

### Contents

	Foreword
1	Scope
2	Normative references
3	Terms and definitions
4	Symbols
4.1	Symbols specified in ISO/IEC 10118#1
4.2	Symbols specific to this document
5	Requirements
6	Models for dedicated hash-functions
6.1	Use of models
6.2	Round-function model
6.3	Sponge model
7	Dedicated Hash-Function 1 (RIPEMD-160)
7.1	General
7.2	Parameters, functions and constants
7.2.1	Parameters
7.2.2	Byte ordering convention
7.2.3	Functions
7.2.4	Constants
7.2.5	Initializing value
7.3	Padding method
7.4	Description of the round-function
8	Dedicated Hash-Function 2 (RIPEMD-128)
8.1	General
8.2	Parameters, functions and constants
8.2.1	Parameters
8.2.2	Byte ordering convention
8.2.3	Functions
8.2.4	Constants
8.2.5	Initializing value
8.3	Padding method
8.4	Description of the round-function
9	Dedicated Hash-Function 3 (SHA-1)
9.1	General
9.2	Parameters, functions and constants
9.2.1	Parameters
9.2.2	Byte ordering convention
9.2.3	Functions
9.2.4	Constants
9.2.5	Initializing value
9.3	Padding method
9.4	Description of the round-function
10	Dedicated Hash-Function 4 (SHA-256)
10.1	General

- 10.2 Parameters, functions and constants
  - 10.2.1 Parameters
  - 10.2.2 Byte ordering convention
  - 10.2.3 Functions
  - 10.2.4 Constants
  - 10.2.5 Initializing value
- 10.3 Padding method
- 10.4 Description of the round-function
- 11 Dedicated Hash-Function 5 (SHA-512)
  - 11.1 General
  - 11.2 Parameters, functions and constants
    - 11.2.1 Parameters
    - 11.2.2 Byte ordering convention
    - 11.2.3 Functions
    - 11.2.4 Constants
    - 11.2.5 Initializing value
  - 11.3 Padding method
  - 11.4 Description of the round-function
- 12 Dedicated Hash-Function 6 (SHA-384)
  - 12.1 General
  - 12.2 Parameters, functions and constants
    - 12.2.1 Parameters
    - 12.2.2 Byte ordering convention
    - 12.2.3 Functions
    - 12.2.4 Constants
    - 12.2.5 Initializing value
  - 12.3 Padding method
  - 12.4 Description of the round-function
- 13 Dedicated Hash-Function 7 (WHIRLPOOL)
  - 13.1 General
  - 13.2 Parameters, functions and constants
    - 13.2.1 Parameters
    - 13.2.2 Byte ordering convention
    - 13.2.3 Functions
    - 13.2.4 Constants
    - 13.2.5 Initializing value
  - 13.3 Padding method
  - 13.4 Description of the round-function
- 14 Dedicated Hash-Function 8 (SHA-224)
  - 14.1 General
  - 14.2 Parameters, functions and constants
    - 14.2.1 Parameters
    - 14.2.2 Byte ordering convention
    - 14.2.3 Functions
    - 14.2.4 Constants
    - 14.2.5 Initializing value
  - 14.3 Padding method
  - 14.4 Description of the round-function
- 15 Dedicated Hash-Function 9 (SHA-512/224)
  - 15.1 General
  - 15.2 Parameters, functions and constants
    - 15.2.1 Parameters
    - 15.2.2 Byte ordering convention
    - 15.2.3 Functions
    - 15.2.4 Constants
    - 15.2.5 Initializing value
  - 15.3 Padding method
  - 15.4 Description of the round-function

- 16           **Dedicated Hash-Function 10 (SHA-512/256)**
  - 16.1        **General**
  - 16.2        **Parameters, functions and constants**
    - 16.2.1      **Parameters**
    - 16.2.2      **Byte ordering convention**
    - 16.2.3      **Functions**
    - 16.2.4      **Constants**
    - 16.2.5      **Initializing value**
  - 16.3        **Padding method**
  - 16.4        **Description of the round-function**
  
- 17           **Dedicated Hash-Function 11 (STREEBOG-512)**
  - 17.1        **General**
  - 17.2        **Parameters, functions and constants**
    - 17.2.1      **Parameters**
    - 17.2.2      **Byte ordering convention**
    - 17.2.3      **Functions**
      - 17.2.3.1    **General**
      - 17.2.3.2    **Function X**
      - 17.2.3.3    **Function S**
      - 17.2.3.4    **Function P**
      - 17.2.3.5    **Function L**
      - 17.2.3.6    **Truncation function**
    - 17.2.4      **Constants**
    - 17.2.5      **Initializing value**
  - 17.3        **Padding method**
  - 17.4        **Description of the round-function**
  
