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

知识星球https://t.zsxq.com/JmiaeUR

目　　次

知识星球https://t.zsxq.com/JmiaeUR

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。

知识星球https://t.zsxq.com/JmiaeUR

引　言

本部分规定的前三种 MAC 算法通常称作 CBC-MAC。在 ANSI X9.9 中所规定的 MAC 算法是本部分中 MAC 算法的一种特例(当 $n=64$、$m=32$ 时,使用 MAC 算法 1、填充方法 1 和分组密码 DEA(见 ANSI X3.92:1981))。在 ANSI X9.19 中所规定的 MAC 算法也是本部分中 MAC 算法的一种特例(当 $n=64$、$m=32$ 时,使用 MAC 算法 1 或 3、填充方法 1 和分组密码 DEA(见 ANSI X3.92:1981))。

第 4 种 MAC 算法是 CBC-MAC 的一个变种,它使用了一个特殊的初始变换。当 MAC 算法的密钥长度是分组密码密钥长度两倍的时候,建议使用 MAC 算法 4。

第 5 种 MAC 算法并行使用 MAC 算法 1,然后把所得到的两个结果相异或。

第 6 种 MAC 算法并行使用 MAC 算法 4,然后把所得到的两个结果相异或。

本部分例子中提及的分组密码均为举例性说明,具体使用时均须采用国家密码管理部门批准的相应分组密码。

知识星球https://t.zsxq.com/JmiaeUR

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

1　范围

GB/T 15852的本部分规定了六种采用分组密码的消息鉴别码算法。这些消息鉴别码算法可用作数据完整性检验,检验数据是否被非授权地改变。同样这些消息鉴别码算法也可用作消息鉴别,保证消息源的合法性。数据完整性和消息鉴别的强度依赖于密钥的长度及其保密性、分组密码的算法强度以及分组长度、消息鉴别码的长度和具体的消息鉴别码算法。

本部分适用于任何安全体系结构、进程及应用的安全服务。

2　规范性引用文件

下列文件中的条款通过GB/T 15852的本部分的引用而成为本部分的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本部分,然而,鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本部分。

GB/T 9387.2—1995　信息处理系统　开放系统互连　基本参考模型　第2部分:安全体系结构(idt ISO 7498-2:1989)

GB/T 15843.1—2008　信息技术　安全技术　实体鉴别　第1部分:概述(ISO/IEC 9798-1:1997,IDT)

GB/T 17964—2008　信息安全技术　分组密码算法的工作模式

3　术语和定义

下列术语和定义适用于本部分。

3.1　本部分采用GB/T 9387.2—1995中定义的如下术语。

3.1.1

数据完整性　data integrity

数据没有被非授权地修改或破坏的性质。

3.2　下列术语和定义适用于本部分。

3.2.1

分组　block

一种定义了长度的比特串。

3.2.2

分组密码密钥　block cipher key

控制分组密码运算的密钥。

3.2.3

初始变换　initial transformation

消息鉴别码算法起始时所应用的函数。

3.2.4

消息鉴别码(MAC)算法密钥　MAC algorithm key

一种用于控制消息鉴别码算法运算的密钥。

3.2.5

消息鉴别码　message authentication code (MAC)

利用对称密码技术和秘密密钥,由消息所导出的数据项。任何持有这一秘密密钥的实体,可利用消

知识星球https://t.zsxq.com/JmiaeUR

息鉴别码检查消息的完整性和始发者。

3.2.6

消息鉴别码算法　message authentication code algorithm

消息鉴别码算法简称 MAC 算法，其输入为密钥和消息，输出为一个固定长度的比特串，满足下面两个性质：

——对于任何密钥和消息，MAC 算法都能够快速有效地计算。

——对于任何固定的密钥，攻击者在没有获得密钥信息的情况下，即使获得了一些（消息、MAC）对，对任何新的消息预测其 MAC 在计算上是不可行的。

注 1：一个 MAC 算法有时被称作一个密码校验函数。

注 2：计算不可行性依赖于使用者具体的安全要求及其环境。

3.2.7

输出变换　output transformation

应用在算法中，对迭代操作的输出所进行的变换。

3.3　本部分采用 GB/T 15843.1—2008 中定义的如下术语。

3.3.1

密文　ciphertext

经变换，信息内容被隐藏起来的数据。

3.3.2

解密　decipherment

一个密文转换为一个明文的处理

3.3.3

加密　encipherment

为产生密文，即隐藏相应数据的信息内容，而利用密码算法对数据进行的（可逆）变换。

3.3.4

密钥　key

一种用于控制密码变换操作（例如加密、解密、密码检验函数计算、签名生成或签名验证）的符号序列。

3.3.5

明文　plaintext

待加密的数据。

3.4　本部分采用 GB/T 17964—2008 中定义的如下术语。

3.4.1

***n* 比特分组密码　*n*-bit block cipher**

分组长度为 n 比特的分组密码。

4　符号和记法

下列符号和记法适用于本部分。

D	输入 MAC 算法的比特串；
D_j	填充操作后，比特串 D 的一个消息块；
$d_K(C)$	使用分组密码 e 和密钥 K 对密文 C 进行解密；
$e_K(P)$	使用分组密码 e 和密钥 K 对明文 P 进行加密；
g	输出变换；
G	输出变换 g 的输出；
H_j	MAC 算法运算中的中间变量；
I	初始变换；
k	分组密码的密钥长度；
k_M	MAC 算法的密钥长度；

知识星球https://t.zsxq.com/JmiaeUR

$K,K',K'',K''',K_1,K_1',K_1'',K_2,K_2',K_2''$	分组密码的密钥；
L	填充方法 3 中的表示长度的消息块；
L_D	比特串 D 的长度；
m	MAC 值的长度；
n	分组密码的分组长度
q	填充和分割操作之后比特串 D 的消息块个数；
$j\sim X$	比特串 X 最左边 j 比特串；
$X\oplus Y$	比特串 X 和比特串 Y 的异或操作；
$X\|\|Y$	比特串 X 和比特串 Y 的连接；
$:=$	MAC 算法中使用的赋值符号，表示符号左边的值等于符号右边的值。

