INTERNATIONAL STANDARD

ISO/IEC 10118-3

Third edition 2004-03-01

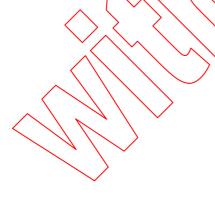
Information technology — Security techniques — Hash-functions —

Part 3:

Dedicated hash-functions

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

Partie 3: Fonctions de brouillage dédiées



ISO/IEC 10118-3:2004(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/IEC 2004

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

Con	tents	Page
Forew	vord	iv
Introd	luction	v
1	Scope	1
2	Normative references	1
3	Tarma and definitions	4
4 4.1 4.2	Symbols (and abbreviated terms) Symbols specified in ISO/IEC 10118-1 Symbols specific to this part Requirements	1 1 2
5	Requirements	3
6	Model for dedicated hash-functions	4
7 7.1 7.2 7.3	Dedicated Hash-Function 1 (RIPEMD-160) Parameters, functions and constants Padding method Description of the round-function	4
8 8.1 8.2 8.3	Requirements Model for dedicated hash-functions Dedicated Hash-Function 1 (RIPEMD-160) Parameters, functions and constants Padding method Description of the round-function Dedicated Hash-Function 2 (RIPEMD-128) Parameters, functions and constants Padding method Description of the round-function	8 9
9 9.1 9.2 9.3	Dedicated Hash-Function 3 (SHA-1) Parameters, functions and constants Padding method Description of the round-function	10 10 11
10 10.1 10.2 10.3	Dedicated Hash-Function 4 (SHA-256) Parameters, functions and constants Padding method Description of the round-function	13
11 11.1 11.2 11.3	Dedicated Hash-Function 5 (SHA-512) Parameters, functions and constants Padding method Description of the round-function	15
12 12.1 12.2 12.3	Dedicated Hash-Function 6 (SHA-384)	18
13 13.1 13.2 13.3	Dedicated Hash-Function 7 (WHIRLPOOL) Parameters, functions and constants Padding method Description of the round-function	19 21
Annex	x A (informative) Examples	23
Annex	x B (informative) Formal specifications	78
Annex	x C (normative) ASN.1 Module	91
	ography	

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, Rart 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.

ISO/IEC 10118-3 was prepared by Joint Technical Committee ISO/IEC JTC 1 Information technology, Subcommittee SC 27, IT Security techniques.

This third edition cancels and replaces the second edition (ISO/IEC 10118-3:2003), which has been technically revised.

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

- Part 1: General
- Part 2: Hash-functions using an n-bit block-cipher
- Part 3: Dedicated hash-functions
- Part 4: Hash-functions using modular arithmetic

Introduction

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this International Standard may involve the use of patents.

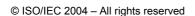
ISO and IEC take no position concerning the evidence, validity and scope of this patent right.

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 the ISO and IEC Information may be obtained from:

ISO/IEC JTC 1/SC 27 Standing Document 8 (SD8) "Patent Information"

Standing Document 8 (SD8) is publicly available at: http://www.ni.din.de/sc27

Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights other than those identified above. 150 and IEC shall not be held responsible for identifying any or all such patent rights.



Information technology — Security techniques — Hashfunctions —

Part 3:

Dedicated hash-functions

1 Scope

This part of ISO/IEC 10118 specifies dedicated hash-functions, i.e. specially designed hash-functions. The hash-functions in this part of ISO/IEC 10118 are based on the iterative use of a round-function. Seven distinct round-functions are specified, giving rise to distinct dedicated hash-functions.

The first and third dedicated hash-functions in Clauses 7 and 9 respectively provide hash-codes of lengths up to 160 bits; the second in Clause 8 provides hash-codes of lengths up to 128 bits; the fourth in Clause 10 provides hash-codes of lengths up to 256 bits; the sixth in Clause 12 provides hash-codes of a fixed length, 384 bits; and the fifth and seventh in Clauses 11 and 13 respectively provide hash-codes of lengths up to 512 bits.

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 10118-1:2000, Information technology - Security techniques - Hash-functions - Part 1: General