

INTERNATIONAL
STANDARD

ISO/IEC
9797

Second edition
1994-04-15

**Information technology — Security
techniques — Data integrity mechanism
using a cryptographic check function
employing a block cipher algorithm**

iTeh STANDARD PREVIEW

(standards.iteh.ai)

*Technologies de l'information — Techniques de sécurité — Mécanisme
d'intégrité des données utilisant une fonction de contrôle cryptographique
employant un algorithme de chiffrement par bloc*

[https://standards.iteh.ai/catalog/standards/sis/2e0d95e1-788c-497f-b883-](https://standards.iteh.ai/catalog/standards/sis/2e0d95e1-788c-497f-b883-c77fd8636057/iso-iec-9797-1994)

[c77fd8636057/iso-iec-9797-1994](https://standards.iteh.ai/catalog/standards/sis/2e0d95e1-788c-497f-b883-c77fd8636057/iso-iec-9797-1994)



Reference number
ISO/IEC 9797:1994(E)

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 9797 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Sub-Committee SC27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 9797: 1989) which has been revised and extended to include an additional padding method, an additional method for the optional process as well as a new annex containing examples.

Annex A forms an integral part of this International Standard. Annexes B and C are for information only.

[ISO/IEC 9797:1994](https://standards.iteh.ai/catalog/standards/sist/2c0f95c1-788c-457f-b083-c77fd8636057/iso-iec-9797-1994)

<https://standards.iteh.ai/catalog/standards/sist/2c0f95c1-788c-457f-b083-c77fd8636057/iso-iec-9797-1994>

© 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

The mechanism specified in this International Standard is similar to that used in ISO 8731-1, ISO 9807 and in the 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, and that an additional padding method is specified.

The calculation of cryptographic check values as described in ISO 8731-1, ANSI X9.9 and ANSI X9.19 is a specific case of this International Standard when $n = 64$ and $m = 32$, when padding method 1 specified in 5.1 is used, and when DEA (see ANSI X3.92: 1981) is used.

iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO/IEC 9797:1994](https://standards.iteh.ai/catalog/standards/sist/2c0f95c1-788c-457f-b083-c77fd8636057/iso-iec-9797-1994)

<https://standards.iteh.ai/catalog/standards/sist/2c0f95c1-788c-457f-b083-c77fd8636057/iso-iec-9797-1994>

iTeh STANDARD PREVIEW
This page intentionally left blank
(standards.iteh.ai)

ISO/IEC 9797:1994

<https://standards.iteh.ai/catalog/standards/sist/2c0f95c1-788c-457f-b083-c77fd8636057/iso-iec-9797-1994>

Information technology - Security techniques - Data integrity mechanism using a cryptographic check function employing a block cipher algorithm

1 Scope

This International Standard specifies a method of using a key and an n -bit block cipher algorithm to calculate an m -bit cryptographic check value. This method can be used as a data integrity mechanism to detect that data has not been altered in an unauthorised manner. The strength of the data integrity mechanism is dependent on the key length and its secrecy, on the nature of the cryptographic algorithm, and on m , the length of the check value.

This International Standard can be applied to the security services of any security architecture, process, or application.

2 Normative references

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

ISO 7498-2: 1989, *Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture*.

ISO/IEC 10116: 1991, *Information technology - Modes of operation for an n -bit block cipher algorithm*.

3 Definitions and notation

3.1 Definitions

This International Standard makes use of the following terms defined in ISO 7498-2 and ISO/IEC 10116.

3.1.1 cryptographic check value: Information which is derived by performing a cryptographic transformation on the data unit.

3.1.2 data integrity: The property that data has not been altered or destroyed in an unauthorized manner.

3.1.3 n -bit block cipher algorithm: A block cipher algorithm with the property that plaintext blocks and ciphertext blocks are n bits in length.

3.2 Notation

This International Standard refers to the cryptographic check value as a Message Authentication Code (MAC).

In contexts where the terms “most significant bit/byte” and “least significant bit/byte” have a meaning, e.g., where strings of bits are treated as numerical values, then the leftmost bits of a block shall be the most significant.

