INTERNATIONAL STANDARD

ISO/IEC 18032

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)

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 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

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*.

Information technology — Security techniques — Prime number generation

1 Scope

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

Firstly, this International Standard specifies methods for testing whether a given number is prime. The testing methods included in this International Standard can be divided into two groups:

- Probabilistic primality tests, which have a small error probability. All probabilistic tests described here may declare a composite to be a prime. One test described here may declare a prime to be composite.

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

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

NOTE Readers with a background in algorithm theory may have had previous encounters with probabilistic and deterministic algorithms. We stress that the deterministic methods in this International Standard internally still make use of random bits, and “deterministic” only refers to the fact that the output is correct with probability one.

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

The methods for generating, proving and verifying primality defined by this International Standard are applicable to cryptographic systems based on the properties of the primes.

NOTE The specifications of the tests given in this International Standard define the properties to be tested in the simplest possible form. Following these specifications directly will not necessarily produce the most efficient implementations. This is especially the case for the Frobenius-Grantham test.

2 Normative references

The following referenced documents are indispensable for the application 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 9796-2:2002, *Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms*

ISO/IEC 15946-1:2002, *Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 1: General*