5 要求

采用本部分 MAC 算法的使用者应当选择：

1) 分组密码 e；

2) 从 6.1 中选取一种填充方法；

3) 从 7.1 中选取一种 MAC 算法；

4) MAC 的长度 m；

5) 一种密钥诱导方法；MAC 算法 4、5 和 6 需要此方法，MAC 算法 2 也可能需要。

MAC 的长度 m 应该是一个正整数并且不大于分组长度 n。

如果使用填充方法 3，那么比特串 D 的比特长度应该小于 2^n。

对于具体分组密码 e、填充方法、MAC 算法、m 的值以及密钥诱导方法（如果需要）的选择超出了本部分所规定的范围。

注：上述选择将影响 MAC 算法的安全强度，具体请参考附录 B。

生成 MAC 和验证 MAC 应当使用同样的密钥。如果消息也加密，那么 MAC 算法密钥应当不同于用作加密的密钥。

6 MAC 算法的模型

MAC 算法的应用需要如下六步操作：消息填充、数据分割、初始变换、迭代应用分组密码、输出变换和截断操作。其中，第 3 步至第 6 步如图 1 所示。

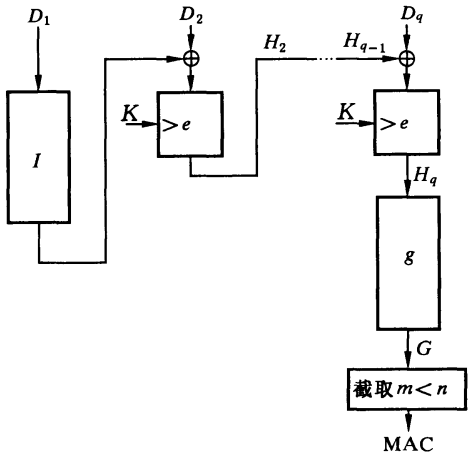

图 1 MAC 算法模型

知识星球https://t.zsxq.com/JmiaeUR

6.1 消息填充

在这一步骤中，用额外的比特串作为前缀或后缀对消息比特串 D 进行填充，使得填充后比特串的长度是 n 的整数倍。

根据选择的填充方法，填充比特串只用来计算 MAC，所以这些填充比特串不必随原消息存储或发送。

MAC 的验证者应当知道填充比特串是否已经被存储或发送，以及使用的是何种填充方法。

本部分规定了三种填充方法，其中的任何一种都可以被用在本部分所规定的六种 MAC 算法中。

6.1.1 填充方法 1

在消息比特串 D 的右侧填充“0”，尽可能少填充(甚至不填充)，使填充后比特串的长度是 n 的整数倍。

注 1：面对简单伪造攻击，使用填充方法 1 的 MAC 算法可能是不安全的。详细信息参见附录 B。

注 2：如果消息比特串 D 是空串，那么填充方法 1 规定对其填充 n 个“0”。

6.1.2 填充方法 2

在消息比特串 D 的右侧填充一个比特“1”，然后在所得到的比特串右侧填充“0”，尽可能少填充(甚至不填充)，使填充后比特串的长度是 n 的整数倍。

6.1.3 填充方法 3

在消息比特串 D 的右侧填充“0”，尽可能少填充(甚至不填充)，使填充后比特串的长度是 n 的整数倍。然后在所得到的比特串左侧填充一个消息块 L。消息块 L 由尽可能少的“0”和比特串 D 长度 L_D 的二进制表示组成，其中位于 L_D 二进制表示的左侧的“0”尽可能少，且使 L 的长度为 n 比特。L 最右端的比特和 L_D 的二进制表示中的最低位相对应。

注：如果在计算 MAC 之前不知比特串的长度，则填充方法 3 不适用。

6.2 数据分割

这一步骤中，把填充后的比特串分割成 q 个 n 比特块 $D_1, D_2, \cdots, D_q$。这里 D_1 表示填充后比特串的第一个 n 比特，D_2 表示随后的 n 个比特，以此类推。

6.3 初始变换

初始变换 I 用来处理填充后比特串的第一个 n 比特块 D_1 以得到 H_1。

本部分的六种 MAC 算法规定使用如下两种初始变换之一。

6.3.1 初始变换 1

初始变换 1 需要一个分组密码密钥 K。按照如下的方法使用密钥 K 和分组密码 e 计算 H_1：

$$H_1 := e_K(D_1)$$

6.3.2 初始变换 2

初始变换 2 需要两个分组密码密钥 K 和 K''。按照如下的方法使用密钥 K 和 K''，以及分组密码 e 计算 H_1：

$$H_1 := e_{K''}(e_K(D_1))$$

6.4 迭代应用分组密码

对比特串 D_i 和 H_{i-1} 的异或值迭代应用分组密码得到 $H_2, H_3, \cdots H_q$：

$$H_i := e_K(D_i \oplus H_{i-1}), i = 2, \cdots, q$$

如果 $q=1$，那么第 4 步省略。

6.5 输出变换

对于第 4 步得到的结果 H_q(若 $q=1$，则为第 3 步得到的结果)，用输出函数 g 再处理。

本部分规定了三种输出变换。

6.5.1 输出变换 1

输出变换 1 是一个恒等变换：

$$G := H_q$$

知识星球https://t.zsxq.com/JmiaeUR

6.5.2 输出变换 2

输出变换 2 是用密钥 K'和分组密码 e 对 H_q 加密操作：

$$G := e_{K'}(H_q)$$

6.5.3 输出变换 3

输出变换 3 首先用密钥 K'和分组密码 e 对 H_q 进行解密操作，然后用密钥 K 和分组密码 e 对得到的结果进行加密操作：

$$G := e_K(d_{K'}(H_q))$$

6.6 截断操作

截取 G 最左边的 m 比特作为 MAC 值：

$$\text{MAC} := m \sim G$$

7 MAC 算法

本部分规定了六种 MAC 算法。每种 MAC 算法明确规定了初始变换和输出变换，但是没有明确规定填充方法；每个 MAC 算法可以结合 6.1 规定的任何一种填充方法使用。

注：对填充方法的选择会影响 MAC 算法的安全强度，详细信息请见附录 B。

7.1 MAC 算法 1

MAC 算法 1 使用初始变换 1 和输出变换 1。MAC 算法密钥就是分组密码密钥 K。

MAC 算法 1 如图 2 所示。

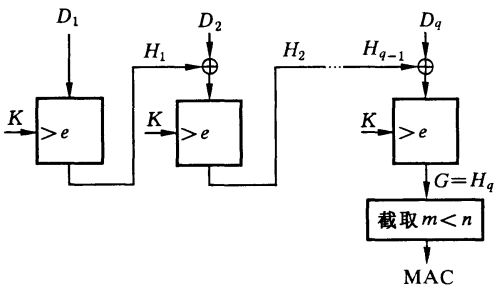

图 2 MAC 算法 1

7.2 MAC 算法 2

MAC 算法 2 使用初始变换 1 和输出变换 2。MAC 算法密钥由两个分组密码密钥 K 和 K'''组成。K'''的值可以由 K 通过密钥诱导方法生成，但是应当满足 $K''' \neq K$。

注 1：由 K 推导出 K'''的一个例子是对 K 从第一个 4 比特组开始，每隔 4 比特交替取补和不变；另外一个例子是通过主密钥生成 K 和 K'''。

注 2：若 $K=K'''$，一个简单的异或伪造攻击就能够攻击 MAC 算法 2，详细信息请见附录 B。

注 3：若 K 和 K'''相互独立，MAC 算法 2 针对密钥恢复攻击的安全强度低于 MAC 算法 2 采用的密钥长度所应该提供的安全强度，详细信息请见附录 B。

MAC 算法 2 如图 3 所示。

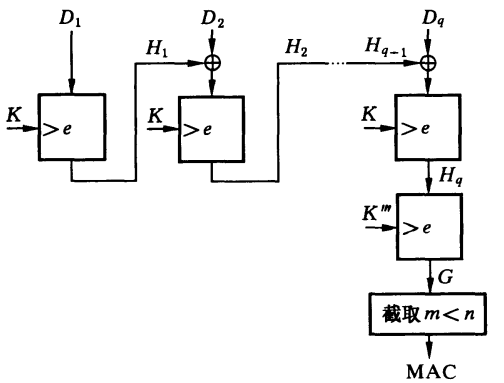

图 3 MAC 算法 2

知识星球https://t.zsxq.com/JmiaeUR

7.3 MAC 算法 3

MAC 算法 3 使用初始变换 1 和输出变换 3。MAC 算法密钥由两个分组密码密钥 K 和 K'组成。密钥 K 和 K'应当独立选取。若 $K=K'$,MAC 算法 3 和 MAC 算法 1 一致。

