
**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