INTERNATIONAL STANDARD

ISO/IEC 18032

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

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**

© ISO/IEC 2020 – All rights reserved

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.

© ISO/IEC 2020 – All rights reserved

Information security — Prime number generation

1 Scope

This document specifies methods for generating and testing prime numbers as required in cryptographic protocols and algorithms.

Firstly, this document specifies methods for testing whether a given number is prime. The testing methods included in this document are divided into two groups:

— probabilistic primality tests, which have a small error probability. All probabilistic tests described here can declare a composite to be a prime;

— deterministic methods, which are guaranteed to give the right verdict. These methods use so-called primality certificates.

Secondly, this document specifies methods to generate prime numbers. Again, both probabilistic and deterministic methods are presented.

NOTE It is possible that readers with a background in algorithm theory have already had previous encounters with probabilistic and deterministic algorithms. The deterministic methods in this document internally still make use of random bits (to be generated via methods described in ISO/IEC 18031), and "deterministic" only refers to the fact that the output is correct with probability one.

Annex A provides error probabilities that are utilized by the Miller-Rabin primality test.

Annex B describes variants of the methods for generating primes so that particular cryptographic requirements can be met.

Annex C defines primitives utilized by the prime generation and verification methods.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 18031, *Information technology — Security techniques — Random bit generation*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
composite number
composite
integer for which divisors exist that are not *trivial divisors* (3.8)

© ISO/IEC 2020 – All rights reserved

3.2
deterministic random bit generator
DRBG
random bit generator that produces a random-appearing sequence of bits by applying a deterministic algorithm to a suitably random initial value called a seed and, possibly, some secondary inputs on which the security of the random bit generator does not depend

3.3
entropy
measure of the disorder, randomness or variability in a closed system

[SOURCE: ISO/IEC 18031:2011, 3.11]

3.4
Jacobi symbol
Jacobi symbol of a positive integer *a* with respect to an odd integer *n*
product of the Legendre symbols of a with respect to the prime factors of n, including *multiplicity* (3.5)

Note 1 to entry: If the prime factor p occurs with multiplicity $m \geq 1$ in the factorization of n, then the Legendre symbol of a with respect to p occurs with multiplicity m in the product that yields the Jacobi symbol of a with respect to n.

Note 2 to entry: The Legendre symbol of a positive integer a with respect to a prime number p is the value

$a^{(p-1)/2} \bmod p$

3.5
multiplicity
multiplicity of a prime divisor *p* of *n*
largest positive integer e with p^e dividing n

3.6
primality certificate
mathematical proof that a given integer is indeed a prime

Note 1 to entry: For a small integer, primality is most efficiently proven by trial division. In this case, the primality certificate can therefore be empty.

3.7
prime number
prime
positive integer for which there exist only *trivial divisors* (3.8)

3.8
trivial divisors
trivial divisors of a nonzero integer *N*
1, -1, N and $-N$

Note 1 to entry: Any nonzero integer N is divisible by (at least) 1, -1, N and $-N$.

4 Symbols and abbreviated terms

a div n	for integers a and n, with $n \neq 0$, a div n is the unique integer s satisfying $a = s \cdot n + r$ where $0 \leq r < n$.
a mod n	for integers a and n, with $n \neq 0$, a mod n is the unique non-negative integer r satisfying $a = (a \text{ div } n) \cdot n + r$.
C	primality certificate

© ISO/IEC 2020 – All rights reserved