ICS 35.040
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 15852.1-2020

Replacing GB/T 15852.1-2008

Information technology. Security techniques-Message authentication codes - Part 1: Mechanisms using a block cipher

Issued on: December 14, 2020 **Implemented on: July 1, 2021**

Issued by: State Administration for Market Regulation, China National Standardization Administration

Table of Contents

Foreword

GB/T 15852 "Information Technology Security Technical Message Identification Code" is divided into the following three parts:

---Part 1: The mechanism of using block ciphers;

---Part 2: The mechanism of using a dedicated hash function;

---Part 3: Using the mechanism of universal hash function:

This part is Part 1 of GB/T 15852:

This section was drafted in accordance with the rules given in GB/T 1:1-2009:

This part replaces GB/T 15852:1-2008 "Information Technology Security Technical Message Authentication Code Part 1: Using Block Ciphers

Mechanisms":

Compared with GB/T 15852:1-2008, the main technical changes are as follows:

---Deleted the description of the purpose of the message authentication code algorithm (see Chapter 1 of the:2008 edition);

---Added the common name reference of the MAC algorithm (see Chapter 5 and Chapter 7);

---Deleted the normative reference documents GB/T 9387:2-1995 and GB/T 15843:1-2008 (see the second edition of the:2008 edition)

chapter);

---The term "initial transformation" (see 3:13) has been added, and the definition of the term "output transformation" has been modified to adapt to the modified MAC algorithm

The general model (see 3:14, 3:2:7 of the:2008 edition);

--- Added 16 symbols and modified 3 symbols (see 4:1, Chapter 4 of the:2008 edition); added "abbreviations" (see 4:2);

--- Modify the title of Chapter 5, change "requirements" to "user requirements"; modify the requirements for users to select key induction methods (see Chapter

Chapter 5, Chapter 5 of the:2008 edition);

---Added the requirement of data string length when using MAC algorithm 4 and the requirement of MAC length when using MAC algorithm 7 (see section

Chapter 5);

---Modified the general model of the MAC algorithm and the "MAC algorithm model"

diagram, and added key induction and final iterative operations to suit

Used for all MAC algorithms specified in this section (see Chapter 6:1, Chapter 6 of the:2008 edition);

---Added the overview and method of the key induction operation, and the overview and method of the final iterative operation (see 6:2, 6:7); added the filling method

Method 4, initial transformation 3 (see 6:3:5, 6:5:4); modified iterative application block cipher operation (see 6:6,:2008 edition 6:4); add

Added an overview of truncation operation and truncation operation 2 (see 6:9); modified and added the operation method specified in this section of MAC

Description of the application in the algorithm (see 6:3:1, 6:5:1, 6:7:1, 6:8:1, 6:9:1, 6:1, 6:3, 6:5 of the:2008 edition);

---Modified the comment of the common name of MAC algorithm 4, deleted the description of the key length when using DEA (see 7:5,:2008

Version 7:4);

---Modified MAC algorithm 5 and replaced it with CMAC (see 7:6, 7:5 in the:2008 edition); modified MAC algorithm 6 and replaced it with

LMAC (see 7:7, 7:6 of the:2008 edition);

---Added MAC algorithm 7 (TrCBC) and MAC algorithm 8 (CBCR) (see 7:8, 7:9);

--- Modify the title of Appendix A "Examples" to "Test Vector"; modify the block cipher algorithm used, modify DEA to SM4

Block cipher algorithm; modified the plaintext, key, and result (see Appendix B, Appendix A of the:2008 edition); added MAC algorithm 7

And the test vector of MAC algorithm 8 (see B:8, B:9);

--- Modify the efficiency of the algorithms numbered 1:2 and 4:2 in Table C:1; increase the security of MAC algorithm 7 and MAC algorithm 8

Description, characteristics of the algorithm, security strength estimation (see Appendix C):

This part uses the redrafting law to amend and adopt ISO /IEC 9797-1:2011 "Information Technology Security Technical Message Identification Code No: 1

Part: The Mechanism of Using Block Ciphers:

Compared with ISO /IEC 9797-1:2011, this part has many adjustments in structure: Appendix A lists this part and ISO /IEC

9797-1:2011 chapter number comparison list: