



# 中华人民共和国国家标准

GB/T 15852.1—2020  
代替 GB/T 15852.1—2008

## 信息技术 安全技术 消息鉴别码 第 1 部分：采用分组密码的机制

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

[ISO/IEC 9797-1:2011, Information technology—Security techniques—  
Message Authentication Codes (MACs)—  
Part 1: Mechanisms using a block cipher, MOD]

2020-12-14 发布

2021-07-01 实施

国家市场监督管理总局 发布  
国家标准化管理委员会



## 目 次

前言 .....	III
引言 .....	VI
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 符号和缩略语 .....	2
4.1 符号 .....	2
4.2 缩略语 .....	4
5 用户要求 .....	4
6 MAC 算法的模型 .....	5
6.1 一般模型 .....	5
6.2 密钥诱导(第 1 步) .....	5
6.2.1 概述 .....	5
6.2.2 密钥诱导方法 1 .....	6
6.2.3 密钥诱导方法 2 .....	6
6.3 消息填充(第 2 步) .....	6
6.3.1 概述 .....	6
6.3.2 填充方法 1 .....	6
6.3.3 填充方法 2 .....	6
6.3.4 填充方法 3 .....	6
6.3.5 填充方法 4 .....	7
6.4 数据分割(第 3 步) .....	7
6.5 初始变换(第 4 步) .....	7
6.5.1 概述 .....	7
6.5.2 初始变换 1 .....	7
6.5.3 初始变换 2 .....	7
6.5.4 初始变换 3 .....	7
6.6 迭代应用分组密码(第 5 步) .....	7
6.7 最终迭代(第 6 步) .....	8
6.7.1 概述 .....	8
6.7.2 最终迭代 1 .....	8
6.7.3 最终迭代 2 .....	8
6.7.4 最终迭代 3 .....	8
6.7.5 最终迭代 4 .....	8
6.8 输出变换(第 7 步) .....	8
6.8.1 概述 .....	8
6.8.2 输出变换 1 .....	8