- 18           **Dedicated Hash-Function 12 (STREEBOG-256)**
  - 18.1        **General**
  - 18.2        **Parameters, functions and constants**
    - 18.2.1      **Parameters**
    - 18.2.2      **Byte ordering convention**
    - 18.2.3      **Functions**
    - 18.2.4      **Constants**
    - 18.2.5      **Initializing value**
  - 18.3        **Padding method**
  - 18.4        **Description of the round-function**
  
- 19           **Dedicated Hash-Function 13 (SHA3-224)**
  - 19.1        **General**
  - 19.2        **Parameters, functions and constants**
    - 19.2.1      **Parameters**
    - 19.2.2      **Byte ordering convention**
    - 19.2.3      **Functions**
      - 19.2.3.1    **General**
      - 19.2.3.2    **State**
      - 19.2.3.3    **Parts of the state array**
      - 19.2.3.4    **Converting strings to state arrays**
      - 19.2.3.5    **Converting state arrays to strings**
      - 19.2.3.6    **Labelling convention for the state array**
      - 19.2.3.7    **Step mappings**
        - 19.2.3.7.1   **General**
        - 19.2.3.7.2   **Specification of  $\theta$**
        - 19.2.3.7.3   **Specification of  $\rho$**
        - 19.2.3.7.4   **Specification of  $\pi$**
        - 19.2.3.7.5   **Specification of  $\chi$**
        - 19.2.3.7.6   **Specification of  $\iota$**
      - 19.2.3.8    **Keccak-p**
    - 19.3        **Padding method**
    - 19.4        **Description of a round-function**
    - 19.5        **Output transformation**

- 20           **Dedicated Hash-Function 14 (SHA3-256)**
  - 20.1        **General**
  - 20.2        **Parameters, functions and constants**
    - 20.2.1      **Parameters**
    - 20.2.2      **Byte ordering convention**
    - 20.2.3      **Functions**
    - 20.2.4      **Constants**
    - 20.2.5      **Initializing value**
  - 20.3        **Padding method**
  - 20.4        **Description of round-function**
  - 20.5        **Output transformation**

- 21           **Dedicated Hash-Function 15 (SHA3-384)**
  - 21.1        **General**
  - 21.2        **Parameters, functions and constants**
    - 21.2.1      **Parameters**
    - 21.2.2      **Byte ordering convention**
    - 21.2.3      **Functions**
    - 21.2.4      **Constants**
    - 21.2.5      **Initializing value**
  - 21.3        **Padding method**
  - 21.4        **Description of round-function**
  - 21.5        **Output transformation**

- 22           **Dedicated Hash-Function 16 (SHA3-512)**
  - 22.1        **General**
  - 22.2        **Parameters, functions and constants**
    - 22.2.1      **Parameters**
    - 22.2.2      **Byte ordering convention**
    - 22.2.3      **Functions**
    - 22.2.4      **Constants**
    - 22.2.5      **Initializing value**
  - 22.3        **Padding method**
  - 22.4        **Description of round-function**
  - 22.5        **Output transformation**

- 23           **Dedicated Hash-Function 17 (SM3)**
  - 23.1        **General**
  - 23.2        **Parameters, functions and constants**
    - 23.2.1      **Parameters**
    - 23.2.2      **Byte ordering convention**
    - 23.2.3      **Functions**
    - 23.2.4      **Constants**
    - 23.2.5      **Initializing value**
  - 23.3        **Padding method**
  - 23.4        **Description of the round-function**

**Annex A (normative) Object identifiers**

**Annex B (informative) Numerical examples**

- B.1        **General**
- B.2        **Dedicated Hash-Function 1 (RIPEMD-160)**
  - B.2.1      **Example 1**
  - B.2.2      **Example 2**
  - B.2.3      **Example 3**
  - B.2.4      **Example 4**
  - B.2.5      **Example 5**
  - B.2.6      **Example 6**
  - B.2.7      **Example 7**
  - B.2.8      **Example 8**
  - B.2.9      **Example 9**
  - B.2.10     **Example 10**
  - B.2.11     **Example 11**

