AS ISO/IEC 10118.3:2019

Australian STANDARD

IT Security techniques — Hash-functions

Part 3: Dedicated hash-functions

STANDARDS Australia

AS ISO/IEC 10118.3:2019

This Australian Standard® was prepared by IT-005, Financial Transaction Systems. It was approved on behalf of the Council of Standards Australia on 5 August 2019.

This Standard was published on 28 August 2019.

The following are represented on Committee IT-005:

Australian Payments Network
EFTPOS Payments Australia
New Payments Platform Australia

Additional Interests

American Express
ANZ Banking Group
Coles Group
Commonwealth Bank of Australia
Diebold Nixdorf
Eracom Technologies Australia
FIS Global
Gemalto
Mag-Tek
National Australia Bank
Pacific Research
SWIFT
Thales eSecurity
Triton Systems of Delaware LLC
UL Transaction Security
Westpac Banking Corporation
Woolworths Group

This Standard was issued in draft form for comment as DR AS ISO/IEC 10118.3:2019.

Keeping Standards up-to-date

Ensure you have the latest versions of our publications and keep up-to-date about Amendments, Rulings, Withdrawals, and new projects by visiting:
www.standards.org.au

ISBN 978 1 76072 575 4

Australian STANDARD

IT Security techniques — Hash-functions

Part 3: Dedicated hash-functions

Originated as AS 2805.13.2—2000.
Revised and redesignated as AS ISO/IEC 10118.3:2019.

Preface

This Standard was prepared by the Standards Australia Committee IT-005, Financial Transaction Systems, to supersede AS 2805.13.2—2000, *Electronic funds transfer — Requirements for interfaces, Part 13.2: Secure hash functions — MD5.*

The objective of this Standard is to specify dedicated hash-functions, i.e. specially designed hash-functions. The hash-functions in this document are based on the iterative use of a round-function. Distinct round-functions are specified, giving rise to distinct dedicated hash-functions.

This Standard is identical with, and has been reproduced from, ISO/IEC 10118-3:2018, *IT Security techniques — Hash-functions — Part 3: Dedicated hash-functions*.

As this document has been reproduced from an International Standard, a full point substitutes for a comma when referring to a decimal marker.

Australian or Australian/New Zealand Standards that are identical adoptions of international normative references may be used interchangeably. Refer to the online catalogue for information on specific Standards.

The terms “normative” and “informative” are used in Standards to define the application of the appendices or annexes to which they apply. A “normative” appendix or annex is an integral part of a Standard, whereas an “informative” appendix or annex is only for information and guidance.

Contents

Preface ii
Foreword vii
1 Scope 1
2 Normative references 1
3 Terms and definitions 1
4 Symbols 2
4.1 Symbols specified in ISO/IEC 10118-1 2
4.2 Symbols specific to this document 2
5 Requirements 4
6 Models for dedicated hash-functions 4
6.1 Use of models 4
6.2 Round-function model 4
6.3 Sponge model 5
7 Dedicated Hash-Function 1 (RIPEMD-160) 6
7.1 General 6
7.2 Parameters, functions and constants 6
7.2.1 Parameters 6
7.2.2 Byte ordering convention 6
7.2.3 Functions 7
7.2.4 Constants 7
7.2.5 Initializing value 9
7.3 Padding method 9
7.4 Description of the round-function 10
8 Dedicated Hash-Function 2 (RIPEMD-128) 11
8.1 General 11
8.2 Parameters, functions and constants 11
8.2.1 Parameters 11
8.2.2 Byte ordering convention 11
8.2.3 Functions 12
8.2.4 Constants 12
8.2.5 Initializing value 12
8.3 Padding method 12
8.4 Description of the round-function 12
9 Dedicated Hash-Function 3 (SHA-1) 14
9.1 General 14
9.2 Parameters, functions and constants 14
9.2.1 Parameters 14
9.2.2 Byte ordering convention 14
9.2.3 Functions 14
9.2.4 Constants 14
9.2.5 Initializing value 15
9.3 Padding method 15
9.4 Description of the round-function 15
10 Dedicated Hash-Function 4 (SHA-256) 16
10.1 General 16
10.2 Parameters, functions and constants 17
10.2.1 Parameters 17
10.2.2 Byte ordering convention 17
10.2.3 Functions 17
10.2.4 Constants 17

10.2.5 Initializing value 17
10.3 Padding method 18
10.4 Description of the round-function 18

11 Dedicated Hash-Function 5 (SHA-512) 19
11.1 General 19
11.2 Parameters, functions and constants 19
11.2.1 Parameters 19
11.2.2 Byte ordering convention 19
11.2.3 Functions 20
11.2.4 Constants 20
11.2.5 Initializing value 21
11.3 Padding method 21
11.4 Description of the round-function 21

12 Dedicated Hash-Function 6 (SHA-384) 22
12.1 General 22
12.2 Parameters, functions and constants 23
12.2.1 Parameters 23
12.2.2 Byte ordering convention 23
12.2.3 Functions 23
12.2.4 Constants 23
12.2.5 Initializing value 23
12.3 Padding method 23
12.4 Description of the round-function 23

13 Dedicated Hash-Function 7 (WHIRLPOOL) 24
13.1 General 24
13.2 Parameters, functions and constants 24
13.2.1 Parameters 24
13.2.2 Byte ordering convention 24
13.2.3 Functions 24
13.2.4 Constants 26
13.2.5 Initializing value 26
13.3 Padding method 26
13.4 Description of the round-function 26