4 Requirements

The length (m) of the MAC will be less than or equal to the block length (n). The result of the calculation and of any optional process is an information block of length n . The m leftmost bits of the final n -bit block form the MAC.

5 MAC calculation

5.1 Padding and blocking

The generation of a MAC requires the selection of one of two padding methods. The way in which the selection is made is beyond the scope of this International Standard.

Method 1

The data for which the MAC is to be calculated shall be appended with as few (possibly none) ‘0’ bits as necessary to obtain a data string whose length (in bits) is an integer multiple of n .

Method 2

The data for which the MAC is to be calculated shall be appended with a single '1' bit. The resulting data shall then be appended with as few (possibly none) '0' bits as necessary to obtain a data string whose length (in bits) is an integer multiple of n .

NOTE — If the length of data is not known by a verifier then padding method 2 should be used, since it permits a verifier to detect the addition or deletion of trailing '0' bits.

The resulting data is divided into n -bit blocks (D_1, D_2, \dots, D_q). The bits which are padded to the original data, according to the chosen padding method, are only used for calculating and verifying the MAC. Consequently, the padding bits (if any) need not be stored or transmitted with the data. The verifier shall know whether or not the padding bits have been stored or transmitted, and which padding method is in use.

5.2 The cryptographic key

The key should be randomly or pseudo-randomly generated. If the same algorithm is used for encipherment of the message, the key used for the calculation of the MAC should be different from that used for encipherment.

5.3 The initial stage

The MAC is calculated as illustrated in figure 1. [ISO/IEC 9797:1994](https://standards.iteh.ai/catalog/standards/sist/2c0f95c1-788c-457f-b083-c77103d1-057/iso-iec-9797-1994)

The input register is initialized with the first block (D_1). This input data (I_1) is passed through the algorithm (A), which uses a key (K) to produce n bits in the output register (O_1).

5.4 Subsequent stages

The next n bits of data (D_2) are bitwise exclusive or'ed with the n bits of the output register (O_1) and the result is loaded into the input register of the next stage (I_2). The contents of the input register (I_2) is passed through the algorithm (A), which uses the key (K) to produce n bits in the output register (O_2).

This operation continues until all blocks have been processed. The result will be the final output block (O_q).

5.5 Optional Process

The final output block (O_q) may be subjected to optional processing to increase the strength of the MAC. The optional process (if used) shall be selected from those specified in normative annex A.

5.6 The MAC

The m leftmost bits of the final n -bit block form the MAC.

NOTE — Use of the optional process specified in A.1 of annex A reduces the threat of exhaustive search attacks. In particular, this optional process is recommended when $m = n$.

(standards.iteh.ai)

