INTERNATIONAL STANDARD

ISO/IEC 10118-1

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

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

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