

INTERNATIONAL STANDARD

ISO/IEC 10118-4

First edition
1998-12-15

Information technology — Security techniques — Hash-functions —

Part 4: Hash-functions using modular arithmetic

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

Partie 4: Fonctions de hachage utilisant l'arithmétique modulaire



Contents

1	Scope	1
2	Normative reference	1
3	Terms and definitions.....	1
3.1	From ISO/IEC 10118-1	1
3.2	Unique to this part of ISO/IEC 10118.....	1
3.3	Conventions	2
4	Symbols and abbreviated terms.....	2
4.1	From ISO/IEC 10118-1	2
4.2	Unique to this part of ISO/IEC 10118.....	3
5	Requirements	4
6	Variables and values needed for the hash operation.....	4
6.1	The length of the hash-code and of the modulus.....	4
6.2	The modulus of the round-function	4
6.3	Initializing value	5
6.4	Exponent.....	5
6.5	Reduction-function prime number	5
7	Hashing procedure	5
7.1	Preparation of the data string.....	5
7.1.1	Padding the data string	5
7.1.2	Appending the length	5
7.1.3	Splitting the data string.....	5
7.1.4	Expansion	5
7.2	Application of the round-function	5

© ISO/IEC 1998

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 the publisher.

ISO/IEC Copyright Office • Case postale 56 • CH-1211 Genève 20 • Switzerland
Printed in Switzerland

7.3	The Reduction-function.....	6
7.3.1	Splitting the block H_q.....	6
7.3.2	Extending the data string.....	6
7.3.3	Processing the half-blocks	6
7.3.4	Reduction	6
8	Hash-functions.....	6
8.1	MASH-1	6
8.2	MASH-2	7
Annex A (informative)	Examples	9
Annex B (informative)	Additional Information.....	22
Annex C (informative)	Bibliography	23

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. 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.

International Standard ISO/IEC 10118-4 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC27, *IT Security techniques*.

ISO/IEC 10118 consists of the following parts, under the general title *Information technology – Security techniques – Hash-functions*:

- Part 1: *General*
- Part 2: *Hash-functions using an n-bit block cipher algorithm*
- Part 3: *Dedicated hash-functions*
- Part 4: *Hash-functions using modular arithmetic*

Annexes A, B and C of this part of ISO/IEC 10118 are for information only.

Information technology — Security techniques — Hash functions —

Part 4: Hash-functions using modular arithmetic

1 Scope

This part of ISO/IEC 10118 specifies two hash-functions which make use of modular arithmetic. These hash-functions, which are believed to be collision-resistant, compress messages of arbitrary but limited length to a hash-code whose length is determined by the length of the prime number used in the reduction-function defined in 7.3. Thus, the hash-code is easily scaled to the input length of any mechanism (e.g., signature algorithm, identification scheme).

The hash-functions specified in this part of ISO/IEC 10118, known as MASH-1 and MASH-2 (Modular Arithmetic Secure Hash) are particularly suitable for environments in which implementations of modular arithmetic of sufficient length are already available. The two hash-functions differ only in the exponent used in the round-function.

2 Normative reference

The following standard contains provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 10118. At the time of publication, the edition indicated was valid. All standards are subject to revision and parties to agreements based on this part of ISO/IEC 10118 are encouraged to investigate the possibility of applying the most recent edition of the standard indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO/IEC 10118-1: 1994, *Information technology – Security techniques – Hash-functions – Part 1: General*.