
**IT Security techniques — Hash-
functions —**

**Part 3:
Dedicated hash-functions**

*Techniques de sécurité IT — Fonctions de brouillage —
Partie 3: Fonctions de brouillage dédiées*





COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2018

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

	Page
Foreword	vii
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols	2
4.1 Symbols specified in ISO/IEC 10118-1	2
4.2 Symbols specific to this document	2
5 Requirements	4
6 Models for dedicated hash-functions	4
6.1 Use of models	4
6.2 Round-function model	4
6.3 Sponge model	5
7 Dedicated Hash-Function 1 (RIPEMD-160)	6
7.1 General	6
7.2 Parameters, functions and constants	7
7.2.1 Parameters	7
7.2.2 Byte ordering convention	7
7.2.3 Functions	7
7.2.4 Constants	8
7.2.5 Initializing value	10
7.3 Padding method	10
7.4 Description of the round-function	11
8 Dedicated Hash-Function 2 (RIPEMD-128)	12
8.1 General	12
8.2 Parameters, functions and constants	12
8.2.1 Parameters	12
8.2.2 Byte ordering convention	12
8.2.3 Functions	13
8.2.4 Constants	13
8.2.5 Initializing value	13
8.3 Padding method	13
8.4 Description of the round-function	13
9 Dedicated Hash-Function 3 (SHA-1)	15
9.1 General	15
9.2 Parameters, functions and constants	15
9.2.1 Parameters	15
9.2.2 Byte ordering convention	15
9.2.3 Functions	15
9.2.4 Constants	15
9.2.5 Initializing value	16
9.3 Padding method	16
9.4 Description of the round-function	16
10 Dedicated Hash-Function 4 (SHA-256)	17
10.1 General	17
10.2 Parameters, functions and constants	18
10.2.1 Parameters	18
10.2.2 Byte ordering convention	18
10.2.3 Functions	18
10.2.4 Constants	18
10.2.5 Initializing value	18
10.3 Padding method	19

10.4	Description of the round-function	19
11	Dedicated Hash-Function 5 (SHA-512)	20
11.1	General.....	20
11.2	Parameters, functions and constants	20
11.2.1	Parameters.....	20
11.2.2	Byte ordering convention.....	20
11.2.3	Functions.....	21
11.2.4	Constants.....	21
11.2.5	Initializing value.....	22
11.3	Padding method.....	22
11.4	Description of the round-function	22
12	Dedicated Hash-Function 6 (SHA-384)	23
12.1	General.....	23
12.2	Parameters, functions and constants	24
12.2.1	Parameters.....	24
12.2.2	Byte ordering convention.....	24
12.2.3	Functions.....	24
12.2.4	Constants.....	24
12.2.5	Initializing value.....	24
12.3	Padding method.....	24
12.4	Description of the round-function	24
13	Dedicated Hash-Function 7 (WHIRLPOOL)	25
13.1	General.....	25
13.2	Parameters, functions and constants	25
13.2.1	Parameters.....	25
13.2.2	Byte ordering convention.....	25
13.2.3	Functions.....	25
13.2.4	Constants.....	27
13.2.5	Initializing value.....	27
13.3	Padding method.....	27
13.4	Description of the round-function	27
14	Dedicated Hash-Function 8 (SHA-224)	28
14.1	General.....	28
14.2	Parameters, functions and constants	28
14.2.1	Parameters.....	28
14.2.2	Byte ordering convention.....	28
14.2.3	Functions.....	28
14.2.4	Constants.....	29
14.2.5	Initializing value.....	29
14.3	Padding method.....	29
14.4	Description of the round-function	29
15	Dedicated Hash-Function 9 (SHA-512/224)	29
15.1	General.....	29
15.2	Parameters, functions and constants	29
15.2.1	Parameters.....	29
15.2.2	Byte ordering convention.....	29
15.2.3	Functions.....	30
15.2.4	Constants.....	30
15.2.5	Initializing value.....	30
15.3	Padding method.....	30
15.4	Description of the round-function	30
16	Dedicated Hash-Function 10 (SHA-512/256)	30
16.1	General.....	30
16.2	Parameters, functions and constants	30
16.2.1	Parameters.....	30

