

Third edition
2016-10-15

Information technology — Security techniques — Hash-functions —

Part 1: General

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

Partie 1: Généralités

Reference number
ISO/IEC 10118-1:2016(E)





COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2016, Published in Switzerland

All rights reserved. Unless otherwise specified, 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
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

This is a preview of "ISO/IEC 10118-1:2016". Click here to purchase the full version from the ANSI store.

Contents

	Page
Foreword	iv
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols and abbreviated terms	2
4.1 General symbols	2
4.2 Symbols specific to this document	3
4.3 Coding conventions	3
5 Requirements	3
6 General model for hash-functions	3
6.1 General	3
6.2 Hashing operation	4
6.2.1 General	4
6.2.2 Step 1 (padding)	4
6.2.3 Step 2 (splitting)	4
6.2.4 Step 3 (iteration)	4
6.2.5 Step 4 (output transformation)	4
6.3 Use of the general model	5
Annex A (normative) Padding methods	6
Annex B (normative) Criteria for submission of hash-functions for possible inclusion in ISO/IEC 10118 (all parts)	7
Annex C (informative) Security considerations	10
Bibliography	12

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.

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).

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

For an explanation on 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 the following URL: www.iso.org/iso/foreword.html.

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This third edition cancels and replaces the second edition (ISO/IEC 10118-1:2000), which has been technically revised.

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