L 80

中华人民共和国国家标准

GB 15852—1995
idt ISO/IEC 9797:1994

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

Information technology—Security techniques —Data integrity mechanism using a cryptographic check function employing a block cipher algorithm

1995-12-13 发布　　1996-08-01 实施

国家技术监督局　发布

前　　言

本标准等同采用国际标准 ISO/IEC 9797:1994《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》。

该国际标准规定的用块密码算法作密码校验函数的数据完整性机制，适合于我国使用。

本标准的附录 A 是标准的附录。

本标准的附录 B 和附录 C 是提示的附录。

本标准由中华人民共和国电子工业部提出。

本标准由电子工业部标准化研究所归口。

本标准起草单位：电子工业部第三十研究所。

本标准主要起草人：龚奇敏、黄月江、吴世忠、杜明钰。

ISO/IEC 前言

ISO(国际标准化组织)和IEC(国际电工委员会)形成了一个世界范围内的标准化专门系统。ISO 或 IEC 的成员国,通过由处理特殊技术活动领域的各个组织所建立的技术委员会来参与国际标准的开发。ISO 和 IEC 的技术委员会在共同感兴趣的领域内合作,其他与 ISO 和 IEC 有联络的官方和非官方国际性组织,也参与这项工作。

在信息技术领域内,ISO 和 IEC 已建立了一个联合技术委员会 ISO/IEC JTC1。被联合技术委员会接受的国际标准草案分送给各成员国表决。一个国际标准的发布,需要至少 75% 的成员国投赞成票。

国际标准 ISO/IEC 9797 是由信息技术联合技术委员会 ISO/IEC JTC1 的 IT 安全技术 SC 27 分委员会制定的。

第二版取代其第一版(ISO/IEC 9797:1989),第一版已经过修改和扩充,增加了一种填充方法和一种可选进程,同时还增加了一个包含若干例子的新附录。

附录 A 是本国际标准的组成部分,附录 B、C 仅仅是一种信息。

引　　言

本标准中规定的机制除了用 n 比特数据块的算法、m 比特的校验值和规定了一种附加的填充方法外，与 ISO 8731-1、ISO 9807 和 ANSI X9.9 标准中所用的相同。

ISO 8731-1、ANSI X9.9 和 ANSI X9.19 中叙述的密码校验值的计算方法是本标准的一种特殊情况，即当 $n=64$，$m=32$，采用 5.1 中规定的填充方法 1 以及使用 DEA（见 ANSI X3.92;1981）数据加密算法。

中华人民共和国国家标准

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

GB 15852—1995
idt ISO/IEC 9797:1994

Information technology—Security techniques —Data integrity mechanism using a cryptographic check function employing a block cipher algorithm

1　范围

本标准规定了一种使用密钥和 n 比特块密码算法计算 m 比特密码校验值的方法。这种方法可用作数据完整性机制，以检测数据是否已被非授权地改变。这种数据完整性机制的强度依赖于密钥的长度及其保密性，依赖于密码算法的特性以及校验值的长度 m。

本标准适用于任何安全体系结构、进程或应用的安全服务。

2　引用标准

下列标准所包含的条文，通过在本标准中引用而构成本标准的条文。本标准出版时，所示版本均为有效。所有标准都会被修订，使用本标准的各方应探讨使用下列标准最新版本的可能性。

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)

ISO/IEC 10116:1991　信息技术　n 位块密码算法的工作方式

3　定义和记法

3.1　定义

本标准使用了 GB/T 9387.2 和 ISO/IEC 10116 中定义的术语。

3.1.1　密码校验值　cryptographic check value

对数据单元进行加密变换所得到的信息。

3.1.2　数据完整性　data integrity

指数据没有被非授权地改变或破坏的性质。

3.1.3　n 比特块密码算法　n-bit block cipher algorithm

明文块和密文块长度均是 n 比特的块密码算法。

3.2　记法

本标准将密码校验值称作消息鉴别码(MAC)。

在本标准上下文中，当术语“最高有效位/字节”和“最低有效位/字节”具有某种含义时，例如，把比特串看成是数值，则一个块的最左边若干比特便是最高有效位。

4　要求

MAC 的长度(m)应小于或等于块的长度(n)，计算的结果和任何可选进程的结果都是长度为 n 的一个信息块，而最后 n 比特块的最左边 m 比特便形成了 MAC。

