INTERNATIONAL STANDARD

ISO/IEC 9797-1

Second edition
2011-03-01

Information technology — Security techniques — Message Authentication Codes (MACs) —

Part 1: **Mechanisms using a block cipher**

Technologies de l'information — Techniques de sécurité — Codes d'authentification de message (MAC) —

Partie 1: Mécanismes utilisant un chiffrement par blocs

Reference number
ISO/IEC 9797-1:2011(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. 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.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 9797-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 9797-1:1999), which has been technically revised. MAC Algorithms 5 and 6 of ISO/IEC 9797-1:1999, which consisted of two single CBC-MAC computations, have been replaced by two other MAC algorithms, which perform single CBC-MAC computations and which offer improved efficiency. Annex A on object identifiers has been added. The security analysis in Annex C has been updated and Annex D on the relationship to previous standards has been added.

ISO/IEC 9797 consists of the following parts, under the general title *Information technology — Security techniques — Message Authentication Codes (MACs)*:

- *Part 1: Mechanisms using a block cipher*

- *Part 2: Mechanisms using a dedicated hash-function*

- *Part 3: Mechanisms using a universal hash-function*

Further parts may follow.

Introduction

In an IT environment, it is often required that one can verify that electronic data has not been altered in an unauthorized manner and that one can provide assurance that a message has been originated by an entity in possession of the secret key. A MAC (Message Authentication Code) algorithm is a commonly used data integrity mechanism that can satisfy these requirements.

This part of ISO/IEC 9797 specifies six MAC algorithms that are based on an n-bit block cipher. They compute a short string as a function of a secret key and a message of variable length.

The strength of the data integrity mechanism and message authentication mechanism is dependent on the length (in bits) k^* and secrecy of the key, on the block length (in bits) n and strength of the block cipher, on the length (in bits) m of the MAC, and on the specific mechanism.

The first mechanism specified in this part of ISO/IEC 9797 is commonly known as CBC-MAC (CBC is an abbreviation of Cipher Block Chaining).

The other five mechanisms are variants of CBC-MAC. MAC Algorithms 2, 3, 5 and 6 apply a special transformation at the end of the processing. MAC Algorithm 6 is an optimized variant of MAC Algorithm 2. MAC Algorithm 5 uses the minimum number of encryptions. MAC Algorithm 5 requires only a single block cipher key setup but it needs a longer internal key. MAC Algorithm 4 applies a special transformation at both the beginning and the end of the processing; this algorithm is recommended for use in applications which require that the key length of the MAC algorithm be twice that of the block cipher.

Information technology — Security techniques — Message Authentication Codes (MACs) —

Part 1: Mechanisms using a block cipher

1 Scope

This part of ISO/IEC 9797 specifies six MAC algorithms that use a secret key and an n-bit block cipher to calculate an m-bit MAC.

This part of ISO/IEC 9797 can be applied to the security services of any security architecture, process, or application.

Key management mechanisms are outside the scope of this part of ISO/IEC 9797.

This part of ISO/IEC 9797 specifies object identifiers that can be used to identify each mechanism in accordance with ISO/IEC 8825-1. Numerical examples and a security analysis of each of the six specified algorithms are provided, and the relationship of this part of ISO/IEC 9797 to previous standards is explained.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 18033-3, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*