ISO/IEC 10118-1:2016-10 (E)

Information technology - Security techniques - Hash-functions - Part 1: General

Contents

Page

Foreword iv

1 Scope 1

2 Normative references 1

3 Termsanddefinitions 1

4 Symbols and abbreviated terms 2
4.1 General symbols 2
4.2 Symbols specific to this document 3
4.3 Coding conventions 3

5 Requirements 3

6 General model for hash-functions 3
6.1 General 3
6.2 Hashing operation 4
6.2.1 General 4
6.2.2 Step 1 (padding) 4
6.2.3 Step 2 (splitting) 4
6.2.4 Step 3 (iteration) 4
6.2.5 Step 4 (output transformation) 4
6.3 Use of the general model 5

Annex A (normative) Padding methods 6

Annex B (normative) Criteria for submission of hash-functions for possible inclusion in Annex C (informative) Security considerations 10

Bibliography 12