MAC 算法 3 如图 4 所示。

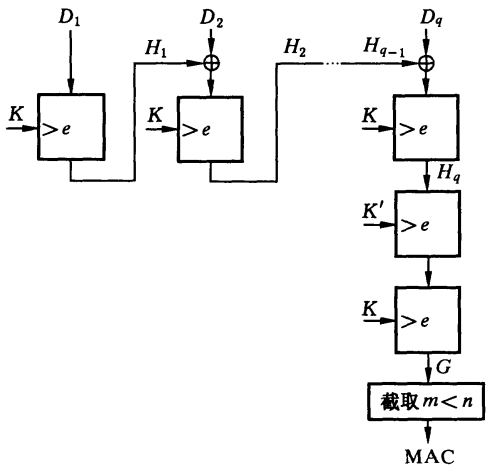

图 4 MAC 算法 3

7.4 MAC 算法 4

MAC 算法 4 使用初始变换 2 和输出变换 2。MAC 算法密钥由两个分组密码密钥 K 和 K'组成。密钥 K 和 K'应当独立选取。另外,第三个密钥 K''由 K'通过密钥诱导方法得出。密钥 K、K'和 K''应当互不相同。密钥 K 和 K''用于初始变换 2,密钥 K 和 K'用于输出变换 2。

注:对 K'从第一个 4 比特组开始,每隔 4 比特交替取补和不变即是由 K'推导出 K''的一个例子,另外一个例子是通过主密钥生成 K'和 K''。

填充后比特串的长度应当不小于 $2n$,即 $q\geqslant 2$。

MAC 算法 4 如图 5 所示。

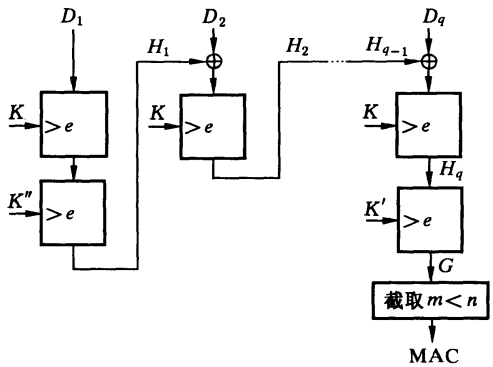

图 5 MAC 算法 4

7.5 MAC 算法 5

MAC 算法 5 使用两个并行的 MAC 算法 1,分别得到两个中间量 MAC_1 和 MAC_2。MAC 算法 5 的密钥就是分组密码密钥 K。两个并行 MAC 算法 1 的密钥 K_1 和 K_2 由密钥 K 生成,而且应当满足 $K_1\neq K_2$。

注:令 $K_1=K$,对 K 从第一个 4 比特组开始,每隔 4 比特交替取补和不变生成 K_2,即是由 K 推导出 K_1 和 K_2 的一个例子;另外一个例子是通过密钥 K 生成 K_1 和 K_2,而且满足 $K_1\neq K_2$。

知识星球https://t.zsxq.com/JmiaeUR

将两个中间量 MAC_1 和 MAC_2 相异或，得到最终的 MAC：

$$MAC := MAC_1 \oplus MAC_2$$

7.6 MAC 算法 6

MAC 算法 6 使用两个并行的 MAC 算法 4，分别得到两个中间量 MAC_1 和 MAC_2。MAC 算法 6 的密钥由两个分组密码密钥 K 和 K' 组成。密钥 K 和 K' 应当独立选取。

两个并行 MAC 算法 4 的密钥 (K_1, K_1') 和 (K_2, K_2') 由主密钥 (K, K') 生成，而且应当满足 $K_1 \neq K_1'$、$K_2 \neq K_2'$ 和 $(K_1, K_1') \neq (K_2, K_2')$。

注 1：令 $K_1 = K$、$K_1' = K'$，对 K_1 从第一个 4 比特组开始，每隔 4 比特交替取补和不变生成 K_2，对 K_1' 从第一个 4 比特组开始，每隔 4 比特交替取补和不变生成 K_2' 即是由 (K, K') 推导出 (K_1, K_1') 和 (K_2, K_2') 的一个例子。

注 2：MAC 算法 4 在其内部使用一个诱导的密钥 K''，意味着 MAC 算法 6 总共使用六个密钥 (K_1, K_1', K_1'') 和 (K_2, K_2', K_2'')。建议使用前确保六个密钥互不相同。

填充后比特串的长度应当不小于 $2n$，即 $q \geqslant 2$。

将两个中间量 MAC_1 和 MAC_2 相异或，得到最终的 MAC：

$$MAC := MAC_1 \oplus MAC_2$$

知识星球https://t.zsxq.com/JmiaeUR

附 录 A
（资料性附录）
例 子

本附录提供了使用 DEA(见 ANSI X3.92)生成 MAC 的过程示例。明文是如下的 7 比特 ASCII 码字(没有奇偶校验位):比特串 1:“Now __ is __ the __ time __ for __ all __”,比特串 2:“Now __ is __ the __ time __ for __ it”,其中__表示一个空格。ASCII 编码等同于 ISO 646 所使用的编码。这里使用的两个密钥是 K=0123456789ABCDEF(16 进制)和 K'=FEDCBA9876543210(16 进制),其中的密钥奇偶校验比特被省略。诱导密钥的方式是从第一个 4 比特组开始,每隔 4 比特交替取补和不变。对于 MAC 算法 1、2、3 和 4,m=32;对于 MAC 算法 5 和 6,m=64。所有的值都是用 16 进制表示。

对于比特串 1,分别经过 3 种填充方法后得到的结果如下:

- 填充方法 1: q=3

D_1	4E	6F	77	20	69	73	20	74
D_2	68	65	20	74	69	6D	65	20
D_3	66	6F	72	20	61	6C	6C	20

- 填充方法 2: q=4

D_1	4E	6F	77	20	69	73	20	74
D_2	68	65	20	74	69	6D	65	20
D_3	66	6F	72	20	61	6C	6C	20
D_4	80	00	00	00	00	00	00	00

- 填充方法 3: q=4

D_1	00	00	00	00	00	00	00	C0
D_2	4E	6F	77	20	69	73	20	74
D_3	68	65	20	74	69	6D	65	20
D_4	66	6F	72	20	61	6C	6C	20

对于比特串 2,分别经过 3 种填充方法后得到的结果如下:

- 填充方法 1: q=3

D_1	4E	6F	77	20	69	73	20	74
D_2	68	65	20	74	69	6D	65	20
D_3	66	6F	72	20	69	74	00	00

- 填充方法 2: q=3

D_1	4E	6F	77	20	69	73	20	74
D_2	68	65	20	74	69	6D	65	20
D_3	66	6F	72	20	69	74	80	00

- 填充方法 3: q=4

D_1	00	00	00	00	00	00	00	B0
D_2	4E	6F	77	20	69	73	20	74
D_3	68	65	20	74	69	6D	65	20
D_4	66	6F	72	20	69	74	00	00

知识星球https://t.zsxq.com/JmiaeUR

A.1 MAC 算法 1

使用比特串 1 和填充方法 1

密钥(K)	01	23	45	67	89	AB	CD	EF
H_1	3F	A4	0E	8A	98	4D	48	15
$D_2 \oplus H_1$	57	C1	2E	FE	F1	20	2D	35
H_2	0B	2E	73	F8	8D	C5	85	6A
$D_3 \oplus H_2$	6D	41	01	D8	EC	A9	E9	4A
$G=H_3$	70	A3	06	40	CC	76	DD	8B

MAC=70 A3 06 40

使用比特串 1 和填充方法 2

密钥(K)	01	23	45	67	89	AB	CD	EF
H_1	3F	A4	0E	8A	98	4D	48	15
$D_2 \oplus H_1$	57	C1	2E	FE	F1	20	2D	35
H_2	0B	2E	73	F8	8D	C5	85	6A
$D_3 \oplus H_2$	6D	41	01	D8	EC	A9	E9	4A
H_3	70	A3	06	40	CC	76	DD	8B
$D_4 \oplus H_3$	F0	A3	06	40	CC	76	DD	8B
$G=H_4$	10	E1	F0	F1	08	34	1B	6D

MAC=10 E1 F0 F1

使用比特串 1 和填充方法 3

密钥(K)	01	23	45	67	89	AB	CD	EF
H_1	4B	B5	82	65	DD	87	B3	05
$D_2 \oplus H_1$	05	DA	F5	45	B4	F4	93	71
H_2	40	C4	00	AD	74	2E	4F	D6
$D_3 \oplus H_2$	28	A1	20	D9	1D	43	2A	F6
H_3	23	7D	5F	95	0B	F7	1F	57
$D_4 \oplus H_3$	45	12	2D	B5	6A	9B	73	77
$G=H_4$	2C	58	FB	8F	F1	2A	AE	AC

MAC=2C 58 FB 8F

使用比特串 2 和填充方法 1

密钥(K)	01	23	45	67	89	AB	CD	EF
H_1	3F	A4	0E	8A	98	4D	48	15
$D_2 \oplus H_1$	57	C1	2E	FE	F1	20	2D	35
H_2	0B	2E	73	F8	8D	C5	85	6A
$D_3 \oplus H_2$	6D	41	01	D8	E4	B1	85	6A
$G=H_3$	E4	5B	3A	D2	B7	CC	08	56

MAC=E4 5B 3A D2

知识星球https://t.zsxq.com/JmiaeUR

使用比特串 2 和填充方法 2

密钥(K)	01	23	45	67	89	AB	CD	EF
H_1	3F	A4	0E	8A	98	4D	48	15
$D_2 \oplus H_1$	57	C1	2E	FE	F1	20	2D	35
H_2	0B	2E	73	F8	8D	C5	85	6A
$D_3 \oplus H_2$	6D	41	01	D8	E4	B1	05	6A
$G=H_3$	A9	24	C7	21	36	14	92	11

MAC=A9 24 C7 21

使用比特串 2 和填充方法 3

密钥(K)	01	23	45	67	89	AB	CD	EF
H_1	DF	9C	D6	EA	7E	5A	E1	62
$D_2 \oplus H_1$	91	F3	A1	CA	17	29	C1	16
H_2	C7	6F	B0	02	94	A4	19	BE
$D_3 \oplus H_2$	AF	0A	90	76	FD	C9	7C	9E
H_3	83	02	28	FD	78	D7	BE	71
$D_4 \oplus H_3$	E5	6D	5A	DD	11	A3	BE	71
$G=H_4$	B1	EC	D6	FC	8B	37	C3	92

MAC=B1 EC D6 FC

A.2 MAC 算法 2

前 q 步操作和 MAC 算法 1 一致。唯一的不同是 MAC 算法 2 使用输出变换 2。

使用比特串 1 和填充方法 1

密钥(K'')	F1	D3	B5	97	79	5B	3D	1F
G	10	F9	BC	67	A0	3C	D5	D8

MAC=10 F9 BC 67

使用比特串 1 和填充方法 2

密钥(K'')	F1	D3	B5	97	79	5B	3D	1F
G	BE	7C	2A	B7	D3	6B	F5	B7

MAC=BE 7C 2A B7

使用比特串 1 和填充方法 3

密钥(K'')	F1	D3	B5	97	79	5B	3D	1F
G	8E	FC	8B	C7	C2	72	6E	5C

MAC=8E FC 8B C7

知识星球https://t.zsxq.com/JmiaeUR

使用比特串 2 和填充方法 1

密钥(K'')	F1 D3 B5 97 79 5B 3D 1F
G	21 5E 9C E6 D9 1B C7 FB

MAC=21 5E 9C E6

使用比特串 2 和填充方法 2

密钥(K'')	F1 D3 B5 97 79 5B 3D 1F
G	17 36 AC 1A 63 63 0E FB

MAC=17 36 AC 1A

使用比特串 2 和填充方法 3

密钥(K'')	F1 D3 B5 97 79 5B 3D 1F
G	05 38 26 96 27 4F B4 F0

MAC=05 38 26 96

A.3 MAC 算法 3

前 q 步操作和 MAC 算法 1 一致。唯一的不同是 MAC 算法 3 使用输出变换 3。

使用比特串 1 和填充方法 1

密钥(K')	FE DC BA 98 76 54 32 10
d 的输出	B4 8D 36 EC 7A D5 69 4F
G	A1 C7 2E 74 EA 3F A9 B6

MAC=A1 C7 2E 74

使用比特串 1 和填充方法 2

密钥(K')	FE DC BA 98 76 54 32 10
d 的输出	79 53 7F EE 18 CF 18 93
G	E9 08 62 30 CA 3B E7 96

MAC=E9 08 62 30

使用比特串 1 和填充方法 3

密钥(K')	FE DC BA 98 76 54 32 10
d 的输出	FE B3 B9 66 1D BE DE CD
G	AB 05 94 63 D7 A7 D1 70

MAC=AB 05 94 63

知识星球https://t.zsxq.com/JmiaeUR

使用比特串 2 和填充方法 1

密钥(K')	FE	DC	BA	98	76	54	32	10
d 的输出	32	8A	C7	8B	A1	CA	0B	3F
G	2E	2B	14	28	CC	78	25	4F

MAC=2E 2B 14 28

使用比特串 2 和填充方法 2

密钥(K')	FE	DC	BA	98	76	54	32	10
d 的输出	7A	71	AF	2F	5D	15	40	A7
G	5A	69	2C	E6	4F	40	41	45

MAC=5A 69 2C E6

使用比特串 2 和填充方法 3

密钥(K')	FE	DC	BA	98	76	54	32	10
d 的输出	20	97	B4	05	F1	9E	2D	D8
G	C5	9F	7E	ED	32	8D	DD	69

