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

**Part 3:
Dedicated hash-functions**

*Technologies de l'information — Techniques de sécurité — Fonctions
de brouillage —*

Partie 3: Fonctions de brouillage dédiées

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/IEC 2003

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.org
Web www.iso.org

Published in Switzerland

Contents

	Page
Foreword.....	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols (and abbreviated terms)	2
4.1 Symbols specified in ISO/IEC 10118-1	2
4.2 Symbols specific to this part	2
5 Requirements	3
6 Model for dedicated hash-functions	4
7 Dedicated Hash-Function 1 (RIPEMD-160)	4
7.1 Parameters, functions and constants	4
7.1.1 Parameters	4
7.1.2 Byte ordering convention	4
7.1.3 Functions	5
7.1.4 Constants	5
7.1.5 Initializing value	6
7.2 Padding method	7
7.3 Description of the round-function	7
8 Dedicated Hash-Function 2 (RIPEMD-128)	8
8.1 Parameters, functions and constants	8
8.1.1 Parameters	8
8.1.2 Byte ordering convention	8
8.1.3 Functions	9
8.1.4 Constants	9
8.1.5 Initializing value	9
8.2 Padding method	9
8.3 Description of the round-function	9
9 Dedicated Hash-Function 3 (SHA-1)	10
9.1 Parameters, functions and constants	11
9.1.1 Parameters	11
9.1.2 Byte ordering convention	11
9.1.3 Functions	11
9.1.4 Constants	11
9.1.5 Initializing value	11
9.2 Padding method	12
9.3 Description of the round-function	12
10 Dedicated Hash-Function 4 (SHA-256)	13
10.1 Parameters, functions and constants	13
10.1.1 Parameters	13
10.1.2 Byte ordering convention	13
10.1.3 Functions	13
10.1.4 Constants	14
10.1.5 Initializing value	14
10.2 Padding method	14
10.3 Description of the round-function	14
11 Dedicated Hash-Function 5 (SHA-512)	15
11.1 Parameters, functions and constants	15