INTERNATIONAL STANDARD

ISO/IEC 10118-3

Third edition
2004-03-01

AMENDMENT 1
2006-02-15

Information technology — Security techniques — Hash-functions —

Part 3: Dedicated hash-functions

AMENDMENT 1: Dedicated Hash-Function 8 (SHA-224)

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

Partie 3: Fonctions de brouillage dédiées

AMENDEMENT 1: Fonction de brouillage dédiée 8 (SHA-224)

Reference number
ISO/IEC 10118-3:2004/Amd.1:2006(E)

Documents
Document Sharing Hub
© ISO/IEC 2006

Full document details: ISO_IEC 10118-3_2004_Amd 1_2006

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 2006

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

Documents
Document Sharing Hub

© ISO/IEC 2006 – All rights reserved

Full document details: ISO_IEC 10118-3_2004_Amd 1_2006

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.

Amendment 1 to ISO/IEC 10118-3:2004 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Amendment 1 to ISO/IEC 10118-3:2004 was written to serve two purposes.

First, with the inclusion of Dedicated Hash-Function 8 (SHA-224), ISO/IEC 10118-3:2004 now includes the complete family of SHA hash-functions. The description of SHA-224 is given in Clause 14. Test vectors for SHA-224 are given in A.8.

Second, it was noted that there were implementations of SHA-384 and SHA-512 in the field which correctly reproduced the test vector examples in ISO/IEC 10118-3:2004, yet still failed for inputs containing bytes that were not standard ASCII codes. In order to perform comprehensive testing of the SHA-224, SHA-256, SHA-384 and SHA-512 hash-functions, an extended set of test vectors is included for ISO/IEC 10118-3:2004 as a part of this amendment. This additional test vector information is given in A.9.

© ISO/IEC 2006 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 10118-3_2004_Amd 1_2006

Documents
Document Sharing Hub

Full document details: ISO_IEC 10118-3_2004_Amd 1_2006

Information technology — Security techniques — Hash-functions —

Part 3: Dedicated hash-functions

AMENDMENT 1: Dedicated Hash-Function 8 (SHA-224)

Page 22

Add the following after Figure 6.

14 Dedicated Hash-Function 8 (SHA-224)

In this clause we specify a padding method, an initialising value, and a round-function for use in the general model for hash-functions described in ISO/IEC 10118-1:2000. The padding method, initialising value and round-function specified here, when used in the above general model, together define Dedicated Hash-Function 8. This dedicated hash-function can be applied to all data strings D containing at most 2^{64}-1 bits.

The ISO/IEC hash-function identifier for Dedicated Hash-Function 8 is equal to 38 (hexadecimal).

NOTE Dedicated Hash-Function 8 defined in this clause is commonly called SHA-224, [2].

14.1 Parameters, functions and constants

14.1.1 Parameters

For this hash-function $L_1 = 512$, $L_2 = 256$ and $L_H = 224$.

14.1.2 Byte ordering convention

The byte ordering convention for this hash-function is the same as that for the hash-function of clause 10.

14.1.3 Functions

The functions for this hash-function are the same as those for the hash-function of clause 10.

14.1.4 Constants

The constants for this hash-function are the same as those for the hash-function of clause 10.

© ISO/IEC 2006 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 10118-3_2004_Amd 1_2006