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)

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.

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

Information technology - Security techniques - Hash-functions

Part 1 : General

1 Scope

ISO/IEC 10118 specifies hash-functions and is therefore applicable to the provision of authentication, integrity and non-repudiation services.

NOTE - In contrast to the calculation of a Message Authentication Code (MAC), the goal of which is to ensure authentication of a message employing a secret key, the generation of a hash-code does not involve a secret key. For the calculation of the MAC the user is referred to ISO/IEC 9797 [1].

This part of ISO/IEC 10118 contains definitions, symbols, abbreviations and requirements which are common to all the other parts of ISO/IEC 10118.

2 Definitions

For the purposes of ISO/IEC 10118, the following definitions apply.

2.1 collision-resistant hash-function: A hash-function satisfying the following property.

- it is computationally infeasible to find any two distinct inputs which map to the same output.

NOTE - Computational feasibility depends on the user's specific security requirements and environment.

2.2 data string (data): The string of bits which is the input to a hash-function.

2.3 hash-code: The string of bits which is the output of a hash-function.

NOTE - The literature of the subject contains a variety of terms which have the same or similar meaning as hash-code. Modification Detection Code, Manipulation Detection Code, digest, hash-result, hash-value and imprint are some examples.

2.4 hash-function: A function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties.

- it is computationally infeasible to find for a given output an input which maps to this output;
- it is computationally infeasible to find for a given input a second input which maps to the same output.

NOTES

1 - The literature of the subject contains a variety of terms which have the same or similar meaning as hash-function. Compressed encoding and condensing function are some examples.

2 - Computational feasibility depends on the user's specific security requirements and environment.

2.5 initializing value: A value used in defining the starting point of a hash-function.

2.6 padding: Appending extra bits to a data string.

3 Symbols and notation

Throughout ISO/IEC 10118, the following symbols and abbrevations are used :

D	Data
H	Hash-code
IV	Initializing value
L_X	Length (in bits) of a string of bits X
$X \| Y$	Concatenation of strings of bits X and Y in that order
$X \oplus Y$	Exclusive-or of strings of bits X and Y

All strings of bits are written with the first bit in the leftmost position. 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 lefmost bits of a block shall be the most significant.

4 Requirements

The use of a hash-function requires that the parties involved shall operate upon precisely the same data, even though the representation may be different in each entity's environment. This may require one or more of the entities to convert the data into an agreed representation prior to applying a hash-function.

Some of the hash-functions specified in ISO/IEC 10118 use one (or more) initializing value(s). In this case, provisions shall be made in order to ensure that the entity which produces the hash-code and the one which checks it shall use the same initializing value(s). Examples of such provisions are presented in annex A.

Some of the hash-functions specified in ISO/IEC 10118 require padding, so that the data string is of the required length. The padding methods may be specified in each part of ISO/IEC 10118 where padding is needed. Examples of such methods are presented in annex B.

Annex A
(informative)

Guidance on the initializing value

An initializing value can be chosen in a variety of ways; it can, for example, be :

- a fixed value;

- a value randomly chosen at each execution of the hash-function;

- a value depending on one or more characteristics of the data to be hashed (length, type, etc.).

Clause 4 of this part of ISO/IEC 10118 states that provisions shall be made in order to ensure that the entity which produces the hash-code and the one which checks it use the same initializing value. This can be achieved by using a fixed value. Where the initializing value is not previously known to the checking entity, it is to be conveyed in a manner which ensures its integrity. For example, the *IV* may be concatenated with the hash-code for input to a digital signature mechanism.

Annex B
(informative)

Padding methods

The calculation of a hash-code, as specified in other parts of ISO/IEC 10118, may require the selection of a padding method. Two methods are presented in this annex. If the length of the data for which the hash-code is to be calculated is not known by a verifier of the hash-code, then padding method 2 is recommended. 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.

B.1 Method 1

The data for which the hash-code is to be calculated are appended with as few (possibly no) '0' bits as are necessary to obtain the required length.

B.2 Method 2

The data for which the hash-code is to be calculated are appended with a single '1' bit. The resulting data are then appended with as few (possible no) '0' bits as are necessary to obtain the required length.

NOTE - Method 2 always requires the addition of at least one padding bit.

Annex C
(informative)

Bibliography

[1] ISO/IEC 9797: 1994, *Information technology - Security techniques - Data integrity mechanism using a cryptographic check function employing a block cipher algorithm.*