

Information technology — Security techniques — Encryption algorithms —

Part 1: General

ICS 35.040

National foreword

This British Standard is the UK implementation of ISO/IEC 18033-1:2005+A1:2011. It supersedes BS ISO/IEC 18033-1:2005, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33, Information technology — Security techniques.

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

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 cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 10 August 2005

© BSI 2011

ISBN 978 0 580 68082 3

Amendments/corrigenda issued since publication

Date	Comments
31 July 2011	Implementation of ISO/IEC amendment 1:2011: bibliography replaced

INTERNATIONAL STANDARD

ISO/IEC
18033-1

First edition
2005-02-01

Information technology — Security techniques — Encryption algorithms — Part 1: **General**

*Technologies de l'information — Techniques de sécurité — Algorithmes
de chiffrement —*

Partie 1: Généralités



Reference number
ISO/IEC 18033-1:2005(E)

AVA **Documents**
Document Sharing Hub

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Terms and definitions	1
3 The nature of encryption	4
3.1 The purpose of encryption	4
3.2 Symmetric and asymmetric ciphers	4
3.3 Key management	5
4 The use and properties of encryption	5
4.1 Asymmetric ciphers	5
4.2 Block ciphers	5
4.2.1 Modes of operation	5
4.2.2 Message Authentication Codes (MACs)	6
4.3 Stream ciphers	6
5 Object identifiers	6
Annex A (informative) Criteria for inclusion of ciphers in ISO/IEC 18033	7
Bibliography	8

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 18033-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

ISO/IEC 18033 consists of the following parts, under the general title *Information technology — Security techniques — Encryption algorithms*:

- *Part 1: General*
- *Part 2: Asymmetric ciphers*
- *Part 3: Block ciphers*
- *Part 4: Stream ciphers*