

Second edition
2020-12

Information security — Prime number generation

Sécurité de l'information — Génération de nombres premiers



Reference number
ISO/IEC 18032:2020(E)

© ISO/IEC 2020



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2020

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier; Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

This is a preview of "ISO/IEC 18032:2020". 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	1
4 Symbols and abbreviated terms	2
5 Trial division	3
6 Probabilistic primality test	4
6.1 General.....	4
6.2 Requirements.....	4
6.3 Miller-Rabin primality test.....	4
7 Deterministic primality verification methods	5
7.1 General.....	5
7.2 Elliptic curve primality proving algorithm.....	6
7.2.1 General.....	6
7.2.2 Elliptic curve primality certificate generation.....	6
7.2.3 Elliptic curve primality certificate verification.....	7
7.3 Primality certificate based on The Shawe-Taylor algorithm.....	7
8 Prime number generation	8
8.1 General.....	8
8.2 Requirements.....	8
8.3 Using the Miller-Rabin primality test.....	9
8.3.1 General.....	9
8.3.2 Random search.....	9
8.3.3 Incremental search.....	9
8.3.4 Primes with an elliptic curve primality certificate.....	9
8.4 Using deterministic methods.....	9
8.4.1 General.....	9
8.4.2 The Shawe-Taylor algorithm.....	10
Annex A (normative) Error probabilities	11
Annex B (normative) Generating primes with side conditions	13
Annex C (normative) Additional random number generation methods	16
Annex D (normative) Auxiliary methods	17
Annex E (informative) Prime generation examples	31
Bibliography	33

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see <http://patents.iec.ch>).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This second edition cancels and replaces the first edition (ISO/IEC 18032:2005), which has been technically revised.

The main changes compared to the previous edition are as follows:

- the Frobenius-Grantham primality test in 6.2, the Lehmann primality test in 6.3 and Maurer's algorithm in 8.3.1, have been removed;
- the Elliptic curve primality proving algorithm, The Shawe-Taylor algorithm and the algorithm to generate primes with side conditions, have been added or substantially revised.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.