MAC=C5 9F 7E ED

A.4 MAC 算法 4

使用比特串 1 和填充方法 1

密钥(K)	01	23	45	67	89	AB	CD	EF
密钥(K')	FE	DC	BA	98	76	54	32	10
密钥(K'')	0E	2C	4A	68	86	A4	C2	E0
e 的输出	3F	A4	0E	8A	98	4D	48	15
H_1	EA	F0	4B	F5	31	ED	33	5E
$D_2 \oplus H_1$	82	95	6B	81	58	80	56	7E
H_2	7E	7F	98	A0	C8	B1	65	6C
$D_3 \oplus H_2$	18	10	EA	80	A9	DD	09	4C
H_3	7B	93	0A	AE	67	4A	C9	24
G	AD	35	02	B7	AC	4A	48	A0

MAC=AD 35 02 B7

使用比特串 1 和填充方法 2

密钥(K)	01	23	45	67	89	AB	CD	EF
密钥(K')	FE	DC	BA	98	76	54	32	10
密钥(K'')	0E	2C	4A	68	86	A4	C2	E0
e 的输出	3F	A4	0E	8A	98	4D	48	15
H_1	EA	F0	4B	F5	31	ED	33	5E
$D_2 \oplus H_1$	82	95	6B	81	58	80	56	7E
H_2	7E	7F	98	A0	C8	B1	65	6C
$D_3 \oplus H_2$	18	10	EA	80	A9	DD	09	4C
H_3	7B	93	0A	AE	67	4A	C9	24
$D_4 \oplus H_3$	FB	93	0A	AE	67	4A	C9	24
H_4	26	C4	FA	D7	2E	6D	D3	A2
G	61	C3	33	E3	42	C5	53	7C

MAC=61 C3 33 E3

知识星球https://t.zsxq.com/JmiaeUR

使用比特串 1 和填充方法 3

密钥(K)	01	23	45	67	89	AB	CD	EF
密钥(K')	FE	DC	BA	98	76	54	32	10
密钥(K'')	0E	2C	4A	68	86	A4	C2	E0
e 的输出	4B	B5	82	65	DD	87	B3	05
H_1	71	5A	F8	BE	DA	BE	90	44
$D_2 \oplus H_1$	3F	35	8F	9E	B3	CD	B0	30
H_2	50	2A	04	42	6A	80	B6	0B
$D_3 \oplus H_2$	38	4F	24	36	03	ED	D3	2B
H_3	AF	13	8C	54	99	9B	84	30
$D_4 \oplus H_3$	C9	7C	FE	74	F8	F7	E8	10
H_4	7F	90	05	61	B4	2C	CE	D2
G	95	2A	F8	38	98	9B	5C	00

MAC=95 2A F8 38

使用比特串 2 和填充方法 1

密钥(K)	01	23	45	67	89	AB	CD	EF
密钥(K')	FE	DC	BA	98	76	54	32	10
密钥(K'')	0E	2C	4A	68	86	A4	C2	E0
e 的输出	3F	A4	0E	8A	98	4D	48	15
H_1	EA	F0	4B	F5	31	ED	33	5E
$D_2 \oplus H_1$	82	95	6B	81	58	80	56	7E
H_2	7E	7F	98	A0	C8	B1	65	6C
$D_3 \oplus H_2$	18	10	EA	80	A1	C5	65	6C
H_3	21	FC	35	F2	B2	26	6C	9A
G	05	F1	08	4C	1D	E3	A3	3D

MAC=05 F1 08 4C

使用比特串 2 和填充方法 2

密钥(K)	01	23	45	67	89	AB	CD	EF
密钥(K')	FE	DC	BA	98	76	54	32	10
密钥(K'')	0E	2C	4A	68	86	A4	C2	E0
e 的输出	3F	A4	0E	8A	98	4D	48	15
H_1	EA	F0	4B	F5	31	ED	33	5E
$D_2 \oplus H_1$	82	95	6B	81	58	80	56	7E
H_2	7E	7F	98	A0	C8	B1	65	6C
$D_3 \oplus H_2$	18	10	EA	80	A1	C5	E5	6C
H_3	8F	76	9B	55	48	42	23	FD
G	A1	BC	09	31	52	BB	3E	0F

MAC=A1 BC 09 31

知识星球https://t.zsxq.com/JmiaeUR

使用比特串 2 和填充方法 3

密钥(K)	01	23	45	67	89	AB	CD	EF
密钥(K')	FE	DC	BA	98	76	54	32	10
密钥(K'')	0E	2C	4A	68	86	A4	C2	E0
e 的输出	DF	9C	D6	EA	7E	5A	E1	62
H_1	82	61	94	52	C7	6D	04	F1
$D_2 \oplus H_1$	CC	0E	E3	72	AE	1E	24	85
H_2	ED	33	1C	07	37	D6	B8	26
$D_3 \oplus H_2$	85	56	3C	73	5E	BB	DD	06
H_3	7C	A1	DE	70	BB	1F	7F	07
$D_4 \oplus H_3$	1A	CE	AC	50	D2	6B	7F	07
H_4	40	B7	45	2E	F3	CF	71	49
G	AF	DE	E0	F9	50	39	66	3D

MAC=AF DE E0 F9

A.5 MAC 算法 5

第 1 部分的计算和 A.1 MAC 算法 1 中一致。

使用比特串 1 和填充方法 1

密钥(K_1)	01	23	45	67	89	AB	CD	EF
MAC_1	70	A3	06	40	CC	76	DD	8B
密钥(K_2)	FE	DC	BA	98	76	54	32	10
MAC_2	84	47	04	F6	7B	5A	CE	9C
$MAC_1 \oplus MAC_2$	F4	E4	02	B6	B7	2C	13	17

MAC=F4 E4 02 B6 B7 2C 13 17

使用比特串 1 和填充方法 2

密钥(K_1)	01	23	45	67	89	AB	CD	EF
MAC_1	10	E1	F0	F1	08	34	1B	6D
密钥(K_2)	FE	DC	BA	98	76	54	32	10
MAC_2	60	11	AE	38	EC	C3	34	F4
$MAC_1 \oplus MAC_2$	70	F0	5E	C9	E4	F7	2F	99

MAC=70 F0 5E C9 E4 F7 2F 99

使用比特串 1 和填充方法 3

密钥(K_1)	01	23	45	67	89	AB	CD	EF
MAC_1	2C	58	FB	8F	F1	2A	AE	AC
密钥(K_2)	FE	DC	BA	98	76	54	32	10
MAC_2	FA	47	AA	7D	1B	00	83	CF
$MAC_1 \oplus MAC_2$	D6	1F	51	F2	EA	2A	2D	63

MAC=D6 1F 51 F2 EA 2A 2D 63

知识星球https://t.zsxq.com/JmiaeUR

使用比特串 2 和填充方法 1

密钥(K_1)	01 23 45 67 89 AB CD EF
MAC_1	E4 5B 3A D2 B7 CC 08 56
密钥(K_2)	FE DC BA 98 76 54 32 10
MAC_2	EB 7F 87 76 1B EE 07 19
$MAC_1 \oplus MAC_2$	0F 24 BD A4 AC 22 0F 4F

MAC=0F 24 BD A4 AC 22 0F 4F

使用比特串 2 和填充方法 2

密钥(K_1)	01 23 45 67 89 AB CD EF
MAC_1	A9 24 C7 21 36 14 92 11
密钥(K_2)	FE DC BA 98 76 54 32 10
MAC_2	49 20 D4 60 AC E8 84 1A
$MAC_1 \oplus MAC_2$	E0 04 13 41 9A FC 16 0B

