

This is a preview of "INCITS/ISO/IEC 18033...". Click here to purchase the full version from the ANSI store.

INCITS/ISO/IEC 18033-1-2005  
(ISO/IEC 18033-1:2005, IDT)

# American National Standard

INCITS/ISO/IEC 18033-1:2005[R2014]

*Information technology —  
Security techniques —  
Encryption algorithms —  
Part 1: General*

**Developed by**



*Where IT all begins*



This is a preview of "INCITS/ISO/IEC 18033...". [Click here to purchase the full version from the ANSI store.](#)

**PDF disclaimer**

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

**Adopted by INCITS (InterNational Committee for Information Technology Standards) as an American National Standard.**

Date of ANSI Approval: 11/3/2005

Published by American National Standards Institute,  
25 West 43rd Street, New York, New York 10036

Copyright 2005 by Information Technology Industry Council (ITI).  
All rights reserved.

These materials are subject to copyright claims of International Standardization Organization (ISO), International Electrotechnical Commission (IEC), American National Standards Institute (ANSI), and Information Technology Industry Council (ITI). Not for resale. No part of this publication may be reproduced in any form, including an electronic retrieval system, without the prior written permission of ITI. All requests pertaining to this standard should be submitted to ITI, 1250 Eye Street NW, Washington, DC 20005.  
Printed in the United States of America

First edition  
2005-02-01

---

---

# Information technology — Security techniques — Encryption algorithms —

## Part 1: General

*Technologies de l'information — Techniques de sécurité — Algorithmes de chiffrement —*

*Partie 1: Généralités*

---

---

Reference number  
ISO/IEC 18033-1:2005(E)



This is a preview of "INCITS/ISO/IEC 18033...". [Click here to purchase the full version from the ANSI store.](#)

**PDF disclaimer**

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

© ISO/IEC 2005

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
Case postale 56 • CH-1211 Geneva 20  
Tel. + 41 22 749 01 11  
Fax + 41 22 749 09 47  
E-mail [copyright@iso.org](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland

This is a preview of "INCITS/ISO/IEC 18033...". [Click here to purchase the full version from the ANSI store.](#)

## Contents

Page

|  |    |
|--|----|
| Foreword .....   | iv |
| Introduction .....   | v  |
| 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  |

## 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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. 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.

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.

ISO/IEC 18033-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

ISO/IEC 18033 consists of the following parts, under the general title *Information technology — Security techniques — Encryption algorithms*:

- *Part 1: General*
- *Part 2: Asymmetric ciphers*
- *Part 3: Block ciphers*
- *Part 4: Stream ciphers*

This is a preview of "INCITS/ISO/IEC 18033...". [Click here to purchase the full version from the ANSI store.](#)

## 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.