ISO/IEC 18033-1:2015-08 (E)

Information technology - Security techniques - Encryption algorithms - Part 1: General

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Termsanddefinitions 1

3 Symbols and abbreviated terms 5
3.1 Symbols 5
3.2 Abbreviated terms 5

4 The nature of encryption 5
4.1 The purpose of encryption 5
4.2 Symmetric and asymmetric ciphers 6
4.3 Key management 6

5 The use and properties of encryption 6
5.1 Asymmetric ciphers 6
5.2 Block ciphers 7
5.2.1 General 7
5.2.2 Modes of operation 7
5.2.3 Message Authentication Codes (MACs) 7
5.3 Stream ciphers 7
5.4 Identity-based mechanisms 8

6 Objectidentifiers 8

Annex A (normative) Criteria for submission of ciphers for possible inclusion in this International Standard 9

Annex B (normative) Criteria for the deletion of ciphers from this International Standard 13

Annex C (informative) Attacks on encryption algorithms 14

Bibliography 16