MAC=E0 04 13 41 9A FC 16 0B

使用比特串 2 和填充方法 3

密钥(K_1)	01 23 45 67 89 AB CD EF
MAC_1	B1 EC D6 FC 8B 37 C3 92
密钥(K_2)	FE DC BA 98 76 54 32 10
MAC_2	6C 33 88 2F 84 2F 28 6E
$MAC_1 \oplus MAC_2$	DD DF 5E D3 0F 18 EB FC

MAC=DD DF 5E D3 0F 18 EB FC

A.6 MAC 算法 6

第 1 部分的计算和 A.4 MAC 算法 4 中一致。

使用比特串 1 和填充方法 1

密钥(K_1)	01 23 45 67 89 AB CD EF
密钥(K_1')	FE DC BA 98 76 54 32 10
密钥(K_1'')	0E 2C 4A 68 86 A4 C2 E0
MAC_1	AD 35 02 B7 AC 4A 48 A0
密钥(K_2)	FE 23 BA 67 76 AB 32 EF
密钥(K_2')	01 DC 45 98 89 54 CD 10
密钥(K_2'')	F1 2C B5 68 79 A4 3D E0
MAC_2	FA 4B F0 96 B4 84 15 1A
$MAC_1 \oplus MAC_2$	57 7E F2 21 18 CE 5D BA

MAC=57 7E F2 21 18 CE 5D BA

知识星球https://t.zsxq.com/JmiaeUR

使用比特串 1 和填充方法 2

密钥(K_1)	01 23 45 67 89 AB CD EF
密钥(K_1')	FE DC BA 98 76 54 32 10
密钥(K_1'')	0E 2C 4A 68 86 A4 C2 E0
MAC_1	61 C3 33 E3 42 C5 53 7C
密钥(K_2)	FE 23 BA 67 76 AB 32 EF
密钥(K_2')	01 DC 45 98 89 54 CD 10
密钥(K_2'')	F1 2C B5 68 79 A4 3D E0
MAC_2	01 B7 53 5B 9A 05 AE 86
$MAC_1 \oplus MAC_2$	60 74 60 B8 D8 C0 FD FA

MAC=60 74 60 B8 D8 C0 FD FA

使用比特串 1 和填充方法 3

密钥(K_1)	01 23 45 67 89 AB CD EF
密钥(K_1')	FE DC BA 98 76 54 32 10
密钥(K_1'')	0E 2C 4A 68 86 A4 C2 E0
MAC_1	95 2A F8 38 98 9B 5C 00
密钥(K_2)	FE 23 BA 67 76 AB 32 EF
密钥(K_2')	01 DC 45 98 89 54 CD 10
密钥(K_2'')	F1 2C B5 68 79 A4 3D E0
MAC_2	68 17 43 56 69 FE 5B 54
$MAC_1 \oplus MAC_2$	FD 3D BB 6E F1 65 07 54

MAC=FD 3D BB 6E F1 65 07 54

使用比特串 2 和填充方法 1

密钥(K_1)	01 23 45 67 89 AB CD EF
密钥(K_1')	FE DC BA 98 76 54 32 10
密钥(K_1'')	0E 2C 4A 68 86 A4 C2 E0
MAC_1	05 F1 08 4C 1D E3 A3 3D
密钥(K_2)	FE 23 BA 67 76 AB 32 EF
密钥(K_2')	01 DC 45 98 89 54 CD 10
密钥(K_2'')	F1 2C B5 68 79 A4 3D E0
MAC_2	15 06 4F 9D 52 91 61 14
$MAC_1 \oplus MAC_2$	10 F7 47 D1 4F 72 C2 29

MAC=10 F7 47 D_1 4F 72 C2 29

知识星球https://t.zsxq.com/JmiaeUR

使用比特串 2 和填充方法 2

密钥(K_1)	01 23 45 67 89 AB CD EF
密钥(K_1')	FE DC BA 98 76 54 32 10
密钥(K_1'')	0E 2C 4A 68 86 A4 C2 E0
MAC_1	A1 BC 09 31 52 BB 3E 0F
密钥(K_2)	FE 23 BA 67 76 AB 32 EF
密钥(K_2')	01 DC 45 98 89 54 CD 10
密钥(K_2'')	F1 2C B5 68 79 A4 3D E0
MAC_2	13 27 93 47 8F A7 07 1D
$MAC_1 \oplus MAC_2$	B2 9B 9A 76 DD 1C 39 12

MAC=B2 9B 9A 76 DD 1C 39 12

使用比特串 2 和填充方法 3

密钥(K_1)	01 23 45 67 89 AB CD EF
密钥(K_1')	FE DC BA 98 76 54 32 10
密钥(K_1'')	0E 2C 4A 68 86 A4 C2 E0
MAC_1	AF DE E0 F9 50 39 66 3D
密钥(K_2)	FE 23 BA 67 76 AB 32 EF
密钥(K_2')	01 DC 45 98 89 54 CD 10
密钥(K_2'')	F1 2C B5 68 79 A4 3D E0
MAC_2	59 9B 1B 84 1D 73 24 89
$MAC_1 \oplus MAC_2$	F6 45 FB 7D 4D 4A 42 B4

MAC=F6 45 FB 7D 4D 4A 42 B4

知识星球https://t.zsxq.com/JmiaeUR

附 录 B
（资料性附录）
MAC 算法的安全性分析

该附录讨论了本部分中 MAC 算法的安全强度。它的目标是协助本部分的使用者选择合适的 MAC 算法。

假定分组密码的密钥长度为 k 比特，MAC 算法的密钥长度为 k_M 比特，所以 $k_M=k$ 或 $k_M=2k$。

该附录中，$MAC_K(D)$ 表示用密钥为 K 的 MAC 算法对消息 D 进行计算所得到的 MAC。

为了确定 MAC 算法的安全强度，本附录考虑了如下两类攻击：

1) 伪造攻击：此类攻击是在没有密钥 K 的情况下，对消息 D 预测 $MAC_K(D)$。如果攻击者能够对一个消息成功预测其 MAC，那么称他有能力“伪造”。实际攻击经常要求伪造是可验证的，也就是说，以接近 1 的概率确认伪造的 MAC 是正确的。在许多应用中消息有特定的格式，这就意味着对消息 D 有额外限制。

2) 密钥恢复攻击：此类攻击根据大量的（消息，MAC）对找到 MAC 算法的密钥 K。密钥恢复攻击比伪造攻击更强大，因为它一旦成功就可进行任意伪造。

一个攻击的可行性依赖于攻击者已知和选择的（消息，MAC）对数目以及离线加密的次数。

对 MAC 算法可能的攻击描述如下，但是这里并不保证列举了所有的攻击。前两种攻击是一般性的，它们对任何 MAC 算法都有效。第三种适用于迭代的 MAC 算法。随后的三种攻击只对本部分中的一个或多个特定 MAC 算法有效（更多信息请参阅[6,9,10,12,13,14]）。

- **猜测 MAC**：这种伪造是不可验证的，成功概率为 $\max(1/2^m, 1/2^{k_M})$。这种攻击适用于所有的 MAC 算法，只有合适地选择 m 和 k_M 才能够抵抗这种攻击。

