ISO/IEC 10118-2:2010-10 (E)

Information technology - Security techniques - Hash-functions - Part 2: Hash-functions using an n-bit block cipher

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Symbols and abbreviated terms 2

5 Use of the general model 2

6 Hash-function 1 2
6.1 General 2
6.2 Parameter selection 2
6.3 Padding method 3
6.4 Initializing value 3
6.5 Round function 3
6.6 Output transformation 4

7 Hash-function 2 4
7.1 General 4
7.2 Parameter selection 4
7.3 Padding method 4
7.4 Initializing value 4
7.5 Round function 4
7.6 Output transformation 5

8 Hash-function 3 6
8.1 General 6
8.2 Parameter selection 6
8.3 Padding method 6
8.4 Initializing value 6
8.5 Round function 6
8.6 Output transformation 9

9 Hash-function 4 9
9.1 General 9
9.2 Parameter selection 9
9.3 Padding method 9
9.4 Initializing value 9
9.5 Round function 9
9.6 Output transformation 11

Annex A (informative) Use of AES 13

A.1 General 13
A.2 Hash-function 1 13
A.3 Hash-function 2 13

A.4 Hash-function 3 13
A.5 Hash-function 4 14

Annex B (informative) Examples 15

B.1 General 15
B.2 Hash-function 1 15
B.3 Hash-function 2 16
B.4 Hash-function 3 17
B.5 Hash-function 4 22

Annex C (normative) ASN.1 Module 27

Bibliography 29