

# Information technology — Security techniques — Prime number generation

ICS 35.040

National foreword

This British Standard reproduces verbatim ISO/IEC 18032:2005 and implements it as the UK national standard.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT security techniques, which has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible international/European committee any enquiries on the interpretation, or proposals for change, and keep the UK interests informed;
- monitor related international and European developments and promulgate them in the UK.

A list of organizations represented on this committee can be obtained on request to its secretary.

Cross-references

The British Standards which implement international publications referred to in this document may be found in the *BSI Catalogue* under the section entitled “International Standards Correspondence Index”, or by using the “Search” facility of the *BSI Electronic Catalogue* or of British Standards Online.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

**Compliance with a British Standard does not of itself confer immunity from legal obligations.**

Summary of pages

This document comprises a front cover, an inside front cover, the ISO/IEC title page, pages ii to iv, pages 1 to 18, an inside back cover and a back cover.

The BSI copyright notice displayed in this document indicates when the document was last issued.

Amendments issued since publication

| Amd. No. | Date | Comments |
|----------|------|----------|
|          |      |          |
|          |      |          |
|          |      |          |
|          |      |          |

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 16 February 2005

© BSI 16 February 2005

# 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*





# 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*

### 3 Terms and definitions

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

#### 3.1

##### **composite number**

##### **composite**

Integer  $N > 1$  is composite if it is not prime, i.e. there exist divisors of  $N$  that are not trivial divisors.

#### 3.2

##### **entropy**

Total amount of information yielded by a set of bits. It is representative of the work effort required for an adversary to be able to reproduce the same set of bits.

#### 3.3

##### **Jacobi symbol**

Jacobi symbol of  $a$  with respect to an odd number  $n$  is the product of the Legendre symbols of  $a$  with respect to the prime factors of  $n$  (repeating the Legendre symbols for repeated prime factors).

NOTE Defined in Annex A of ISO/IEC 9796-2.

#### 3.4

##### **Legendre symbol**

Let  $p$  be an odd prime, and let  $a$  be a positive integer. The Legendre symbol of  $a$  with respect to  $p$  is defined as  $a^{(p-1)/2} \bmod p$ .

NOTE Defined in Annex A of ISO/IEC 9796-2.

#### 3.5

##### **primality certificate**

Mathematical proof that a given number is indeed a prime. For small numbers primality is most efficiently proven by trial division. In these cases, the primality certificate may therefore be empty.

#### 3.6

##### **prime number**

##### **prime**

Integer  $N > 1$  is prime if the only divisors of  $N$  are trivial divisors.

#### 3.7

##### **pseudo-random bit generator**

Deterministic algorithm which when given some form of a bit sequence of length  $k$  outputs a sequence of bits of length  $l > k$ , computationally infeasible to distinguish from true random bits.

#### 3.8

##### **trial division**

Trial division of a number  $N$  means checking all prime numbers smaller than or equal to  $\sqrt{N}$  to see if they divide  $N$ .

#### 3.9

##### **trivial divisor**

Any integer  $N$  is always divisible by 1, -1,  $N$  and  $-N$ . These numbers are the trivial divisors of  $N$ .

### 4 Symbols

$a \bmod n$  – for integers  $a$  and  $n$ ,  $(a \bmod n)$  denotes the (non-negative) remainder obtained when  $a$  is divided by  $n$ .

$C$  – a primality certificate

$C(N)$  – primality certificate of the number  $N$ .