国家技术监督局 1995-12-13 批准　　1996-08-01 实施

5 MAC 计算

5.1 填充和分块

MAC 的产生需要从下列两种填充方法中选出一种。作出这种选择的途径超出了本标准的范围。

方法 1

需计算 MAC 的数据应添补必要的几个(可能一个也没有)'0'比特,以便得到一个长度(按比特计)为 n 的整数倍的数据串。

方法 2

需计算 MAC 的数据应先添补一个'1'比特,然后再添补必要的几个(可能一个也没有)"0"比特,以便得到一个长度(按比特计)为 n 的整数倍的数据串。

注:如果验证者不知道数据的长度,则应选用填充方法 2,因为此方法允许验证者查明所添补的那些'0'比特。

所得数据分成 n 比特的块($D_1, D_2, \cdots, D_q$)。按照所选的填充方法,添补到原始数据上的那些比特,仅仅用于计算和验证 MAC 的,因此,这些填充比特(若有的话)不一定要随原始数据一起存储或传输。验证者应当知道这些填充比特是否已被存储或传输以及使用的是哪一种填充方法。

5.2 加密密钥

密钥应当随机或准随机产生,如果消息加密也使用该算法,则计算 MAC 所用的密钥应当和数据加密用的密钥不同。

5.3 起始步

MAC 按图 1 所示进行计算。

输入寄存器由第一个块(D_1)初始化,输入数据(I_1)通过算法(A),使用密钥(K)产生 n 比特存入输出寄存器(O_1)。

5.4 随后各步

下一个 n 比特数据(D_2)与输出寄存器(O_1)中的 n 比特按位异或运算且结果装入下一步的输入寄存器(I_2),输入寄存器(I_2)中的数据再通过算法(A),使用密钥(K)产生 n 比特存入输出寄存器(O_2)。

