
**Information technology — Security
techniques — Hash-functions —**

**Part 2:
Hash-functions using an n -bit block cipher**

*Technologies de l'information — Techniques de sécurité — Fonctions de
brouillage*
Partie 2: Fonctions de brouillage utilisant un chiffrement par blocs de n bits

<https://standards.iteh.ai/catalog/standards/sist/522c4d31-1853-4be8-b2e1-0e9eab0e5b09/iso-iec-10118-2-2000>

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 10118-2:2000

<https://standards.iteh.ai/catalog/standards/sist/522c4d31-1853-4be8-b2e1-0e9eab0e5b09/iso-iec-10118-2-2000>

© ISO/IEC 2000

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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.ch
Web www.iso.ch

Printed in Switzerland

Contents

Page

Foreword.....	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols and abbreviated terms	1
5 Use of the general model	2
6 Hash-function one	2
6.1 Parameter selection.....	2
6.2 Padding method.....	2
6.3 Initializing value	2
6.4 Round-function	2
6.5 Output transformation.....	3
7 Hash-function two	3
7.1 Parameter selection.....	3
7.2 Padding method.....	3
7.3 Initializing value	3
7.4 Round-function	4
7.5 Output transformation.....	5
8 Hash-function three.....	5
8.1 General.....	5
8.2 Parameter selection.....	5
8.3 Padding method.....	5
8.4 Initializing value	6
8.5 Round-function	6
8.6 Output transformation.....	8
9 Hash-function four.....	8
9.1 General.....	8
9.2 Parameter selection.....	8
9.3 Padding method.....	8
9.4 Initializing value	8
9.5 Round-function	8
9.6 Output transformation.....	10
Annex A (informative) Use of DEA.....	11
Annex B (informative) Examples	14
Bibliography	19

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. 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.

International Standard ISO/IEC 10118-2 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 10118-2:1994), which has been technically revised to conform to the general model described in ISO/IEC 10118-1, and to add two additional hash-functions. Note, however, that implementations which comply with ISO/IEC 10118-2:1994 will be compliant with this edition of ISO/IEC 10118-2.

ISO/IEC 10118 consists of the following parts, under the general title *Information technology — Security techniques — Hash-functions*:

- Part 1: General <https://standards.iteh.ai/catalog/standards/sist/522c4d31-1853-4be8-b2e1-0e9eab0e5b09/iso-iec-10118-2-2000>
- Part 2: Hash-functions using an *n*-bit block cipher
- Part 3: Dedicated hash-functions
- Part 4: Hash-functions using modular arithmetic

Annexes A and B of this part of ISO/IEC 10118 are for information only.

Introduction

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this part of ISO/IEC 10118 may involve the use of a patent concerning the "Data Authentication Using Modification Detection Codes Based on a Public One Way Encryption Function," (U.S. Patent 4,908,861 issued 1990-03-13).

ISO and IEC take no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured ISO and IEC that he is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with ISO and IEC. Information may be obtained from:

Director of Licensing
International Business Machines Corporation
500 Columbus Avenue
Thornwood, NY 10594
U.S.A.

Attention is drawn to the possibility that some of the elements of this part of ISO/IEC 10118 may be the subject of patent rights other than those identified above. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ITeH STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 10118-2:2000
<https://standards.iteh.ai/catalog/standards/sist/522c4d31-1853-4be8-b2e1-0e9eab0e5b09/iso-iec-10118-2-2000>

iTeh STANDARD PREVIEW **(standards.iteh.ai)**

ISO/IEC 10118-2:2000

<https://standards.iteh.ai/catalog/standards/sist/522c4d31-1853-4be8-b2e1-0e9eab0e5b09/iso-iec-10118-2-2000>

Information technology — Security techniques — Hash-functions —

Part 2: Hash-functions using an n -bit block cipher

1 Scope

This part of ISO/IEC 10118 specifies hash-functions which make use of an n -bit block cipher algorithm. They are therefore suitable for an environment in which such an algorithm is already implemented.

