

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

INCITS/ISO/IEC 18033-2:2006[R2013]

INCITS/ISO/IEC 18033-2:2006[R2013]

INCITS/ISO/IEC 18033-2:2006[2008]  
(ISO/IEC 18033-2:2006, IDT)

# American National Standard

*Information technology —  
Security techniques —  
Encryption algorithms —  
Part 2: Asymmetric ciphers*

**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: 7/1/2008

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

Copyright 2008 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  
2006-05-01

---

---

## Information technology — Security techniques — Encryption algorithms —

### Part 2: Asymmetric ciphers

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

*Partie 2: Chiffres asymétriques*

---

---

Reference number  
ISO/IEC 18033-2:2006(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 2006

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.

1	Scope . . . . .	1
2	Normative references . . . . .	1
3	Definitions . . . . .	2
4	Symbols and notation . . . . .	7
5	Mathematical conventions . . . . .	8
5.1	Functions and algorithms . . . . .	8
5.2	Bit strings and octet strings . . . . .	9
5.3	Finite Fields . . . . .	10
5.4	Elliptic curves . . . . .	12
6	Cryptographic transformations . . . . .	14
6.1	Cryptographic hash functions . . . . .	14
6.2	Key derivation functions . . . . .	15
6.3	MAC algorithms . . . . .	16
6.4	Block ciphers . . . . .	16
6.5	Symmetric ciphers . . . . .	17
7	Asymmetric ciphers . . . . .	19
7.1	Plaintext length . . . . .	20
7.2	The use of labels . . . . .	21
7.3	Ciphertext format . . . . .	21
7.4	Encryption options . . . . .	21
7.5	Method of operation of an asymmetric cipher . . . . .	22
7.6	Allowable asymmetric ciphers . . . . .	22
8	Generic hybrid ciphers . . . . .	22
8.1	Key encapsulation mechanisms . . . . .	23
8.2	Data encapsulation mechanisms . . . . .	24
8.3	<i>HC</i> . . . . .	25
9	Constructions of data encapsulation mechanisms . . . . .	26
9.1	<i>DEM1</i> . . . . .	26
9.2	<i>DEM2</i> . . . . .	27
9.3	<i>DEM3</i> . . . . .	28
10	ElGamal-based key encapsulation mechanisms . . . . .	30
10.1	Concrete groups . . . . .	30
10.2	<i>ECIES-KEM</i> . . . . .	32
10.3	<i>PSEC-KEM</i> . . . . .	34
10.4	<i>ACE-KEM</i> . . . . .	36
11	RSA-based asymmetric ciphers and key encapsulation mechanisms . . . . .	39
11.1	RSA key generation algorithms . . . . .	39
11.2	RSA Transform . . . . .	40
11.3	RSA encoding mechanisms . . . . .	40
11.4	<i>RSAES</i> . . . . .	42
11.5	<i>RSA-KEM</i> . . . . .	44
12	Ciphers based on modular squaring . . . . .	45

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

12.3	<i>HIME(R)</i> . . . . .	48
Annex A (normative)	ASN.1 syntax for object identifiers . . . . .	51
Annex B (informative)	Security considerations . . . . .	61
B.1	MAC algorithms . . . . .	61
B.2	Block ciphers . . . . .	62
B.3	Symmetric ciphers . . . . .	62
B.4	Asymmetric ciphers . . . . .	63
B.5	Key encapsulation mechanisms . . . . .	65
B.6	Data encapsulation mechanisms . . . . .	66
B.7	Security of <i>HC</i> . . . . .	68
B.8	Intractability assumptions related to concrete groups . . . . .	68
B.9	Security of <i>ECIES-KEM</i> . . . . .	69
B.10	Security of <i>PSEC-KEM</i> . . . . .	71
B.11	Security of <i>ACE-KEM</i> . . . . .	71
B.12	The RSA inversion problem . . . . .	72
B.13	Security of <i>RSAES</i> . . . . .	73
B.14	Security of <i>RSA-KEM</i> . . . . .	73
B.15	Security of <i>HIME(R)</i> . . . . .	74
Annex C (informative)	Test vectors . . . . .	75
C.1	Test vectors for <i>DEM1</i> . . . . .	75
C.2	Test vectors for <i>ECIES-KEM</i> . . . . .	76
C.3	Test vectors for <i>PSEC-KEM</i> . . . . .	83
C.4	Test vectors for <i>ACE-KEM</i> . . . . .	91
C.5	Test vectors for <i>RSAES</i> . . . . .	100
C.6	Test vectors for <i>RSA-KEM</i> . . . . .	105
C.7	Test vectors for <i>HC</i> . . . . .	109
C.8	Test vectors for <i>HIME(R)</i> . . . . .	112
Bibliography	. . . . .	123

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

## 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.

ISO/IEC 18033-2 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*

## Introduction

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this International Standard may involve the use of patents.

The ISO and IEC take no position concerning the evidence, validity and scope of this patent right. The holder of this patent right has assured the 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 the ISO and IEC. Information may be obtained from:

### *ISO/IEC JTC 1/SC 27 Standing Document 8 (SD8) "Patent Information"*

Standing Document 8 (SD8) is publicly available at: <http://www.ni.din.de/sc27>

Attention is drawn to the possibility that some of the elements of this International Standard 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.