<b>B.3</b>	<b>Dedicated Hash-Function 2 (RIPEMD-128)</b>
B.3.1	Example 1
B.3.2	Example 2
B.3.3	Example 3
B.3.4	Example 4
B.3.5	Example 5
B.3.6	Example 6
B.3.7	Example 7
B.3.8	Example 8
B.3.9	Example 9
B.3.10	Example 10
B.3.11	Example 11
<b>B.4</b>	<b>Dedicated Hash-Function 3 (SHA-1)</b>
B.4.1	Example 1
B.4.2	Example 2
B.4.3	Example 3
B.4.4	Example 4
B.4.5	Example 5
B.4.6	Example 6
B.4.7	Example 7
B.4.8	Example 8
B.4.9	Example 9
B.4.10	Example 10
B.4.11	Example 11
<b>B.5</b>	<b>Dedicated Hash-Function 4 (SHA-256)</b>
B.5.1	Example 1
B.5.2	Example 2
B.5.3	Example 3
B.5.4	Example 4
B.5.5	Example 5
B.5.6	Example 6
B.5.7	Example 7
B.5.8	Example 8
B.5.9	Example 9
B.5.10	Example 10
B.5.11	Example 11
<b>B.6</b>	<b>Dedicated Hash-Function 5 (SHA-512)</b>
B.6.1	Example 1
B.6.2	Example 2
B.6.3	Example 3
B.6.4	Example 4
B.6.5	Example 5
B.6.6	Example 6
B.6.7	Example 7
B.6.8	Example 8
B.6.9	Example 9
B.6.10	Example 10
B.6.11	Example 11
<b>B.7</b>	<b>Dedicated Hash-Function 6 (SHA-384)</b>
B.7.1	Example 1
B.7.2	Example 2
B.7.3	Example 3
B.7.4	Example 4
B.7.5	Example 5
B.7.6	Example 6
B.7.7	Example 7
B.7.8	Example 8
B.7.9	Example 9
B.7.10	Example 10
B.7.11	Example 11
<b>B.8</b>	<b>Dedicated Hash-Function 7 (WHIRLPOOL)</b>
B.8.1	Example 1
B.8.2	Example 2
B.8.3	Example 3

B.8.4	Example 4
B.8.5	Example 5
B.8.6	Example 6
B.8.7	Example 7
B.8.8	Example 8
B.8.9	Example 9
B.9	Dedicated Hash-Function 8 (SHA-224)
B.9.1	Example 1
B.9.2	Example 2
B.9.3	Example 3
B.9.4	Example 4
B.9.5	Example 5
B.9.6	Example 6
B.9.7	Example 7
B.9.8	Example 8
B.9.9	Example 9
B.9.10	Example 10
B.9.11	Example 11
B.9.12	Example 12
B.9.13	Example 13
B.10	Dedicated Hash-Function 9 (SHA-512/224)
B.10.1	Example 1
B.10.2	Example 2
B.11	Dedicated Hash-Function 10 (SHA-512/256)
B.11.1	Example 1
B.11.2	Example 2
B.12	Dedicated Hash-Function 11 (STREEBOG-512)
B.12.1	General
B.12.2	Example 1
B.12.3	Example 2
B.13	Dedicated Hash-Function 12 (STREEBOG-256)
B.13.1	General
B.13.2	Example 1
B.13.3	Example 2
B.14	Dedicated Hash-Function 13 (SHA3-224)
B.15	Dedicated Hash-Function 14 (SHA3-256)
B.16	Dedicated Hash-Function 15 (SHA3-384)
B.17	Dedicated Hash-Function 16 (SHA3-512)
B.18	Dedicated Hash-Function 17 (SM3)
B.18.1	Example 1
B.18.2	Example 2
B.18.3	Example 3
B.18.4	Example 4
B.18.5	Example 5
B.18.6	Example 6
B.18.7	Example 7
B.18.8	Example 8
B.18.9	Example 9
B.18.10	Example 10
B.18.11	Example 11

#### Annex C (informative) SHA-3 Extendable-Output Functions

C.1	SHAKE-128
C.1.1	Parameters, functions and constants
C.1.1.1	Parameters
C.1.1.2	Byte ordering convention
C.1.1.3	Functions
C.1.1.4	Constants
C.1.1.5	Initializing value
C.1.2	Padding method
C.1.3	Description of round-function
C.1.4	Output transformation
C.1.5	Examples
C.2	SHAKE-256

<b>C.2.1</b>	<b>Parameters, functions and constants</b>
<b>C.2.1.1</b>	<b>Parameters</b>
<b>C.2.1.2</b>	<b>Byte ordering convention</b>
<b>C.2.1.3</b>	<b>Functions</b>
<b>C.2.1.4</b>	<b>Constants</b>
<b>C.2.1.5</b>	<b>Initializing value</b>
<b>C.2.2</b>	<b>Padding method</b>
<b>C.2.3</b>	<b>Description of round-function</b>
<b>C.2.4</b>	<b>Output transformation</b>
<b>C.2.5</b>	<b>Examples</b>

**Page count: 398**