Four hash-functions are specified. The first provides hash-codes of length smaller than or equal to n , where n is the block-length of the algorithm used. The second provides hash-codes of length less than or equal to $2n$; the third provides hash-codes of length equal to $2n$; and the fourth provides hash-codes of length $3n$. All four of the hash-functions specified in this part of ISO/IEC 10118 conform to the general model specified in ISO/IEC 10118-1.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 10118. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of ISO/IEC 10118 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO/IEC 10116:1997, *Information technology — Security techniques — Modes of operation for an n -bit block cipher*.

ISO/IEC 10118-1:2000, *Information technology — Security techniques — Hash-functions — Part 1: General*.

3 Terms and definitions

For the purposes of this part of ISO/IEC 10118, the terms and definitions given in ISO/IEC 10118-1 and the following apply.

3.1

n -bit block cipher

a block cipher with the property that plaintext blocks and ciphertext blocks are n bits in length (see ISO/IEC 10116)

4 Symbols and abbreviated terms

For the purposes of this part of ISO/IEC 10118, the symbols and abbreviations given in ISO/IEC 10118-1 and the following apply:

e n -bit block cipher algorithm (see ISO/IEC 10116)

K Key for the algorithm e (see ISO/IEC 10116)

$e_K(P)$	Operation of encipherment using the algorithm e and the key K (see ISO/IEC 10116) on plaintext P
u or u'	Transformation of one n -bit block into a key for the algorithm e
B^L	When n is even, the string composed of the $n/2$ leftmost bits of the block B . When n is odd, the string composed of the $(n+1)/2$ leftmost bits of the block B
B^R	When n is even, the string composed of the $n/2$ rightmost bits of the block B . When n is odd, the string composed of the $(n-1)/2$ rightmost bits of the block B
B^x	When B is a string of n m -bit blocks, B^x represents the x -th m -bit block of B
B^{x-y}	When B is a string of n m -bit blocks, B^{x-y} represents the x -th through the y -th m -bit blocks of B

5 Use of the general model

The hash-functions specified in the next four clauses provide hash-codes H of length L_H . The hash-function conforms to the general model specified in ISO/IEC 10118-1. For each of the four hash-functions that follow, it is therefore only necessary to specify:

- the parameters L_1, L_2 ;
- the padding method;
- the initializing value IV ;
- the round-function ϕ ;
- the output transformation T .

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 10118-2:2000

<https://standards.iteh.ai/catalog/standards/sist/522c4d31-1853-4be8-b2e1-0e9cab0c5b09/iso-iec-10118-2-2000>

The use of a hash-function defined using the general model will also require the selection of the parameter L_H .

6 Hash-function one

6.1 Parameter selection

The parameters L_1 and L_2 and L_H for the hash-function specified in this clause shall satisfy $L_1 = L_2 = n$, and L_H is less than or equal to n .

6.2 Padding method

The selection of the padding method for use with this hash-function is beyond the scope of this part of ISO/IEC 10118. Examples of padding methods are presented in annex A of ISO/IEC 10118-1:2000.

6.3 Initializing value

The selection of the IV for use with this hash-function is beyond the scope of this part of ISO/IEC 10118. The value of the IV shall be agreed upon and fixed by the users of the hash-function.

6.4 Round-function

The round-function ϕ combines a padded data block D_i (of $L_1 = n$ -bits) with H_{i-1} , the previous output of the round-function (of $L_2 = n$ bits), to yield H_i . As part of the round-function it is necessary to choose a function u , which transforms an n -bit block into a key for use with the block cipher algorithm e . The selection of the function u for use with this hash-function is outside the scope of this part of ISO/IEC 10118 (see annex A for guidance).

The round-function itself is defined as follows:

$$\phi(D_j, H_{j-1}) = e_{K_j}(D_j) \oplus D_j$$

where $K_j = u(H_{j-1})$. The round-function is shown in Figure 1.