这一操作继续到所有数据块都被处理后为止。所得结果便是最后的输出块(O_q)。

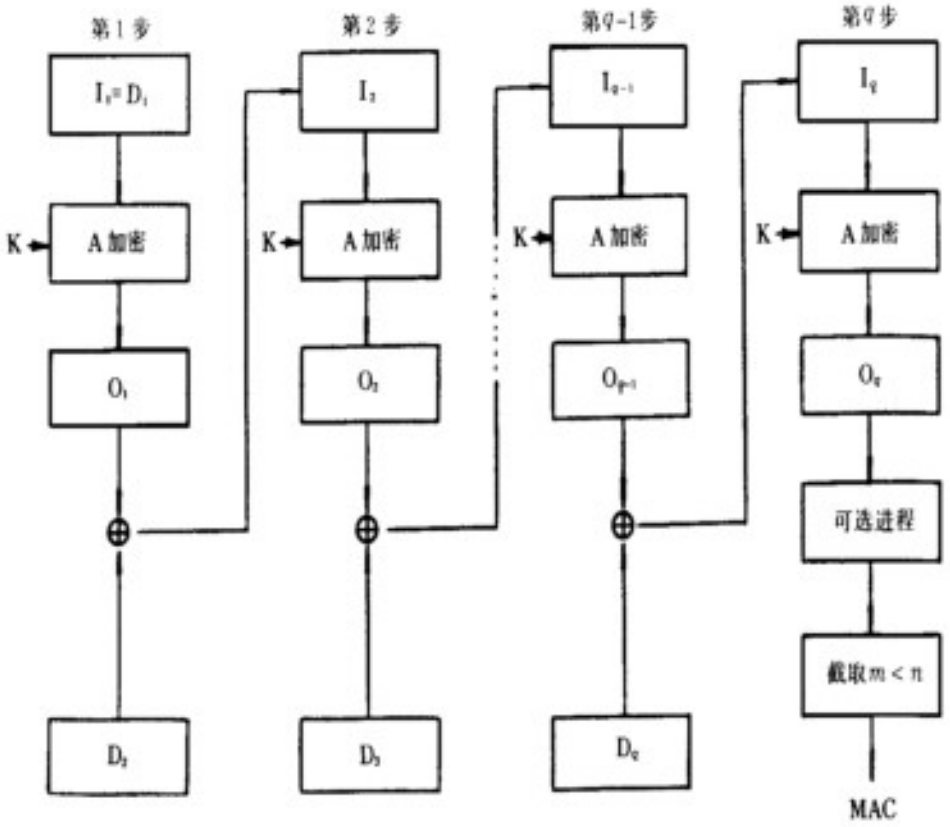
5.5 可选进程

最后的输出块(O_q)或许要作选择性的处理以增加 MAC 的强度。可选进程(如果采用的话)应从附录 A(标准的附录)中规定的几个中选取。

5.6 MAC

最后一个 n 比特块的最左边 m 比特构成 MAC。

注:若选用附录 A(标准的附录)的 A1 条规定的可选进程,可减轻穷搜攻击的威胁。特别,当 m=n 时,建议采用这种可选进程。



I_i 输入块($i=1,\cdots\cdots,q$)
A ■比特块密码算法
O_i 输出块($i=1,\cdots\cdots,q$)
K 密钥
D_i 数据块($i=1,\cdots\cdots,q$)
⊕ 异或