- **密钥穷搜索**：这种攻击需要运行平均 2^{k_M-1} 次 MAC 算法，并且需要 k_M/m 对（消息，MAC）以唯一确定密钥。同样这种攻击适用于所有 MAC 算法，合适地选择 k_M 能够抵抗这种攻击。另外，MAC 算法使用者也可以阻止攻击者获得 k_M/m 对（消息，MAC）以抵抗这种攻击。如果每次使用 MAC 算法后都改变密钥，那么密钥穷搜索攻击并不比猜测 MAC 攻击更有效。

- **生日攻击**：如果攻击者获得足够数目的（消息，MAC）对，他就能够找到消息 D 和消息 D'，使得 $MAC_K(D)=MAC_K(D')$ 并且 H_q 的值在两次 MAC 计算中是相等的（被称为内部碰撞）。如果消息 D 和 D' 构成内部碰撞，那么对任意的比特串 Y 都有 $MAC_K(D \| Y)=MAC_K(D' \| Y)$。这就构成了一种伪造，当攻击者得到比特串 $D \| Y$ 的 MAC 时，就能够预测比特串 $D' \| Y$ 的 MAC。同样，这种伪造依赖于消息的特殊格式，可能对许多应用没有威胁。但是，这种攻击的扩展版本在消息格式方面有更大的灵活性。这种攻击需要一个比特串、大约 $2^{n/2}$ 对已知（消息，MAC）和 2^{n-m} 对选择（消息，MAC）。

通过以下方式可以避免生日攻击：使用填充方法 3，并且在要处理的消息前面加上一个序列号消息块，使得 MAC 算法是带状态的。这就要求在 MAC 算法实现中要保证在一个密钥周期内，每个序列号在 MAC 计算过程中只用一次。但是，若只采取这两种方式中的一种，那么基本生日攻击的修改版本仍然有效而且复杂度也类似；比如说，如果只采用了填充方法 3 而不采用其他措施，那么生日攻击的一个修改版本（基于文献[14]的引理 1）使用 $2^{n/2}$ 个选择明文即成功。

- **简单伪造**：若采用填充方法 1，那么攻击者可以轻易地增加或删除消息最后的几个“0”比特，却保持 MAC 不变。这就意味着填充方法 1 只能用在 MAC 算法使用者事先知道消息长度的情况下，或者消息最后有不同个数的“0”却意义相同的情况。

知识星球https://t.zsxq.com/JmiaeUR

• **异或伪造**:若 MAC 算法 1 采用填充方式 1 或 2,并且 $m=n$,那么就可能存在异或伪造攻击。简单来讲,假如消息 D 或其被填充后的数据 padding(D)只有一个消息块长度,如果攻击者获得了 $MAC_K(D)$,那么攻击者就知道了 $MAC_K(padding(D) \| (D \oplus MAC_K(D)))=MAC_K(D)$。这就意味着攻击者可以构造伪造。注意:即便 MAC 算法的密钥只被用一次,这种攻击仍然适用。如果攻击者获得了 $MAC_K(D)$和 $MAC_K(D')$,经过类似的推导可得:$MAC_K(padding(D) \| (D' \oplus MAC_K(D)))=MAC_K(D')$。如果攻击者获得了 $MAC_K(D)$、$MAC_K(D \| Y)$和 $MAC_K(D')$,那么攻击者就知道了 $MAC_K(padding(D') \| Y')=MAC_K(padding(D) \| Y)$,其中 $Y'=Y \oplus MAC_K(D) \oplus MAC_K(D')$(这里假定 D 和 Y 的比特长度为 n 的整数倍)。这也构成了一个伪造,因为攻击者在获得了两个已知消息和一个选择消息所对应的 MAC 之后,能够对比特串 padding(D') $\| Y'$伪造 MAC。值得注意的是,上述伪造依赖于消息的特殊格式,可能对许多应用没有威胁。

采用填充方法 3 可以抵抗这种攻击。

若 $m<n$,这种攻击仍然适用,但是更加困难一些,需要额外的 $2^{(n-m)/2}$对选择(消息,MAC)。

这种攻击对使用两个相同密钥($K'=K$)的 MAC 算法 2 也适用,不过这里要求 Y 包含至少两个消息块,并且其前面 n 比特为"0"。

• **捷径密钥恢复**:基于内部碰撞的密钥恢复攻击适用于某些 MAC 算法。比如说 MAC 算法 3,以及采用填充方式 1、2 或 3 的 MAC 算法 4[7,8,10,13]。

如下的表格比较了本部分各 MAC 算法的安全强度。这里假定底层分组密码算法没有任何弱点。表 B.1 列举了各 MAC 算法的主要性质。因为采用填充方法 1 存在简单伪造攻击,所以这里只采用填充方法 2 和 3。表 B.2 和表 B.3 针对采用 $n=64$ 和 $k=56$(比如说 DES[3])分组密码的 MAC 算法,介绍了最好的攻击。其中的大部分攻击源自[6,7,8,9,10,12,13,14];针对 MAC 算法 3($m=32$)的捷径密钥恢复攻击(表 B.3,序号 3)源自表 B.2 中相应攻击的一个扩展。表 B.4 和表 B.5 针对采用 $n=128$ 和 $k=128$ 的分组密码的 MAC 算法 1、2 和 5。攻击复杂度使用 4 元组[$\alpha,\beta,\gamma,\delta$]描述,其中 α 表示离线加密的次数,β 表示已知(消息,MAC)的数目,γ 表示选择(消息,MAC)的数目,δ 表示在线验证的次数。

在假设分组密码是伪随机置换的情况下,文献[6]对输入是定长的 MAC 算法 1 做了分析,给出了安全强度的一个下界,证明了其安全性;文献[11]对输入是任意长度的 MAC 算法 2 做了分析,同样证明了其安全性。文献[6,11]同时说明了在假定底层分组密码没有弱点的条件下,前面所述的很多生日攻击接近于最好的攻击。对六种 MAC 算法的系统分析参见文献[15,16]。

表 B.1 六个 MAC 算法的特性;密钥个数表示相互独立的分组密码密钥个数,效率表示处理长度为 tn 比特的比特串所用的加密次数

序号	MAC 算法	初始变换	输出变换	填充方式	密钥个数	效率
1.1	1	1	1	2	1	$t+1$
1.2	1	1	1	3	1	$t+2$
2.1	2	1	2	2	1	$t+2$
2.2	2	1	2	2	2	$t+2$
3	3	1	3	2	2	$t+3$
4.1	4	2	2	2	2	$t+3$
4.2	4	2	2	3	2	$t+4$
5	5	1	1	2	1	$2t+2$
6	6	2	2	2	2	$2t+6$

知识星球https://t.zsxq.com/JmiaeUR

表 B.2　当 $n=64$、$k=56$ 和 $m=64$ 时的安全强度估计；安全强度由四个数字表示：离线加密的次数，已知(比特串，MAC)的数目，选择(比特串，MAC)的数目以及在线验证的次数