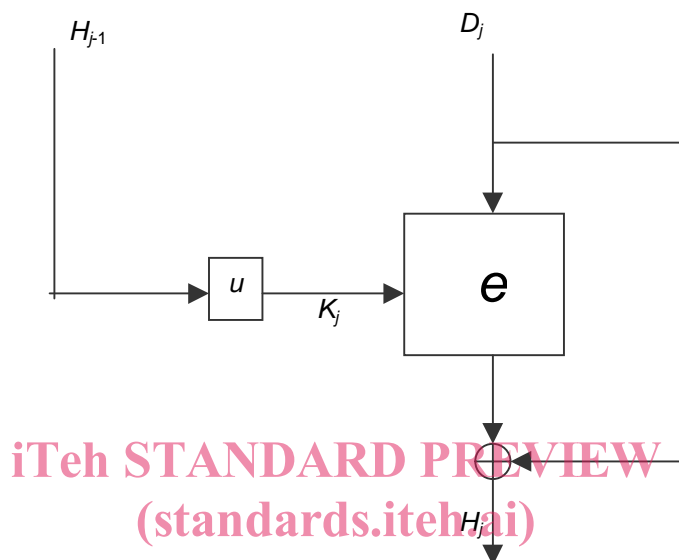


Figure 1 — Round-function of hash-function one

6.5 Output transformation

The output transformation T is simply truncation, i.e., the hash-code H is derived by taking the leftmost L_H bits of the final output block H_q .

7 Hash-function two

7.1 Parameter selection

The parameters L_1 and L_2 and L_H for the hash-function specified in this clause shall satisfy $L_1 = n$, $L_2 = 2n$, and L_H is less than or equal to $2n$.

7.2 Padding method

The selection of the padding method for use with this hash-function is beyond the scope of this part of ISO/IEC 10118. Examples of padding methods are presented in annex A of ISO/IEC 10118-1:2000.

7.3 Initializing value

The selection of the IV (of length $2n$) for use with this hash-function is beyond the scope of this part of ISO/IEC 10118. The value of the IV shall be agreed upon and fixed by the users of the hash-function. However, the IV shall be selected such that $u(IV^L)$ and $u(IV^R)$ are different.

7.4 Round-function

The round-function ϕ combines a padded data block D_i (of $L_1 = n$ bits) with H_{i-1} , the previous output of the round-function (of $L_2 = 2n$ bits), to yield H_i . As part of the round-function it is necessary to choose two transformations u and u' . These transformations are used to transform an output block into two suitable L_K bit keys for the algorithm e . The specification of u and u' is beyond the scope of this part of ISO/IEC 10118. However, it should be taken into consideration that the selection of u and u' is important for the security of the hash-function (see annex A).

Set H_0^L and H_0^R equal to IV^L and IV^R respectively. The output blocks are calculated iteratively in the following way, for $j = 1$ to q :

$$\phi(D_j, H_{j-1}) = H_j$$

$$K_j^L = u(H_{j-1}^L) \text{ and } K_j^R = u'(H_{j-1}^R)$$

$$B_j = e_{K_j^L}(D_j) \oplus D_j, \text{ and } B'_j = e_{K_j^R}(D_j) \oplus D_j$$

$$H_j^L = B_j^L \parallel B'_j{}^R \text{ and } H_j^R = B'_j{}^L \parallel B_j^R$$

The round-function is shown in Figure 2.

