AS ISO/IEC 10118.4—2006

Australian Standard®

Information technology—Security techniques—Hash-functions

Part 4: Hash-functions using modular arithmetic

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 062301.

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Standards may also be withdrawn.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 4: Hash-functions using modular arithmetic

First published as AS ISO/IEC 10118.4—2006.

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

ISBN 0 7337 7667 1

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 two hash-functions which make use of modular arithmetic. These hash-functions, which are believed to be collision-resistant, compress message of arbitrary but limited length to a hash-code whose length is determined by the length of the prime number used in the reduction-function defined in Clause 7.3. Thus, the hash-code is easily scaled to the input length of any mechanism (e.g. signature algorithm, identification scheme).

This Standard is identical with, and has been reproduced from ISO/IEC 10118-4:1998, *Information technology—Security techniques—Hash-functions*—Part 4: *Hash-functions using modular arithmetic*.

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. An 'informative' annex is only for information and guidance.

References to International Standards should be replaced by references to Australian or Australian/New Zealand Standards, as follows:

Reference to International Standard		*Australian Standard*	
ISO/IEC		AS ISO/IEC	
10118	Information technology—Security techniques—Hash functions	10118	Information technology—Security techniques—Hash functions
10118-1	Part 1: General	10118.1	Part 1: General

CONTENTS

Page

Page

AUSTRALIAN STANDARD

Information technology — Security techniques — Hash functions —

Part 4:
Hash-functions using modular arithmetic

1 Scope

This part of ISO/IEC 10118 specifies two hash-functions which make use of modular arithmetic. These hash-functions, which are believed to be collision-resistant, compress messages of arbitrary but limited length to a hash-code whose length is determined by the length of the prime number used in the reduction-function defined in 7.3. Thus, the hash-code is easily scaled to the input length of any mechanism (e.g., signature algorithm, identification scheme).

The hash-functions specified in this part of ISO/IEC 10118, known as MASH-1 and MASH-2 (Modular Arithmetic Secure Hash) are particularly suitable for environments in which implementations of modular arithmetic of sufficient length are already available. The two hash-functions differ only in the exponent used in the round-function.

2 Normative reference

The following standard contains provisions which, through reference in this 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 Terms and definitions

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

3.1 From ISO/IEC 10118-1

– collision-resistant hash-function
– data string (data)
– hash-code
– hash-function
– initializing value
– padding.

3.2 Unique to this part of ISO/IEC 10118

3.2.1
block
a string of bits of length L_ϕ, which shall be an integer multiple of 16 (see also clause 6.1)

EXAMPLE The length of the output H_j of the round-function.