INTERNATIONAL STANDARD

ISO/IEC 18033-1

Information technology — Security techniques — Encryption algorithms —

Part 1:
General

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

Partie 1: Généralités

This is a preview - click here to buy the full publication

Contents

Page

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*

Introduction

ISO/IEC 18033 is a multi-part International Standard that specifies encryption systems (ciphers) for the purpose of data confidentiality. The inclusion of ciphers in ISO/IEC 18033 is intended to promote their use as reflecting the current 'state of the art' in encryption techniques.

The primary purpose of encryption (or *encipherment*) techniques is to protect the confidentiality of stored or transmitted data. An encryption algorithm is applied to data (often called *plaintext* or *cleartext*) to yield encrypted data (or *ciphertext*); this process is known as *encryption*. The encryption algorithm should be designed so that the ciphertext yields no information about the plaintext except, perhaps, its length. Associated with every encryption algorithm is a corresponding *decryption algorithm*, which transforms ciphertext back into its original plaintext.

Ciphers work in association with a key. In a *symmetric* cipher, the same key is used in both the encryption and decryption algorithms. In an *asymmetric* cipher, different but related keys are used for encryption and decryption. ISO/IEC 18033-2 is devoted to asymmetric ciphers. ISO/IEC 18033-3 and ISO/IEC 18033-4 are devoted to two different classes of symmetric ciphers, known as block ciphers and stream ciphers.

Information technology — Security techniques — Encryption algorithms —

Part 1:
General

1   Scope

This part of ISO/IEC 18033 is general in nature, and provides definitions that apply in subsequent parts of ISO/IEC 18033. The nature of encryption is introduced, and certain general aspects of its use and properties are described. The criteria used to select the algorithms specified in subsequent parts of ISO/IEC 18033 are defined in Annex A.