

ISO/IEC 9797-2:2021 (E)

Information security — Message authentication codes (MACs) — Part 2: Mechanisms using a dedicated hash-function

Contents

	Foreword
1	Scope
2	Normative references
3	Terms and definitions
4	Symbols and notation
5	Requirements
6	MAC Algorithm 1
6.1	General
6.2	Description of MAC Algorithm 1
6.2.1	General
6.2.2	Step 1 (key expansion)
6.2.3	Step 2 (modification of the constants and the IV)
6.2.4	Step 3 (hashing operation)
6.2.5	Step 4 (output transformation)
6.2.6	Step 5 (truncation)
6.3	Efficiency
6.4	Computation of the constants
6.4.1	General
6.4.2	Dedicated hash-function 1 (RIPEMD-160)
6.4.3	Dedicated hash-function 2 (RIPEMD-128)
6.4.4	Dedicated hash-function 3 (SHA-1)
6.4.5	Dedicated hash-function 4 (SHA-256)
6.4.6	Dedicated hash-function 5 (SHA-512)
6.4.7	Dedicated hash-function 6 (SHA-384)
6.4.8	Dedicated hash-function 8 (SHA-224)
6.4.9	Dedicated hash-function 17 (SM3)
7	MAC Algorithm 2
7.1	General
7.2	Description of MAC Algorithm 2
7.2.1	General
7.2.2	Step 1 (key expansion)
7.2.3	Step 2 (hashing operation)
7.2.4	Step 3 (output transformation)
7.2.5	Step 4 (truncation)
7.3	Efficiency
8	MAC Algorithm 3
8.1	General
8.2	Description of MAC Algorithm 3
8.2.1	General
8.2.2	Step 1 (key expansion)
8.2.3	Step 2 (modification of the constants and the IV)
8.2.4	Step 3 (padding)
8.2.5	Step 4 (application of the round-function)
8.2.6	Step 5 (truncation)
8.3	Efficiency

9 MAC Algorithm 4

- 9.1 General**
- 9.2 Description of MAC Algorithm 4**
- 9.3 Encoding and padding**
 - 9.3.1 Integer to byte encoding**
 - 9.3.2 String encoding**
 - 9.3.3 Padding**
- 9.4 KMAC128**
 - 9.4.1 General**
 - 9.4.2 Step 1 (Prepare newD)**
 - 9.4.3 Step 2 (Prepare X)**
 - 9.4.4 Step 3 (Generate MAC output)**
- 9.5 KMAC256**
 - 9.5.1 General**
 - 9.5.2 Step 1 (Prepare newD)**
 - 9.5.3 Step 2 (Prepare X)**
 - 9.5.4 Step 3 (Generate MAC output)**
- 9.6 KMACXOF128**
 - 9.6.1 General**
 - 9.6.2 Step 1 (Prepare newD)**
 - 9.6.3 Step 2 (Prepare X)**
 - 9.6.4 Step 3 (Generate MAC output)**
- 9.7 KMACXOF256**
 - 9.7.1 General**
 - 9.7.2 Step 1 (Prepare newD)**
 - 9.7.3 Step 2 (Prepare X)**
 - 9.7.4 Step 3 (Generate MAC output)**

Annex A (normative) Object identifiers

Annex B (informative) Numerical examples

- B.1 General**
- B.2 MAC Algorithm 1**
 - B.2.1 General**
 - B.2.2 Dedicated hash-function 1 (RIPEMD-160)**
 - B.2.3 Dedicated hash-function 2 (RIPEMD-128)**
 - B.2.4 Dedicated hash-function 3 (SHA-1)**
 - B.2.5 Dedicated hash-function 4 (SHA-256)**
 - B.2.6 Dedicated hash-function 5 (SHA-512)**
 - B.2.7 Dedicated hash-function 6 (SHA-384)**
 - B.2.8 Dedicated hash-function 8 (SHA-224)**
 - B.2.9 Dedicated hash-function 17 (SM3)**
- B.3 MAC Algorithm 2**
 - B.3.1 General**
 - B.3.2 Dedicated hash-function 1 (RIPEMD-160)**
 - B.3.3 Dedicated hash-function 2 (RIPEMD-128)**
 - B.3.4 Dedicated hash-function 3 (SHA-1)**
 - B.3.5 Dedicated hash-function 4 (SHA-256)**
 - B.3.6 Dedicated hash-function 5 (SHA-512)**
 - B.3.7 Dedicated hash-function 6 (SHA-384)**
 - B.3.8 Dedicated hash-function 7 (WHIRLPOOL)**
 - B.3.9 Dedicated hash-function 8 (SHA-224)**
 - B.3.10 Dedicated hash-function 11 (STREEBOG-512)**
 - B.3.11 Dedicated hash-function 12 (STREEBOG-256)**
 - B.3.12 Dedicated hash-function 13 (SHA3-224)**
 - B.3.13 Dedicated hash-function 14 (SHA3-256)**
 - B.3.14 Dedicated hash-function 15 (SHA3-384)**
 - B.3.15 Dedicated hash-function 16 (SHA3-512)**
 - B.3.16 Dedicated hash-function 17 (SM3)**
- B.4 MAC Algorithm 3**
 - B.4.1 General**
 - B.4.2 Dedicated hash-function 1 (RIPEMD-160)**
 - B.4.3 Dedicated hash-function 2 (RIPEMD-128)**

- B.4.4 Dedicated hash-function 3 (SHA-1)
- B.4.5 Dedicated hash-function 4 (SHA-256)
- B.4.6 Dedicated hash-function 5 (SHA-512)
- B.4.7 Dedicated hash-function 6 (SHA-384)
- B.4.8 Dedicated hash-function 8 (SHA-224)
- B.4.9 Dedicated hash-function 17 (SM3)
- B.5 MAC Algorithm 4
 - B.5.1 General
 - B.5.2 KMAC128
 - B.5.3 KMAC256
 - B.5.4 KMACXOF128
 - B.5.5 KMACXOF256

Annex C (informative) Security analysis of the MAC algorithms

Page count: 53