

INTERNATIONAL STANDARD

ISO/IEC 10118-1

First edition
1994-10-15

Information technology — Security techniques — Hash-functions —

Part 1: General

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

Partie 1: Généralités



Reference number
ISO/IEC 10118-1:1994(E)



Documents
Document Sharing Hub

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 10118-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *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*

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

© ISO/IEC 1994

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

Introduction

Hash-functions map arbitrary strings of bits to a given range. They can be used for

- reducing a message to a short imprint for input to a digital signature mechanism;
- committing the user to a given string of bits without revealing this string.

The purpose of ISO/IEC 10118 is to provide a variety of hash-functions which are suitable for security techniques. Hash-functions may be used for other purposes outside the scope of this International Standard, such as simulating a random number generator.

This page intentionally left blank