

Australian/New Zealand Standard™

**Information technology—Security
techniques—Encryption algorithms**

Part 1: General



AS/NZS ISO/IEC 18033.1:2006

This Joint Australian/New Zealand Standard was prepared by Joint Technical Committee IT-012, Information Systems, Security and Identification. It was approved on behalf of the Council of Standards Australia on 31 March 2006 and on behalf of the Council of Standards New Zealand on 16 June 2006. This Standard was published on 10 July 2006.

The following are represented on Committee IT-012:

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

Keeping Standards up-to-date

Standards are living documents which 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 Standards may also be withdrawn.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 which may have been published since the Standard was purchased.

Detailed information about joint Australian/New Zealand Standards can be found by visiting the Standards Web Shop at www.standards.com.au or Standards New Zealand web site at www.standards.co.nz and looking up the relevant Standard in the on-line catalogue.

Alternatively, both organizations publish an annual printed Catalogue with full details of all current Standards. For more frequent listings or notification of revisions, amendments and withdrawals, Standards Australia and Standards New Zealand offer a number of update options. For information about these services, users should contact their respective national Standards organization.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Please address your comments to the Chief Executive of either Standards Australia or Standards New Zealand at the address shown on the back cover.

This Standard was issued in draft form for comment as DR 06038.

Australian/New Zealand Standard™

Information technology—Security techniques—Encryption algorithms

Part 1: General

First published as AS/NZS ISO/IEC 18033.1:2006.

COPYRIGHT

© Standards Australia/Standards New Zealand

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher.

Jointly published by Standards Australia, GPO Box 476, Sydney, NSW 2001 and Standards New Zealand, Private Bag 2439, Wellington 6020

ISBN 0 7337 7595 0

PREFACE

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

This Standard is identical with, and has been reproduced from ISO/IEC 18033-1:2005, *Information technology—Security techniques—Encryption algorithms—Part 1: General*.

The objective of this Standard is to provide the Information Security programming and development community with clear guidance to the selection and implementation of appropriate encryption algorithms.

This Standard is Part 1 of AS/NZS ISO/IEC 18033, *Information technology—Security techniques—Encryption algorithms*, which, when complete, will consist of the following:

Part 1: General (this Standard)

Part 2: Asymmetric ciphers

Part 3: Block ciphers

Part 4: Stream ciphers

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.

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 18033’ should read ‘this Australian/New Zealand Standard’.
- (c) A full point substitutes for a comma when referring to a decimal marker.

CONTENTS

Page

1	Scope.....	1
2	Terms and definitions.....	1
3	The nature of encryption.....	4
3.1	The purpose of encryption.....	4
3.2	Symmetric and asymmetric ciphers	4
3.3	Key management	5
4	The use and properties of encryption.....	5
4.1	Asymmetric ciphers.....	5
4.2	Block ciphers.....	5
4.2.1	Modes of operation	5
4.2.2	Message Authentication Codes (MACs).....	6
4.3	Stream ciphers	6
5	Object identifiers.....	6
	Annex A (informative) Criteria for inclusion of ciphers in ISO/IEC 18033	7
	Bibliography	8

INTRODUCTION

ISO/IEC 18033 is a multi-part International Standard that specifies encryption systems (ciphers) for the purpose of data confidentiality. The inclusion of ciphers in ISO/IEC 18033 is intended to promote their use as reflecting the current 'state of the art' in encryption techniques.

The primary purpose of encryption (or *encipherment*) techniques is to protect the confidentiality of stored or transmitted data. An encryption algorithm is applied to data (often called *plaintext* or *cleartext*) to yield encrypted data (or *ciphertext*); this process is known as *encryption*. The encryption algorithm should be designed so that the ciphertext yields no information about the plaintext except, perhaps, its length. Associated with every encryption algorithm is a corresponding *decryption algorithm*, which transforms ciphertext back into its original plaintext.

Ciphers work in association with a key. In a *symmetric* cipher, the same key is used in both the encryption and decryption algorithms. In an *asymmetric* cipher, different but related keys are used for encryption and decryption. ISO/IEC 18033-2 is devoted to asymmetric ciphers. ISO/IEC 18033-3 and ISO/IEC 18033-4 are devoted to two different classes of symmetric ciphers, known as block ciphers and stream ciphers.