \ldots \,||\, KO_8$

$KI = KI_1 \,||\, KI_2 \,||\, \ldots \,||\, KI_8$

(2) for $i = 1, 3, \ldots, 7$ (increment in steps of 2 because the loop body consists of two rounds):

$R_i = \mathrm{FL}(L_{i-1}, KL_i)$

$L_i = \mathrm{FL}(R_{i-1}, KL_{i+1}) \oplus \mathrm{FO}(R_i, KO_i, KI_i)$

$L_{i+1} = R_i \oplus \mathrm{FO}(L_i, KO_{i+1}, KI_{i+1})$

$R_{i+1} = L_i$

for $i = 9$:

$R_i = \mathrm{FL}(L_{i-1}, KL_i)$

$L_i = \mathrm{FL}(R_{i-1}, KL_{i+1})$

(3) $C = L_9 \,||\, R_9$

4.3.3 MISTY1 decryption

The decryption operation is as shown in Figure 2, and is identical in operation to encryption apart from the following two modifications.

(1) All FL functions are replaced by their inverse functions FL^{-1}.

(2) The order in which the subkeys are applied is reversed.

4.3.4 MISTY1 functions

4.3.4.1 MISTY1 function definitions

The MISTY1 algorithm uses a number of functions, namely S_7, S_9, FI, FO, FL and FL^{-1}, which are now defined.

4.3.4.2 Function FL

The FL function is used in encryption only and is shown in Figure 3. The FL function is defined as follows (X and Y are data, KL is a key):

(1) $X_{32} = X_L \,||\, X_R$, $KL_i = KL_{iL} \,||\, KL_{iR}$

(2) $Y_R = (X_L \wedge KL_{iL}) \oplus X_R$

(3) $Y_L = X_L \oplus (Y_R \vee KL_{iR})$

(4) $Y_{32} = Y_L \,||\, Y_R$