Australian Standard®

Information technology—Security techniques—Hash-functions

Part 2: Hash-functions using an *n*-bit block cipher

This Australian Standard® was prepared by Committee IT-012, Information Systems, Security and Identification. It was approved on behalf of the Council of Standards Australia on 23 June 2006.
This Standard was published on 2 August 2006.

The following are represented on Committee IT-012:

- Attorney General's Department
- Australian Association of Permanent Building Societies
- Australian Bankers Association
- Australian Chamber Commerce and Industry
- Australian Electrical and Electronic Manufacturers Association
- Certification Forum of Australia
- Department of Defence
- Department of Social Welfare, NZ
- Government Communications Security Bureau, NZ
- Internet Industry Association
- NSW Police Service
- New Zealand Defence Force
- Reserve Bank of Australia

This Standard was issued in draft form for comment as DR 06300.

Standards Australia wishes to acknowledge the participation of the expert individuals that contributed to the development of this Standard through their representation on the Committee and through public comment period.

Keeping Standards up-to-date

Australian Standards® are living documents that reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued.

Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments that may have been published since the Standard was published.

Detailed information about Australian Standards, drafts, amendments and new projects can be found by visiting **www.standards.org.au**

Standards Australia welcomes suggestions for improvements, and encourages readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at **mail@standards.org.au**, or write to Standards Australia, GPO Box 476, Sydney, NSW 2001.

Australian Standard®

Information technology—Security techniques—Hash-functions

Part 2: Hash-functions using an *n*-bit block cipher

First published as AS ISO/IEC 10118.2—2006.

Published by Standards Australia GPO Box 476, Sydney, NSW 2001, Australia

ISBN 0 7337 7664 7

PREFACE

This Standard was prepared by the Standards Australia Committee IT-012, Information Systems, Security and Identification.

The objective of this Standard is to specify hash-functions which make use of an n-bit block cipher algorithm. They are therefore suitable for an environment in which such an algorithm is already implemented.

Four hash-functions are specified. The first provides hash-codes of length smaller than or equal to n, where *n* is the block-length of the algorithm used. The second provides hash-codes of length less than or equal to 2*n*; the third provides hash-codes of length equal to 2*n*, the fourth provides hash-codes of length 3*n*. All four of the hash-functions specified in this part of AS 10118 conform to the general model specified in AS 10118.1.

This Standard is identical with, and has been reproduced from ISO/IEC 10118-2:2000, *Information technology—Security techniques—Hash-functions*—Part 2: *Hash-functions using an n-bit block cipher*.

As this Standard is reproduced from an international standard, the following applies:

(a) Its number appears on the cover and title page while the international standard number appears only on the cover.

(b) In the source text 'this part of ISO/IEC 10118' should read 'this Australian Standard'.

(c) A full point substitutes for a comma when referring to a decimal marker.

The term 'informative' has been used in this Standard to define the application of the annex to which it applies. A 'informative' annex is an integral part of a Standard.

CONTENTS

Page

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 Symbols and abbreviated terms **1**

5 Use of the general model **2**

6 Hash-function one **2**
6.1 Parameter selection **2**
6.2 Padding method **2**
6.3 Initializing value **2**
6.4 Round-function **2**
6.5 Output transformation **3**

7 Hash-function two **3**
7.1 Parameter selection **3**
7.2 Padding method **3**
7.3 Initializing value **3**
7.4 Round-function **4**
7.5 Output transformation **5**

8 Hash-function three **5**
8.1 General **5**
8.2 Parameter selection **5**
8.3 Padding method **5**
8.4 Initializing value **6**
8.5 Round-function **6**
8.6 Output transformation **8**

9 Hash-function four **8**
9.1 General **8**
9.2 Parameter selection **8**
9.3 Padding method **8**
9.4 Initializing value **8**
9.5 Round-function **8**
9.6 Output transformation **10**

Annex A (informative) **Use of DEA** **11**

Annex B (informative) **Example** **14**

Bibliography **19**

INTRODUCTION

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this part of ISO/IEC 10118 may involve the use of a patent concerning the "Data Authentication Using Modification Detection Codes Based on a Public One Way Encryption Function," (U.S. Patent 4,908,861 issued 1990-03-13).

ISO and IEC take no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured ISO and IEC that he is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with ISO and IEC. Information may be obtained from:

Director of Licensing
International Business Machnies Corporation
500 Columbus Avenue
Thornwood, NY 10594
U.S.A.

Attention is drawn to the possibility that some of the elements of this part of ISO/IEC 10118 may be the subject of patent rights other than those identified above. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

AUSTRALIAN STANDARD

Information technology — Security techniques — Hash-functions —

Part 2:
Hash-functions using an *n*-bit block cipher

1 Scope

This part of ISO/IEC 10118 specifies hash-functions which make use of an *n*-bit block cipher algorithm. They are therefore suitable for an environment in which such an algorithm is already implemented.

Four hash-functions are specified. The first provides hash-codes of length small... than or equal to *n*, where *n* is the block-length of the algorithm used. The second provides hash-codes of leng... less than or equal to 2*n*; the third provides hash-codes of length equal to 2*n*; and the fourth provides hash-codes of length 3*n*. All four of the hash-functions specified in this part of ISO/IEC 10118 conform to the general model specified in ISO/IEC 10118-1.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 10118. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of ISO/IEC 10118 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO/IEC 10116:1997, *Information technology — Security techniques — Modes of operation for an n-bit block cipher.*

ISO/IEC 10118-1:2000, *Information technology — Security techniques — Hash-functions — Part 1: General.*

3 Terms and definitions

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

3.1
***n*-bit block cipher**
a block cipher with the property that plaintext blocks and ciphertext blocks are *n* bits in length (see ISO/IEC 10116)

4 Symbols and abbreviated terms

For the purposes of this part of ISO/IEC 10118, the symbols and abbreviations given in ISO/IEC 10118-1 and the following apply:

e *n*-bit block cipher algorithm (see ISO/IEC 10116)

K Key for the algorithm *e* (see ISO/IEC 10116)