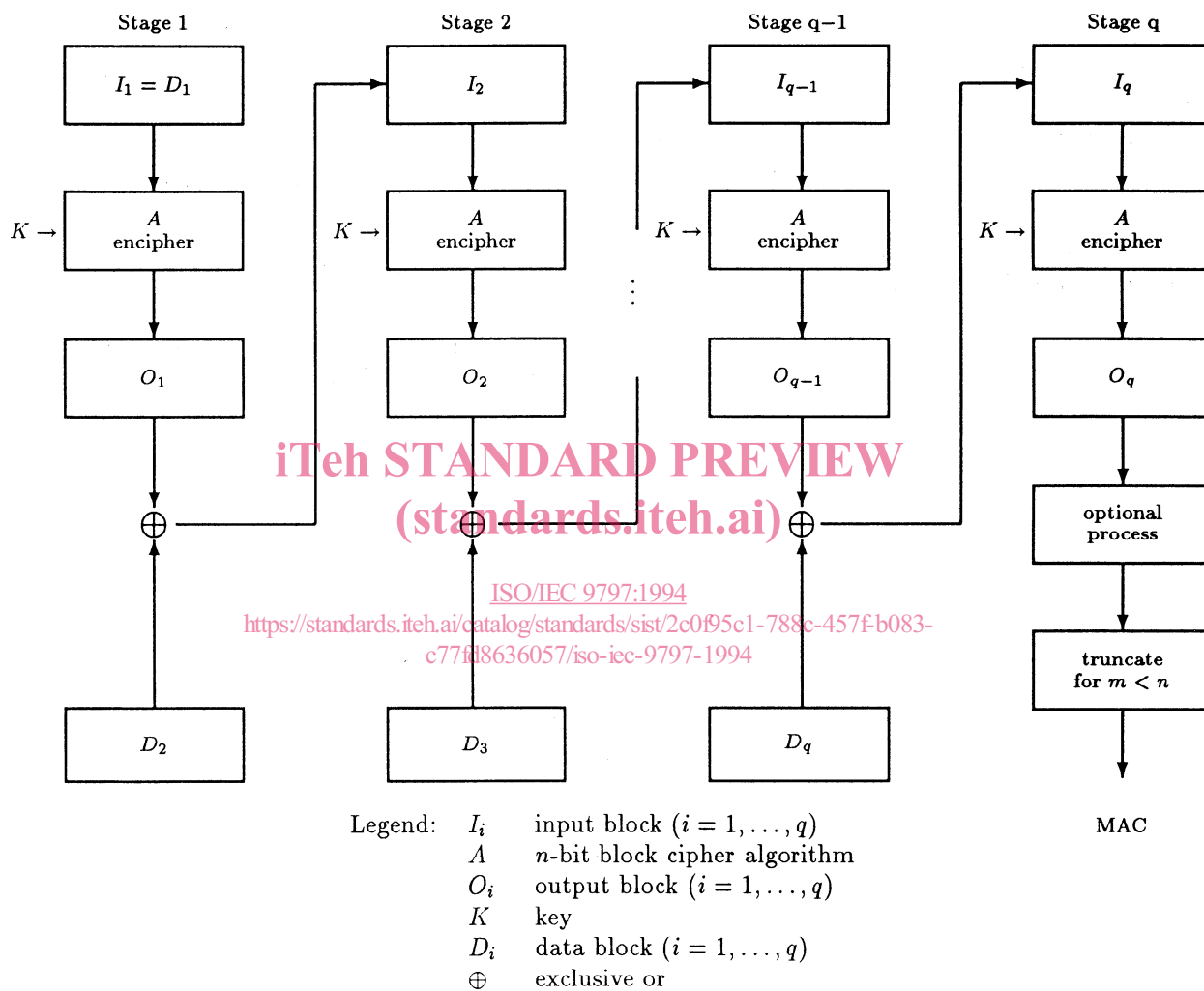


Figure 1 — The MAC calculation

Annex A (normative)

Optional Processes

A.1 Optional process 1

The following procedure specifies an optional process (see 5.5) which may be used in accordance with a pre-defined agreement between sender and receiver. This optional process increases the strength of the MAC with respect to exhaustive key search and chosen plaintext attacks.

In this optional process two cryptographic keys are used, which are denoted by (K) and (K_1) .

The n -bit block (O_q) is first generated using key (K) in the procedure specified in 5.3 and 5.4.

Two additional steps shall then be performed (see figure A.1):

- a) decipher the output (O_q) using key (K_1) to obtain (O'_q) ;
- b) encipher (O'_q) using key (K) to obtain (O''_q) .

This completes the optional process. The MAC is obtained as specified in 5.6.

iTeh STANDARD PREVIEW (standards.iteh.ai)

