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

American National Standard

INCITS/ISO/IEC 10118-1:2016 (2019)

(ISO/IEC 10118-1:2016, IDT)

Information technology -- Security techniques -- Hash-functions -- Part 1: General

Developed by

Where IT all begins

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

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.

Adopted by INCITS (InterNational Committee for Information Technology Standards) as an American National Standard.

Date of ANSI Approval: 11/22/2019

Published by American National Standards Institute,
25 West 43rd Street, New York, New York 10036

Copyright 2019 by Information Technology Industry Council
(ITI). All rights reserved.

These materials are subject to copyright claims of International Standardization Organization (ISO), International Electrotechnical Commission (IEC), American National Standards Institute (ANSI), and Information Technology Industry Council (ITI). Not for resale. No part of this publication may be reproduced in any form, including an electronic retrieval system, without the prior written permission of ITI. All requests pertaining to this standard should be submitted to ITI, 1101 K Street NW, Suite 610, Washington DC 20005.
Printed in the United States of America

© ITIC 2019 – All rights reserved

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

INTERNATIONAL **ISO/IEC**

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)

© ISO/IEC 2016

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

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

 © ISO/IEC 2016 – All rights reserved

This is a preview of "INCITS/ISO/IEC 10118...". 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**

© ISO/IEC 2016 – All rights reserved

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

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.

 © ISO/IEC 2016 – All rights reserved

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

Information technology — Security techniques — Hash-functions —

Part 1: General

1 Scope

ISO/IEC 10118 (all parts) specifies hash-functions and is therefore applicable to the provision of authentication, integrity and non-repudiation services. Hash-functions map strings of bits of variable (but usually upper bounded) length to fixed-length strings of bits, using a specified algorithm. They can be used for

— reducing a message to a short imprint for input to a digital signature mechanism, and

— committing the user to a given string of bits without revealing this string.

NOTE The hash-functions specified in ISO/IEC 10118 (all parts) do not involve the use of secret keys. However, these hash-functions may be used, in conjunction with secret keys, to build message authentication codes. Message Authentication Codes (MACs) provide data origin authentication as well as message integrity. Techniques for computing a MAC using a hash-function are specified in ISO/IEC 9797-2 [1].

This document contains definitions, symbols, abbreviations and requirements that are common to all the other parts of ISO/IEC 10118. The criteria used to select the algorithms specified in subsequent parts of ISO/IEC 10118 are defined in Annex B of this document.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

3.1
collision-resistant hash-function
hash-function satisfying the following property: it is computationally infeasible to find any two distinct inputs which map to the same output

Note 1 to entry: Computational feasibility depends on the specific security requirements and environment. Refer to Annex C.

3.2
data string
data
string of bits which is the input to a hash-function

© ISO/IEC 2016 – All rights reserved