	密钥恢复		伪造		
序号	密钥穷搜索	捷径密钥恢复	猜测 MAC 值	异或	生日伪造
1.1	$[2^{56},1,0,0]$	—	$[0,0,0,2^{56}]$	$[0,1,0,0]$	$[0,2^{32},1,0]$ [a]
1.2	$[2^{56},1,0,0]$	—	$[0,0,0,2^{56}]$	—	$[0,2^{32},1,0]$ [a]
2.1	$[2^{56},1,0,0]$	—	$[0,0,0,2^{56}]$	—	$[0,2^{32},1,0]$ [a]
2.2	$[2^{112},1,0,0]$	$[2^{57},2,0,0]$	$[0,0,0,2^{64}]$	—	$[0,2^{32},1,0]$ [a]
3	$[2^{112},2,0,0]$	$[2^{57},2^{32},0,0]$ $[2^{56},1,0,2^{56}]$	$[0,0,0,2^{64}]$ $[0,1,0,2^{56}]$	—	$[0,2^{32},1,0]$ [a]
4.1	$[2^{112},2,0,0]$	$[2^{58},2^{32},2,0]$ [a] $[2^{58},1,1,2^{56}]$ [a]	$[0,0,0,2^{64}]$ $[2^{58},1,1,2^{56}]$ [a]	—	$[0,2^{32},1,0]$ [a]
4.2	$[2^{112},2,0,0]$	$[2^{57},2^{32}\cdot 2^{50},0]$	$[0,0,0,2^{64}]$	—	$[0,2^{32},1,0]$ [a]
5	$[2^{56},1,0,0]$	—	$[0,0,0,2^{56}]$	—	—
6	$[2^{112},2,0,0]$	—	$[0,0,0,2^{64}]$	—	$[0,2^{64},2^{64},0]$ [a]

[a] 表示采用填充方式 3 并且在比特串头部附加一个序列号消息块可避免相应攻击。

表 B.3　当 $n=64$、$k=56$ 和 $m=32$ 时的安全强度估计；安全强度由四个数字表示：离线加密的次数，已知(比特串，MAC)的数目，选择(比特串，MAC)的数目以及在线验证的次数

	密钥恢复		伪造		
序号	密钥穷搜索	捷径密钥恢复	猜测 MAC 值	异或	生日伪造
1.1	$[2^{56},2,0,0]$	—	$[0,0,0,2^{32}]$	$[0,2,2^{16},0]$	$[0,2^{32},2^{32},0]$ [a]
1.2	$[2^{56},2,0,0]$	—	$[0,0,0,2^{32}]$	—	$[0,2^{32},2^{32},0]$ [a]
2.1	$[2^{56},2,0,0]$	—	$[0,0,0,2^{32}]$	—	$[0,2^{32},2^{32},0]$ [a]
2.2	$[2^{112},4,0,0]$	$[2^{57},2^{32},2^{32},0]$ $[2^{88},4,0,0]$	$[0,0,0,2^{32}]$	—	$[0,2^{32},2^{32},0]$ [a]
3	$[2^{112},4,0,0]$	$[2^{57},2^{32},2^{32},0]$ [a] $[2^{89},2^{32},0,0]$ $[2^{56},2,0,2^{56}]$	$[0,0,0,2^{32}]$	—	$[0,2^{32},2^{32},0]$ [a]
4.1	$[2^{112},4,0,0]$	$[2^{78},2^{32},2^{50},0]$	$[0,0,0,2^{32}]$	—	$[0,2^{32},2^{32},0]$ [a]
4.2	$[2^{112},4,0,0]$	$[2^{78},2^{32},2^{50},0]$	$[0,0,0,2^{32}]$	—	$[0,2^{32},2^{32},0]$ [a]
5	$[2^{56},2,0,0]$	—	$[0,0,0,2^{32}]$	—	—
6	$[2^{112},4,0,0]$	—	$[0,0,0,2^{32}]$	—	$[0,2^{64},2^{96},0]$ [a]

[a] 表示采用填充方式 3 并且在比特串头部附加一个序列号消息块可避免相应攻击。

表 B.4　当 $n=128$、$k=128$ 和 $m=64$ 时的安全强度估计；安全强度由四个数字表示：离线加密的次数，已知(比特串，MAC)的数目，选择(比特串，MAC)的数目以及在线验证的次数

	密钥恢复		伪造		
序号	密钥穷搜索	捷径密钥恢复	猜测 MAC 值	异或	生日伪造
1.1	$[2^{128},2,0,0]$	—	$[0,0,0,2^{64}]$	$[0,2,2^{32},0]$	$[0,2^{64},2^{64},0]$ [a]
1.2	$[2^{128},2,0,0]$	—	$[0,0,0,2^{64}]$	—	$[0,2^{64},2^{64},0]$ [a]
2.1	$[2^{128},2,0,0]$	—	$[0,0,0,2^{64}]$	—	$[0,2^{64},2^{64},0]$ [a]
5	$[2^{128},2,0,0]$	—	$[0,0,0,2^{64}]$	—	—

[a] 表示采用填充方式 3 并且在比特串头部附加一个序列号消息块可避免相应攻击。

知识星球https://t.zsxq.com/JmiaeUR

表 B.5 当 $n=128$、$k=128$ 和 $m=32$ 时的安全强度估计；安全强度由四个数字表示：离线加密的次数，已知(比特串，MAC)的数目，选择(比特串，MAC)的数目以及在线验证的次数

	密钥恢复		伪造		
序号	密钥穷搜索	捷径密钥恢复	猜测 MAC 值	异或	生日伪造
1.1	$[2^{128},4,0,0]$	—	$[0,0,0,2^{32}]$	$[0,2,2^{48},0]$	$[0,2^{64},2^{96},0]$ [a]
1.2	$[2^{128},4,0,0]$	—	$[0,0,0,2^{32}]$	—	$[0,2^{64},2^{96},0]$ [a]
2.1	$[2^{128},4,0,0]$	—	$[0,0,0,2^{32}]$	—	$[0,2^{64},2^{96},0]$ [a]
5	$[2^{128},4,0,0]$	—	$[0,0,0,2^{32}]$	—	—

[a] 表示采用填充方式 3 并且在比特串头部附加一个序列号消息块可避免相应攻击。

基本原理

本部分对 MAC 算法选择的一个重要的因素是与 ANSI、ISO 和 ISO/IEC 标准的前期版本保持兼容性。

与以前的版本相比较，数据填充方法从两个增加为三个。第三种填充方法以很小的代价使得 MAC 算法能够抵抗某些攻击，特别是当 MAC 算法使用者能够容易地在要处理的数据前附加一个长度分组的情况下。

以前版本附录 A 中的可选进程，在本版本中被调整到标准主体中。

另外，新加入了三种 MAC 算法：

- MAC 算法 4 提供了一种改进的增加密钥长度的方法。强烈建议用户采用这个 MAC 算法和填充方式 3；

因为在代价大致相同的情况下，它比 MAC 算法 3 提供了更好的安全性。

- MAC 算法 5 能够更强地抵抗生日伪造攻击。
- MAC 算法 6 不但提供了一种改进的增加密钥长度的方法，而且能够更强地抵抗生日伪造攻击。

相比较于其他改进 CBC-MAC 的方式，本部分中规定的 MAC 算法不仅提供了增强的安全性，而且相对简单，使得分析与实现更加容易。

知识星球https://t.zsxq.com/JmiaeUR

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.

知识星球https://t.zsxq.com/JmiaeUR

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

如有印装差错 由本社发行中心调换
版权专有 侵权必究
举报电话:(010)68533533

GB/T 15852.1-2008

知识星球https://t.zsxq.com/JmiaeUR