图 1 MAC 的计算

附 录 A
（标准的附录）
可 选 进 程

A1 可选进程 1

下述过程规定了一种可选进程（见 5.5），它可按照发方和收方之间的预先商定使用。这种可选进程增加了 MAC 抗穷搜密钥和选择明文攻击的强度。

在这种可选进程中，要用两个加密密钥，分别记作（K）和（K_1）。

首先按照 5.3 和 5.4 中规定的过程，用密钥（K）产生 n 比特块（O_q），接着执行附加的两步（见图 A1）：

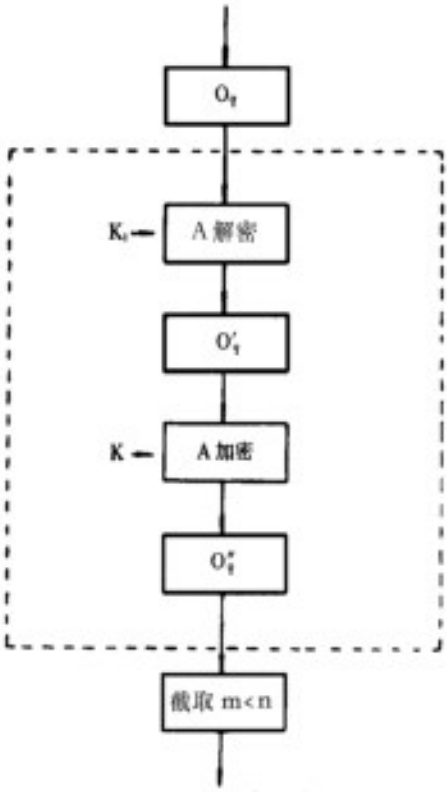


图 A1 可选进程 1

a） 用密钥（K_1）对输出（O_q）解密，得到（O'_q）；

b） 用密钥（K）对（O'_q）加密，得到（O''_q）。

这就完成了可选进程，MAC 按 5.6 规定得到。

A2 可选进程 2

下述过程规定了一种可选进程（见 5.5），它可按照发方和收方之间的预先商定使用。这种可选进程增加了 MAC 抗选择明文攻击的强度。

在这种可选进程中，用了两个加密密钥，分别记作（K）和（K_1），其中（K_1）可从（K）推导得到。

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_1）的一个例子。

首先按 5.3 和 5.4 中规定的过程，用密钥（K）产生 n 比特块（O_q），接着执行附加的一步（见图 A2）：

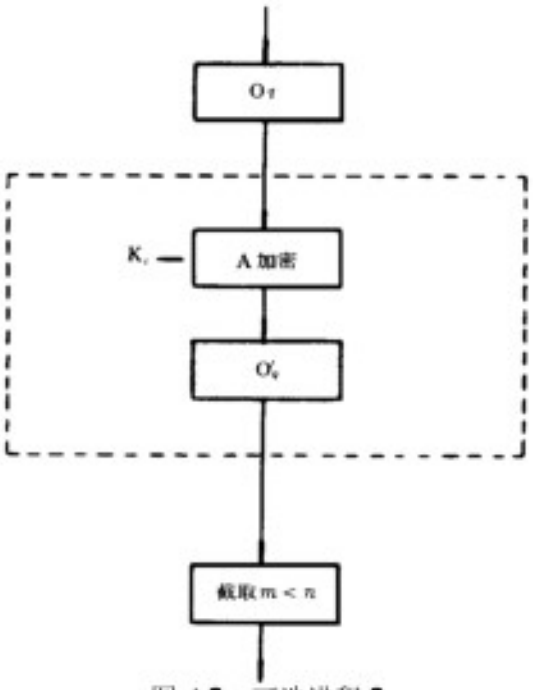


图 A2　可选进程 2

用(K_1)对输出(O_8)加密，得到(O'_8)。

这就完成了可选进程，MAC 按 5.6 的规定得到。

附　录　B
（提示的附录）
例　子

本附录给出了对于填充方法 1 和 2 以及可选进程 1 和 2，使用加密算法 DEA（见 ANSI X3.92）产生 MAC 的若干例子。明文分别是“Now␣is␣the␣time␣for␣all␣”和“Now␣is␣the␣time␣for␣it”的 7 比特 ASC Ⅱ 码（不带奇偶校验位）[1]，其中“␣”表示一个空格。如果选用填充方法 1，则第一个明文不需要作任何填充。密钥（K）是 0123456789ABCDEF，密钥（K_1）在可选进程 1 中选为 FEDCBA9876543210，而在可选进程 2 中，密钥(K_1)是按附录 A（标准的附录）中 A2 的注导出的。

B1　填充方法 1

例 1：Now␣is␣the␣time␣for␣all␣

密钥(K)	01	23	45	67	89	AB	CD	EF
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
$I_1=D_1$	4E	6F	77	20	69	73	20	74
O_1	3F	A4	0E	8A	98	4D	48	15

采用说明：

1] 我国标准 GB 1988—89《信息处理　信息交换用七位编码字符集》与 ASC Ⅱ 代码等效。

续表

密钥(K)	01	23	45	67	89	AB	CD	EF
$I_2=O_1 \oplus D_2$	57	C1	2E	FE	F1	20	2D	35
O_2	0B	2E	73	F8	8D	C5	85	6A
$I_3=O_2 \oplus D_3$	6D	41	01	D8	EC	A9	E9	4A
O_3	70	A3	06	40	CC	76	DD	8B

如果不采用可选进程，MAC 就由(O_3)最左边 m 比特组成。

可选进程 1

密钥(K_1)	FE	DC	BA	98	76	54	32	10
O'_3	B4	8D	36	EC	7A	D5	69	4F
O''_3	A1	C7	2E	74	EA	3F	A9	B6

MAC 由(O''_3)的最左边 m 比特组成。

可选进程 2

密钥(K_1)	F1	D3	B5	97	79	5B	3D	1F
O'_3	10	F9	BC	67	A0	3C	D5	D8

MAC 由(O'_3)的最左边 m 比特组成。

例 2：Now␣is␣the␣time␣for␣it

密钥(K)	01	23	45	67	89	AB	CD	EF
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
$I_1=D_1$	4E	6F	77	20	69	73	20	74
O_1	3F	A4	0E	8A	98	4D	48	15
$I_2=O_1 \oplus D_2$	57	C1	2E	FE	F1	20	2D	35
O_2	0B	2E	73	F8	8D	C5	85	6A
$I_3=O_2 \oplus D_3$	6D	41	01	D8	E4	B1	85	6A
O_3	E4	5B	3A	D2	B7	CC	68	56

