INTERNATIONAL STANDARD

ISO/IEC 10118-3

First edition
1998-06-01

Information technology — Security techniques — Hash-functions —

Part 3:
Dedicated hash-functions

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

Partie 3: Fonctions de hachage dédiées

Reference number
ISO/IEC 10118-3:1998(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 JTC1. 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 10118–3 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Sub-Committee SC27, *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*

— *Part 3: Dedicated hash-functions*

— *Part 4: Hash-functions using modular arithmetic*

Further parts may follow.

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

Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions

1 Scope

This part of ISO/IEC 10118 specifies dedicated hash-functions, i.e. specially designed hash-functions. The hash-functions in this part of ISO/IEC 10118 are based on the iterative use of a round-function. Three distinct round-functions are specified, giving rise to distinct dedicated hash-functions. The first and third provide hash-codes of lengths up to 160 bits, and the second provides hash-codes of lengths up to 128 bits.

2 Normative reference

The following standard contains provisions which, through reference in the text, constitute provisions of this part of ISO/IEC 10118. At the time of publication, the edition indicated was valid. All standards are subject to revision and parties to agreements based on this part of ISO/IEC 10118 are encouraged to investigate the possibility of applying the most recent edition of the standard indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO/IEC 10118–1: 1994, *Information technology — Security techniques — Hash-functions — Part 1: General.*

3 Definitions

For the purposes of this part of ISO/IEC 10118, the definitions given in ISO/IEC 10118–1 and the following definitions apply.

3.1 block: A bit-string of length L_1, i.e. the length of the first input to the round-function.

3.2 hash-function identifier: A byte identifying a specific hash-function.

3.3 round-function: A function $\phi(.,.)$ that transforms two binary strings of lengths L_1 and L_2 to a binary string of length L_2. It is used iteratively as part of a hash-function, where it combines a data string of length L_1 with the previous output of length L_2.

3.4 word: A string of 32 bits.

4 Symbols and notation

This part of ISO/IEC 10118 makes use of the following symbols and notation defined in ISO/IEC 10118–1.

D A data string to be input to the hash-function.

H Hash-code.

IV Initializing value.

L_X Length (in bits) of a bit-string X.

$X \oplus Y$ Exclusive-or of bit-strings X and Y.

For the purpose of this Part of ISO/IEC 10118, the following symbols and notation apply:

a_i, a'_i Sequences of indices used in specifying a round-function.

B_i A byte.

C_i, C'_i Constant words used in the round-functions.