16.2.2	Byte ordering convention	31
16.2.3	Functions	31
16.2.4	Constants	31
16.2.5	Initializing value	31
16.3	Padding method	31
16.4	Description of the round-function	31
17	Dedicated Hash-Function 11 (STREEBOG-512)	31
17.1	General	31
17.2	Parameters, functions and constants	32
17.2.1	Parameters	32
17.2.2	Byte ordering convention	32
17.2.3	Functions	32
17.2.4	Constants	34
17.2.5	Initializing value	34
17.3	Padding method	34
17.4	Description of the round-function	35
18	Dedicated Hash-Function 12 (STREEBOG-256)	36
18.1	General	36
18.2	Parameters, functions and constants	36
18.2.1	Parameters	36
18.2.2	Byte ordering convention	36
18.2.3	Functions	36
18.2.4	Constants	36
18.2.5	Initializing value	36
18.3	Padding method	37
18.4	Description of the round-function	37
19	Dedicated Hash-Function 13 (SHA3-224)	37
19.1	General	37
19.2	Parameters, functions and constants	37
19.2.1	Parameters	37
19.2.2	Byte ordering convention	37
19.2.3	Functions	37
19.3	Padding method	43
19.4	Description of a round-function	43
19.5	Output transformation	44
20	Dedicated Hash-Function 14 (SHA3-256)	44
20.1	General	44
20.2	Parameters, functions and constants	44
20.2.1	Parameters	44
20.2.2	Byte ordering convention	44
20.2.3	Functions	44
20.2.4	Constants	44
20.2.5	Initializing value	44
20.3	Padding method	45
20.4	Description of round-function	45
20.5	Output transformation	45
21	Dedicated Hash-Function 15 (SHA3-384)	45
21.1	General	45
21.2	Parameters, functions and constants	45
21.2.1	Parameters	45
21.2.2	Byte ordering convention	45
21.2.3	Functions	46
21.2.4	Constants	46
21.2.5	Initializing value	46
21.3	Padding method	46
21.4	Description of round-function	46

21.5	Output transformation.....	46
22	Dedicated Hash-Function 16 (SHA3-512)	46
22.1	General.....	46
22.2	Parameters, functions and constants.....	46
22.2.1	Parameters.....	46
22.2.2	Byte ordering convention.....	46
22.2.3	Functions.....	47
22.2.4	Constants.....	47
22.2.5	Initializing value.....	47
22.3	Padding method.....	47
22.4	Description of round-function.....	47
22.5	Output transformation.....	47
23	Dedicated Hash-Function 17 (SM3)	47
23.1	General.....	47
23.2	Parameters, functions and constants.....	48
23.2.1	Parameters.....	48
23.2.2	Byte ordering convention.....	48
23.2.3	Functions.....	48
23.2.4	Constants.....	48
23.2.5	Initializing value.....	48
23.3	Padding method.....	49
23.4	Description of the round-function.....	49
Annex A (normative) Object identifiers		51
Annex B (informative) Numerical examples		55
Annex C (informative) SHA-3 Extendable-Output Functions		245
Bibliography		399

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see <http://patents.iec.ch>).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

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

This fourth edition cancels and replaces the third edition (ISO/IEC 10118-3:2004), which has been technically revised. It also incorporates the Amendment ISO/IEC 10118-3:2004/Amd1:2006 and Technical Corrigendum ISO/IEC 10118-3:2004/Cor1:2011.

The main changes compared to the previous edition are as follows:

- SHA-3, STREEBOG and SM3 hash-functions have been included;
- SHA-3 extendable-output functions have been included;
- cautionary notes for hash-functions with short hash-codes have been added.

A list of all parts in the ISO/IEC 10118 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

IT Security techniques — Hash-functions —

Part 3: Dedicated hash-functions

1 Scope

This document specifies dedicated hash-functions, i.e. specially designed hash-functions. The hash-functions in this document are based on the iterative use of a round-function. Distinct round-functions are specified, giving rise to distinct dedicated hash-functions.

The use of Dedicated Hash-Functions 1, 2 and 3 in new digital signature implementations is deprecated.

NOTE As a result of their short hash-code length and/or cryptanalytic results, Dedicated Hash-Functions 1, 2 and 3 do not provide a sufficient level of collision resistance for future digital signature applications and they are therefore, only usable for legacy applications. However, for applications where collision resistance is not required, such as in hash-functions as specified in ISO/IEC 9797-2, or in key derivation functions specified in ISO/IEC 11770-6, their use is not deprecated.

Numerical examples for dedicated hash-functions specified in this document are given in [Annex B](#) as additional information. For information purposes, SHA-3 extendable-output functions are specified in [Annex C](#).

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 10118-1, *Information technology — Security techniques — Hash-functions — Part 1: General*