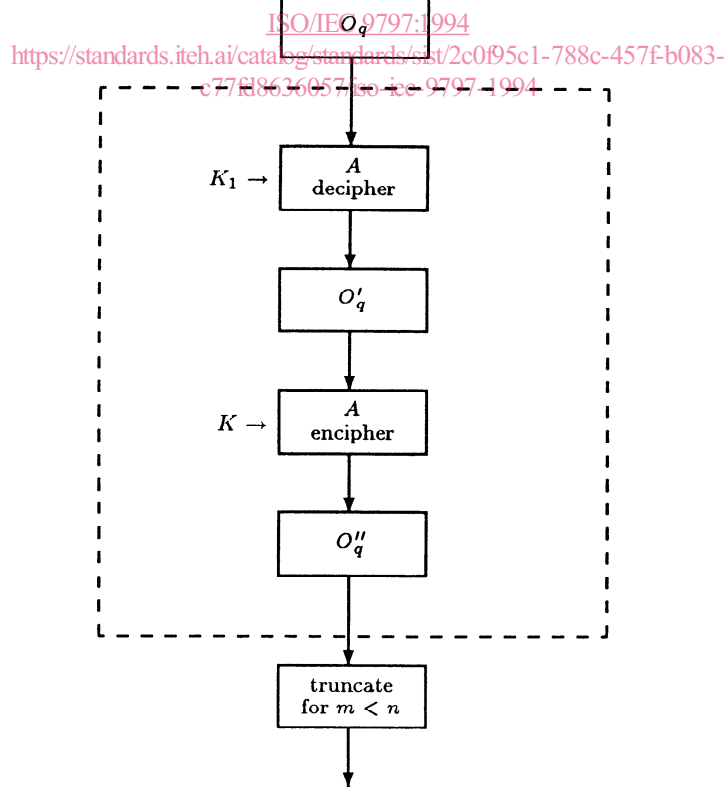


Figure A.1 — Optional process 1

A.2 Optional process 2

The following procedure specifies an optional process (see 5.5) which may be used in accordance with a pre-defined agreement between sender and receiver. This optional process increases the strength of the MAC with respect to chosen plaintext attacks.

In this optional process two cryptographic keys are used, which are denoted by (K) and (K_1) , where (K_1) may be derived from (K) .

NOTE — An example of how to derive (K_1) from (K) is to complement alternate blocks of four bits of (K) commencing with the first four bits.

The n -bit block (O_q) is first generated using key (K) in the procedure specified in 5.3 and 5.4.

An additional step shall then be performed (see figure A.2):

encipher the output (O_q) using key (K_1) to obtain (O'_q) .

This completes the optional process. The MAC is obtained as specified in 5.6.

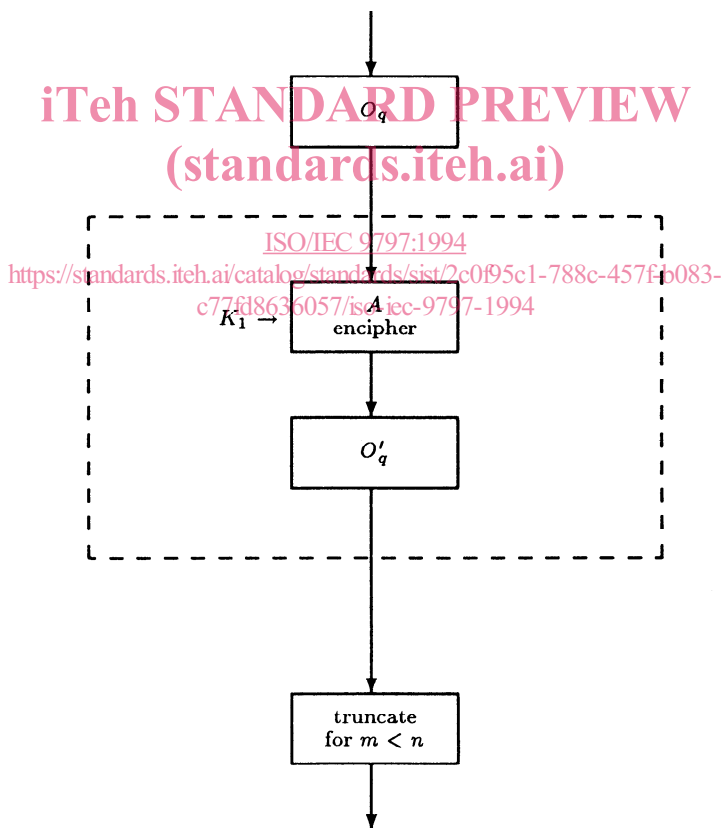


Figure A.2 — Optional process 2