如果不采用可选进程，MAC 就由(O_3)的最左边 m 比特组成。

可选进程 1

密钥(K_1)	FE	DC	BA	98	76	54	32	10
O'_3	32	8A	C7	8B	A1	CA	0B	3F
O''_3	2E	2B	14	28	CC	78	25	4F

MAC 由(O''_3)的最左边 m 比特组成。

可选进程 2

密钥(K_1)	F1	D3	B5	97	79	5B	3D	1F
O'_3	21	5E	9C	E6	D9	1B	C7	FB

MAC 由(O'_3)的最左边 m 比特组成。

B2 填充方法 2

例 1：Now␣is␣the␣time␣for␣all␣

密钥(K)	01	23	45	67	89	AB	CD	EF
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
$I_1=D_1$	4E	6F	77	20	69	73	20	74
O_1	3F	A4	0E	8A	98	4D	48	15
$I_2=O_1\oplus D_2$	57	C1	2E	FE	F1	20	2D	35
O_2	0B	2E	73	F8	8D	C5	85	6A
$I_3=O_2\oplus D_3$	6D	41	01	D8	EC	A9	E9	4A
O_3	70	A3	06	40	CC	76	DD	8B
$I_4=O_3\oplus D_4$	F0	A3	06	40	CC	76	DD	8B
O_4	10	E1	F0	F1	08	34	1B	6D

如果不采用可选进程，MAC 就由(O_4)的最左边 m 比特组成。

可选进程 1

密钥(K_1)	FE	DC	BA	98	76	54	32	10
O'_4	79	53	7F	EE	18	CF	18	93
O''_4	E9	08	62	30	CA	3B	E7	96

MAC 由(O''_4)的最左边 m 比特组成。

可选进程 2

密钥(K_1)	F1	D3	B5	97	79	5B	3D	1F
O'_4	BE	7C	2A	B7	D3	6B	F5	B7

MAC 由(O'_4)的最左边 m 比特组成。

例 2：Now␣is␣the␣time␣for␣it

密钥(K)	01	23	45	67	89	AB	CD	EF
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
$I_1=D_1$	4E	6F	77	20	69	73	20	74
O_1	3F	A4	0E	8A	98	4D	48	15
$I_2=O_1\oplus D_2$	57	C1	2E	FE	F1	20	2D	35
O_2	0B	2E	73	F8	8D	C5	85	6A
$I_3=O_2\oplus D_3$	6D	41	01	D8	E4	B1	05	6A
O_3	A9	24	C7	21	36	14	92	11

如果不采用可选进程，MAC 就由(O_3)的最左边 m 比特组成。

可选进程 1

密钥(K_1)	FE	DC	BA	98	76	54	32	10
O'_3	7A	71	AF	2F	5D	15	40	A7
O''_3	5A	69	2C	E6	4F	40	41	45

MAC 由(O''_3)的最左边 m 比特组成。

可选进程 2

密钥(K_1)	F1	D3	B5	97	79	5B	3D	1F
O'_3	17	36	AC	1A	61	63	0E	FB

MAC 由(O'_3)的最左边 m 比特组成。

附 录 C
(提示的附录)
参考文献

[1] ISO 8731-1:1987 银行业 消息鉴别的许可算法 第 1 部分:数据加密算法(DEA)

[2] ISO 9807:1991 银行业及相关金融业服务 消息鉴别的要求(零售)

[3] ISO/IEC 9979:1991 数据加密技术 密码算法的登记规程

[4] ISO/IEC 10181-5:[1)] 信息技术 开放系统互连 开放系统的安全框架:完整性框架

[5] ANSI X3.92:1981 数据加密算法

[6] ANSI X9.9:1986 金融机构的消息鉴别(批发)

[7] ANSI X9.19:1986 金融机构零售消息鉴别

1) 待发布。