

ISO/IEC 10118-3:2004-03 (E)

Information technology - Security techniques - Hash-functions - Part 3: Dedicated hash-functions

Contents		Page
Foreword		iv
Introduction		v
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Symbols (and abbreviated terms)	1
4.2	Symbols specific to this part	2
5	Requirements	3
6	Model for dedicated hash-functions	4
7	Dedicated Hash-Function 1 (RIPEMD-160)	4
7.1	Parameters, functions and constants	4
7.2	Padding method	7
7.3	Description of the round-function	7
8	Dedicated Hash-Function 2 (RIPEMD-128)	8
8.1	Parameters, functions and constants	8
8.2	Padding method	9
8.3	Description of the round-function	9
9	Dedicated Hash-Function 3 (SHA-1)	10
9.1	Parameters, functions and constants	10
9.2	Padding method	11
9.3	Description of the round-function	12
10	Dedicated Hash-Function 4 (SHA-256)	13
10.1	Parameters, functions and constants	13
10.2	Padding method	14
10.3	Description of the round-function	14
11	Dedicated Hash-Function 5 (SHA-512)	15
11.1	Parameters, functions and constants	15
11.2	Padding method	17
11.3	Description of the round-function	17
12	Dedicated Hash-Function 6 (SHA-384)	18
12.1	Parameters, functions and constants	18
12.2	Padding method	19
12.3	Description of the round-function	19
13	Dedicated Hash-Function 7 (WHIRLPOOL)	19
13.1	Parameters, functions and constants	19
13.2	Padding method	21
13.3	Description of the round-function	22

Annex A (informative) Examples	23
Annex B (informative) Formal specifications	78
Annex C (normative) ASN.1 Module	91
Bibliography	94