

INTERNATIONAL STANDARD

ISO/IEC
9797

First edition
1989-12-01

Data cryptographic techniques — Data integrity mechanism using a cryptographic check function employing a block cipher algorithm

*Techniques cryptographiques — Mécanisme d'intégrité des données utilisant une
fonction de contrôle cryptographique employant un algorithme d'encodage par
blocs*



Reference number
ISO/IEC 9797:1989

AVA Documents
Document Sharing Hub

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) together form a system for worldwide standardization as a whole. 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 approval before their acceptance as International Standards. They are approved in accordance with procedures requiring at least 75 % approval by the national bodies voting.

International Standard ISO/IEC 9797 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*.

© ISO/IEC 1989

All rights reserved. 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

The calculation described in this International Standard is similar to that used in ISO 8731-1 and in the American ANSI X9.9 standard, except that it is defined in terms of an algorithm using n -bit data blocks and an m -bit check value. Thus the calculations of cryptographic check-values described in ISO 8731 and ANSI X9.9 are subsets of this International Standard with $n=64$ and $m=32$ using DEA (see ANSI X3 : 1981).