
**Information security — Message
authentication codes (MACs) —**

**Part 2:
Mechanisms using a dedicated hash-
function**

*Sécurité de l'information — Codes d'authentification de message
(MAC) —*

Partie 2: Mécanismes utilisant une fonction de hachage dédiée





COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols and notation	3
5 Requirements	5
6 MAC Algorithm 1	6
6.1 General.....	6
6.2 Description of MAC Algorithm 1.....	7
6.2.1 General.....	7
6.2.2 Step 1 (key expansion).....	7
6.2.3 Step 2 (modification of the constants and the <i>IV</i>).....	7
6.2.4 Step 3 (hashing operation).....	8
6.2.5 Step 4 (output transformation).....	8
6.2.6 Step 5 (truncation).....	8
6.3 Efficiency.....	8
6.4 Computation of the constants.....	8
6.4.1 General.....	8
6.4.2 Dedicated hash-function 1 (RIPEMD-160).....	9
6.4.3 Dedicated hash-function 2 (RIPEMD-128).....	9
6.4.4 Dedicated hash-function 3 (SHA-1).....	10
6.4.5 Dedicated hash-function 4 (SHA-256).....	10
6.4.6 Dedicated hash-function 5 (SHA-512).....	10
6.4.7 Dedicated hash-function 6 (SHA-384).....	11
6.4.8 Dedicated hash-function 8 (SHA-224).....	11
6.4.9 Dedicated hash-function 17 (SM3).....	12
7 MAC Algorithm 2	12
7.1 General.....	12
7.2 Description of MAC Algorithm 2.....	12
7.2.1 General.....	12
7.2.2 Step 1 (key expansion).....	13
7.2.3 Step 2 (hashing operation).....	13
7.2.4 Step 3 (output transformation).....	13
7.2.5 Step 4 (truncation).....	13
7.3 Efficiency.....	13
8 MAC Algorithm 3	13
8.1 General.....	13
8.2 Description of MAC Algorithm 3.....	14
8.2.1 General.....	14
8.2.2 Step 1 (key expansion).....	14
8.2.3 Step 2 (modification of the constants and the <i>IV</i>).....	14
8.2.4 Step 3 (padding).....	15
8.2.5 Step 4 (application of the round-function).....	15
8.2.6 Step 5 (truncation).....	15
8.3 Efficiency.....	15
9 MAC Algorithm 4	15
9.1 General.....	15
9.2 Description of MAC Algorithm 4.....	16
9.3 Encoding and padding.....	16
9.3.1 Integer to byte encoding.....	16
9.3.2 String encoding.....	17