

This is a preview of "INCITS/ISO/IEC 18032...". Click here to purchase the full version from the ANSI store.

INCITS/ISO/IEC 18032:2005[R2014]

INCITS/ISO/IEC 18032-2005
(ISO/IEC 18032:2005, IDT)

American National Standard

*Information technology —
Security techniques — Prime number
generation*

Developed by



Where IT all begins



This is a preview of "INCITS/ISO/IEC 18032...". [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: 8/29/2005

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

This is a preview of "INCITS/ISO/IEC 18032...". Click [here](#) to purchase the full version from the ANSI store.

First edition
2005-01-15

Information technology — Security techniques — Prime number generation

*Technologies de l'information — Techniques de sécurité — Génération
de nombres premiers*

Reference number
ISO/IEC 18032:2005(E)



© ISO/IEC 2005

This is a preview of "INCITS/ISO/IEC 18032...". [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
Web www.iso.org

Published in Switzerland

This is a preview of "INCITS/ISO/IEC 18032...". Click here to purchase the full version from the ANSI store.

Contents

Page

Foreword.....	iv
1 Scope.....	1
2 Normative references	1
3 Terms and definitions.....	2
4 Symbols	2
5 Trial division	3
6 Probabilistic primality tests	4
6.1 Miller-Rabin primality test	4
6.2 Frobenius-Grantham primality test.....	5
6.3 Lehmann primality test.....	5
7 Deterministic primality verification methods.....	6
7.1 Elliptic curve primality certificate.....	6
7.2 Primality certificate based on Maurer's algorithm	7
8 Prime number generation	8
8.1 Requirements	8
8.2 Using probabilistic tests	9
8.3 Using deterministic methods.....	10
9 Candidate prime testing	11
Annex A (informative) Error probabilities	13
Annex B (informative) Generating primes with side conditions.....	16
Bibliography	18

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 18032 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.