14 Dedicated Hash-Function 8 (SHA-224) 27
14.1 General 27
14.2 Parameters, functions and constants 27
14.2.1 Parameters 27
14.2.2 Byte ordering convention 27
14.2.3 Functions 27
14.2.4 Constants 28
14.2.5 Initializing value 28
14.3 Padding method 28
14.4 Description of the round-function 28

15 Dedicated Hash-Function 9 (SHA-512/224) 28
15.1 General 28
15.2 Parameters, functions and constants 28
15.2.1 Parameters 28
15.2.2 Byte ordering convention 28
15.2.3 Functions 29
15.2.4 Constants 29
15.2.5 Initializing value 29
15.3 Padding method 29
15.4 Description of the round-function 29

16 Dedicated Hash-Function 10 (SHA-512/256) 29
16.1 General 29

16.2 Parameters, functions and constants 29
16.2.1 Parameters 29
16.2.2 Byte ordering convention 30
16.2.3 Functions 30
16.2.4 Constants 30
16.2.5 Initializing value 30
16.3 Padding method 30
16.4 Description of the round-function 30

17 Dedicated Hash-Function 11 (STREEBOG-512) 30
17.1 General 30
17.2 Parameters, functions and constants 31
17.2.1 Parameters 31
17.2.2 Byte ordering convention 31
17.2.3 Functions 31
17.2.4 Constants 33
17.2.5 Initializing value 33
17.3 Padding method 33
17.4 Description of the round-function 34

18 Dedicated Hash-Function 12 (STREEBOG-256) 35
18.1 General 35
18.2 Parameters, functions and constants 35
18.2.1 Parameters 35
18.2.2 Byte ordering convention 35
18.2.3 Functions 35
18.2.4 Constants 35
18.2.5 Initializing value 35
18.3 Padding method 36
18.4 Description of the round-function 36

19 Dedicated Hash-Function 13 (SHA3-224) 36
19.1 General 36
19.2 Parameters, functions and constants 36
19.2.1 Parameters 36
19.2.2 Byte ordering convention 36
19.2.3 Functions 36
19.3 Padding method 42
19.4 Description of round-function 42
19.5 Output transformation 43

20 Dedicated Hash-Function 14 (SHA3-256) 43
20.1 General 43
20.2 Parameters, functions and constants 43
20.2.1 Parameters 43
20.2.2 Byte ordering convention 43
20.2.3 Functions 43
20.2.4 Constants 43
20.2.5 Initializing value 43
20.3 Padding method 44
20.4 Description of round-function 44
20.5 Output transformation 44

21 Dedicated Hash-Function 15 (SHA3-384) 44
21.1 General 44
21.2 Parameters, functions and constants 44
21.2.1 Parameters 44
21.2.2 Byte ordering convention 44
21.2.3 Functions 45
21.2.4 Constants 45
21.2.5 Initializing value 45

21.3 Padding method 45
21.4 Description of round-function 45
21.5 Output transformation 45

22 Dedicated Hash-Function 16 (SHA3-512) 45
22.1 General 45
22.2 Parameters, functions and constants 45
22.2.1 Parameters 45
22.2.2 Byte ordering convention 45
22.2.3 Functions 46
22.2.4 Constants 46
22.2.5 Initializing value 46
22.3 Padding method 46
22.4 Description of round-function 46
22.5 Output transformation 46

23 Dedicated Hash-Function 17 (SM3) 46
23.1 General 46
23.2 Parameters, functions and constants 47
23.2.1 Parameters 47
23.2.2 Byte ordering convention 47
23.2.3 Functions 47
23.2.4 Constants 47
23.2.5 Initializing value 47
23.3 Padding method 48
23.4 Description of the round-function 48

Annex A (normative) **Object identifiers 50**

Annex B (informative) **Numerical examples 54**

Annex C (informative) **SHA-3 Extendable-Output Functions 244**

Bibliography 398

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see http://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

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

This fourth edition cancels and replaces the third edition (ISO/IEC 10118-3:2004), which has been technically revised. It also incorporates the Amendment ISO/IEC 10118-3:2004/Amd1:2006 and Technical Corrigendum ISO/IEC 10118-3:2004/Cor1:2011.

The main changes compared to the previous edition are as follows:

— SHA-3, STREEBOG and SM3 hash-functions have been included;

— SHA-3 extendable-output functions have been included;

— cautionary notes for hash-functions with short hash-codes have been added.

A list of all parts in the ISO/IEC 10118 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

NOTES

Australian Standard®

IT Security techniques — Hash-functions

Part 3: Dedicated hash-functions

1 Scope

This document specifies dedicated hash-functions, i.e. specially designed hash-functions. The hash-functions in this document are based on the iterative use of a round-function. Distinct round-functions are specified, giving rise to distinct dedicated hash-functions.

The use of Dedicated Hash-Functions 1, 2 and 3 in new digital signature implementations is deprecated.

NOTE As a result of their short hash-code length and/or cryptanalytic results, Dedicated Hash-Functions 1, 2 and 3 do not provide a sufficient level of collision resistance for future digital signature applications and they are therefore, only usable for legacy applications. However, for applications where collision resistance is not required, such as in hash-functions as specified in ISO/IEC 9797-2, or in key derivation functions specified in ISO/IEC 11770-6, their use is not deprecated.

Numerical examples for dedicated hash-functions specified in this document are given in Annex B as additional information. For information purposes, SHA-3 extendable-output functions are specified in Annex C.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 10118-1, *Information technology — Security techniques — Hash-functions — Part 1: General*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 10118-1 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

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

3.2
word
string of bits

3.3
circulant matrix
matrix with the property that each row, apart from the first, consists of the right cyclic shift by one position of the row immediately above it

3.4
abelian group
group $(G, *)$ such that $a*b = b*a$ for every a and b in G