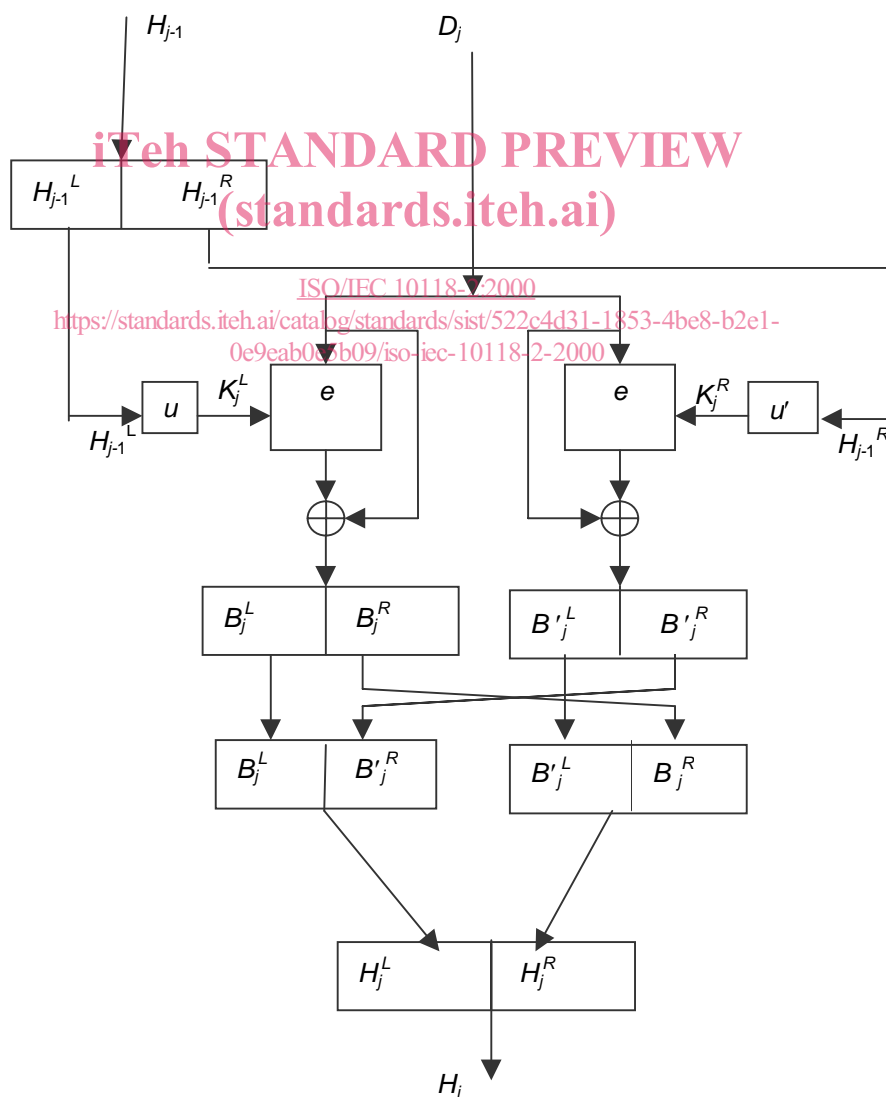


Figure 2 — Round-function of hash-function two

7.5 Output transformation

If L_H is even, the hash-code is the concatenation of the $L_H/2$ leftmost bits of H_q^L and the $L_H/2$ leftmost bits of H_q^R . If L_H is odd, the hash-code is the concatenation of the $(L_H+1)/2$ leftmost bits of H_q^L and the $(L_H-1)/2$ leftmost bits of H_q^R .

8 Hash-function three

The hash-function specified in this clause provides hash-codes of length L_H , where L_H is equal to $2n$ for even values of n .

8.1 General

Some specific definitions that are required to specify hash-function three follow.

Transformation u :

Define r mappings u_1, u_2, \dots, u_r from the ciphertext space to the key space, such that,

For all i, j from the set $\{1, 2, \dots, r\}$, $j \neq i$, $u_i(C) \neq u_j(C)$ for all values of C .

This can be achieved by fixing specific key bits: e.g., if $r = 8$ one can fix three key bits to the values 000, 001, ..., 111. Additional conditions might be imposed upon the mappings u_i , for example, to avoid the problems related to weak keys or complementation properties of the block cipher.

Function f_i :

Define the r functions f_i as follows:

$$f_i(X, Y) = e_{u_i(X)}(Y) \oplus Y, \quad 1 \leq i \leq r.$$

Linear mapping β :

Define the linear mapping β that takes as input a $2n$ -bit string $X = x_0 || x_1 || x_2 || x_3$ and maps it to a $2n$ -bit string $Y = y_0 || y_1 || y_2 || y_3$ as follows:

$$y_0 := x_0 \oplus x_3$$

$$y_1 := x_0 \oplus x_1 \oplus x_3$$

$$y_2 := x_1 \oplus x_2$$

$$y_3 := x_2 \oplus x_3$$

Here x_i and y_j are $n/2$ bit strings.

8.2 Parameter selection

The parameters L_1 and L_2 and L_H for the hash-function specified in this clause shall satisfy $L_1 = 4n$, $L_2 = 8n$, and L_H is equal to $2n$.

8.3 Padding method

The padding method for use with this hash-function shall be that specified in clause A.3 of ISO/IEC 10118-1:2000, such that $r = n$.