ICS 35.040
L 80

中华人民共和国国家标准

GB/T 15852.1—2008/ISO/IEC 9797-1:1999
代替 GB 15852—1995

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(MACs)—Part 1:Mechanisms using a block cipher

(ISO/IEC 9797-1:1999,IDT)

2008-07-02 发布　　2008-12-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

GB/T 15852.1—2008/ISO/IEC 9797-1:1999

中华人民共和国
国家标准
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
GB/T 15852.1—2008/ISO/IEC 9797-1:1999
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946　68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230　1/16　印张 1.75　字数 44 千字
2008年11月第一版　2008年11月第一次印刷
*
书号:155066·1-33732　定价 22.00 元

GB/T 15852.1-2008

目　　次

前言 …… Ⅰ
引言 …… Ⅱ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　符号和记法 …… 2
5　要求 …… 3
6　MAC算法的模型 …… 3
6.1　消息填充 …… 4
6.2　数据分割 …… 4
6.3　初始变换 …… 4
6.4　迭代应用分组密码 …… 4
6.5　输出变换 …… 4
6.6　截断操作 …… 5
7　MAC算法 …… 5
7.1　MAC算法1 …… 5
7.2　MAC算法2 …… 5
7.3　MAC算法3 …… 6
7.4　MAC算法4 …… 6
7.5　MAC算法5 …… 6
7.6　MAC算法6 …… 7
附录A（资料性附录）　例子 …… 8
A.1　MAC算法1 …… 9
A.2　MAC算法2 …… 10
A.3　MAC算法3 …… 11
A.4　MAC算法4 …… 12
A.5　MAC算法5 …… 14
A.6　MAC算法6 …… 15
附录B（资料性附录）　MAC算法的安全性分析 …… 18
参考文献 …… 22

参 考 文 献

[1] ISO 16609:2004 Banking—Requirements for message authentication using symmetric techniques.

[2] ISO/IEC 10181-6:1996 Information technology—Open Systems Interconnection—Security frameworks for open systems:Integrity framework.

[3] ANSI X3.92:1981 Data Encryption Algorithm.

[4] ANSI X9.9:1986 Financial Institution Message Authentication(Wholesale).

[5] ANSI X9.19:1986 Financial Insti8tution Retail Message Authencication.

[6] M. Bellare, J. Kilian, P. Rogaway, "The security of cipher block chaining," Advances in Cryptology-Crypto'94, LNCS 839, pp. 341-358, Springer-Verlag, 1994.

[7] D. Coppersmith, C. J. Mitchell, "Attacks on MacDES MAC algorithm," Electronics Letters, Vol. 35, No. 19, pp. 1626-1627, 1999.

[8] D. Coppersmith, C. J. Mitchell, "Key Recovery and Forgery Attacks on the MacDES MAC Algorithm," Advances in Cryptology-Crypto 2000, LNCS 1880, pp. 184-196, Springer-Verlag, 2000.

[9] L. Knudsen, "Chosen-text attack on CBC-MAC," Electronics Letters, Vol. 33, No. 1, pp. 48-49, 1997.

[10] L. Knudsen, B. Preneel, "MacDES: MAC algorithm based on DES," Electronics Letters, Vol. 34, No. 9, pp. 871-873, 1998.

[11] E. Petrank, C. Rackoff, "CBC MAC for real-time data sources," Journal of Cryptology, Vol. 13, No. 3, pp. 315-338, 2000.

[12] B. Preneel, P. C. van Oorschot, "MDx-MAC and building fast MACs from hash functions," Advances in Cryptology-Crypto'95, LNCS 963, pp. 1-14, Springer-Verlag, 1995.

[13] B. Preneel, P. C. van Oorschot, "A key recovery attack on the ANSI X9.19 retail MAC," Electronics Letters, Vol. 32, No. 17, pp. 1568-1569, 1996.

[14] B. Preneel, P. C. van Oorschot, "On the security of iterated Message Authentication Codes," IEEE Transactions on Information Theory, Vol. 45, No. 1, pp. 188-199, 1999.

[15] Karl Brincat and Chris J. Mitchell, "New CBC-MAC forgery attacks," ACISP 2001, LNCS 2119, pp. 3-14. Springer-Verlag, 2001.

[16] Antoine Joux, Guillaume Poupard, and Jacques Stern, "New attacks against standardized MACs," Fast Software Encryption-FSE 2003, LNCS 2887, pp. 170-181. Springer-Verlag, 2003.

前 言

GB/T 15852《信息技术 安全技术 消息鉴别码》分为2个部分：

——第1部分：采用分组密码的机制；

——第2部分：采用专用杂凑函数的机制。

本部分是GB/T 15852的第1部分，等同采用ISO/IEC 9797-1:1999《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》。除对国际标准中笔误做了修改外，也做了编辑性的修改并更新了参考文献。

本部分是GB 15852—1995《信息技术 安全技术 用块密码算法作密码校验函数的数据完整性机制》的修订版。本部分代替GB 15852—1995。与GB 15852—1995相比较，本部分增加了一种填充方法和三种消息鉴别码(MAC)算法。GB 15852—1995附录A中的可选进程，在本部分中被调整到标准主体内。

本部分的附录A和附录B是资料性附录。

本部分由全国信息安全标准化技术委员会提出并归口。

本部分修订单位：中国科学院软件研究所、信息安全国家重点实验室。

本部分主要修订人：吴文玲、王鹏、张立廷、陈华。

本部分所代替标准历次版本发布情况：

——GB 15852—1995。