INTERNATIONAL STANDARD

ISO/IEC 9797

Second edition
1994-04-15

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

Technologies de l'information — Techniques de sécurité — Mécanisme d'intégrité des données utilisant une fonction de contrôle cryptographique employant un algorithme de chiffrement par bloc

Reference number
ISO/IEC 9797:1994(E)

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75% of the national bodies casting a vote.

International Standard ISO/IEC 9797 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Sub-Committee SC27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 9797: 1989) which has been revised and extended to include an additional padding method, an additional method for the optional process as well as a new annex containing examples.

Annex A forms an integral part of this International Standard. Annexes B and C are for information only.

Introduction

The mechanism specified in this International Standard is similar to that used in ISO 8731–1, ISO 9807 and in the ANSI X9.9 standard, except that it is defined in terms of an algorithm using n-bit data blocks and an m-bit check value, and that an additional padding method is specified.

The calculation of cryptographic check values as described in ISO 8731–1, ANSI X9.9 and ANSI X9.19 is a specific case of this International Standard when $n = 64$ and $m = 32$, when padding method 1 specified in 5.1 is used, and when DEA (see ANSI X3.92: 1981) is used.

This page intentionally left blank

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

1 Scope

This International Standard specifies a method of using a key and an n-bit block cipher algorithm to calculate an m-bit cryptographic check value. This method can be used as a data integrity mechanism to detect that data has not been altered in an unauthorised manner. The strength of the data integrity mechanism is dependent on the key length and its secrecy, on the nature of the cryptographic algorithm, and on m, the length of the check value.

This International Standard can be applied to the security services of any security architecture, process, or application.

2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this International Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO 7498–2: 1989, *Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture.*

ISO/IEC 10116: 1991, *Information technology - Modes of operation for an n-bit block cipher algorithm.*

3 Definitions and notation

3.1 Definitions

This International Standard makes use of the following terms defined in ISO 7498-2 and ISO/IEC 10116.

3.1.1 cryptographic check value: Information which is derived by performing a cryptographic transformation on the data unit.

3.1.2 data integrity: The property that data has not been altered or destroyed in an unauthorized manner.

3.1.3 n-bit block cipher algorithm: A block cipher algorithm with the property that plaintext blocks and ciphertext blocks are n bits in length.

3.2 Notation

This International Standard refers to the cryptographic check value as a Message Authentication Code (MAC).

In contexts where the terms "most significant bit/byte" and "least significant bit/byte" have a meaning, e.g., where strings of bits are treated as numerical values, then the leftmost bits of a block shall be the most significant.

4 Requirements

The length (m) of the MAC will be less than or equal to the block length (n). The result of the calculation and of any optional process is an information block of length n. The m leftmost bits of the final n-bit block form the MAC.

5 MAC calculation

5.1 Padding and blocking

The generation of a MAC requires the selection of one of two padding methods. The way in which the selection is made is beyond the scope of this International Standard.

Method 1
The data for which the MAC is to be calculated shall be appended with as few (possibly none) '0' bits as necessary to obtain a data string whose length (in bits) is an integer multiple of n.

Method 2

The data for which the MAC is to be calculated shall be appended with a single '1' bit. The resulting data shall then be appended with as few (possibly none) '0' bits as necessary to obtain a data string whose length (in bits) is an integer multiple of n.

NOTE — If the length of data is not known by a verifier then padding method 2 should be used, since it permits a verifier to detect the addition or deletion of trailing '0' bits.

The resulting data is divided into n-bit blocks (D_1, D_2, $\cdots$, D_q). The bits which are padded to the original data, according to the chosen padding method, are only used for calculating and verifying the MAC. Consequently, the padding bits (if any) need not be stored or transmitted with the data. The verifier shall know whether or not the padding bits have been stored or transmitted, and which padding method is in use.

5.2 The cryptographic key

The key should be randomly or pseudo-randomly generated. If the same algorithm is used for encipherment of the message, the key used for the calculation of the MAC should be different from that used for encipherment.

5.3 The initial stage

The MAC is calculated as illustrated in figure 1.

The input register is initialized with the first block (D_1). This input data (I_1) is passed through the algorithm (A), which uses a key (K) to produce n bits in the output register (O_1).

5.4 Subsequent stages

The next n bits of data (D_2) are bitwise exclusive or'ed with the n bits of the output register (O_1) and the result is loaded into the input register of the next stage (I_2). The contents of the input register (I_2) is passed through the algorithm (A), which uses the key (K) to produce n bits in the output register (O_2).

This operation continues until all blocks have been processed. The result will be the final output block (O_q).

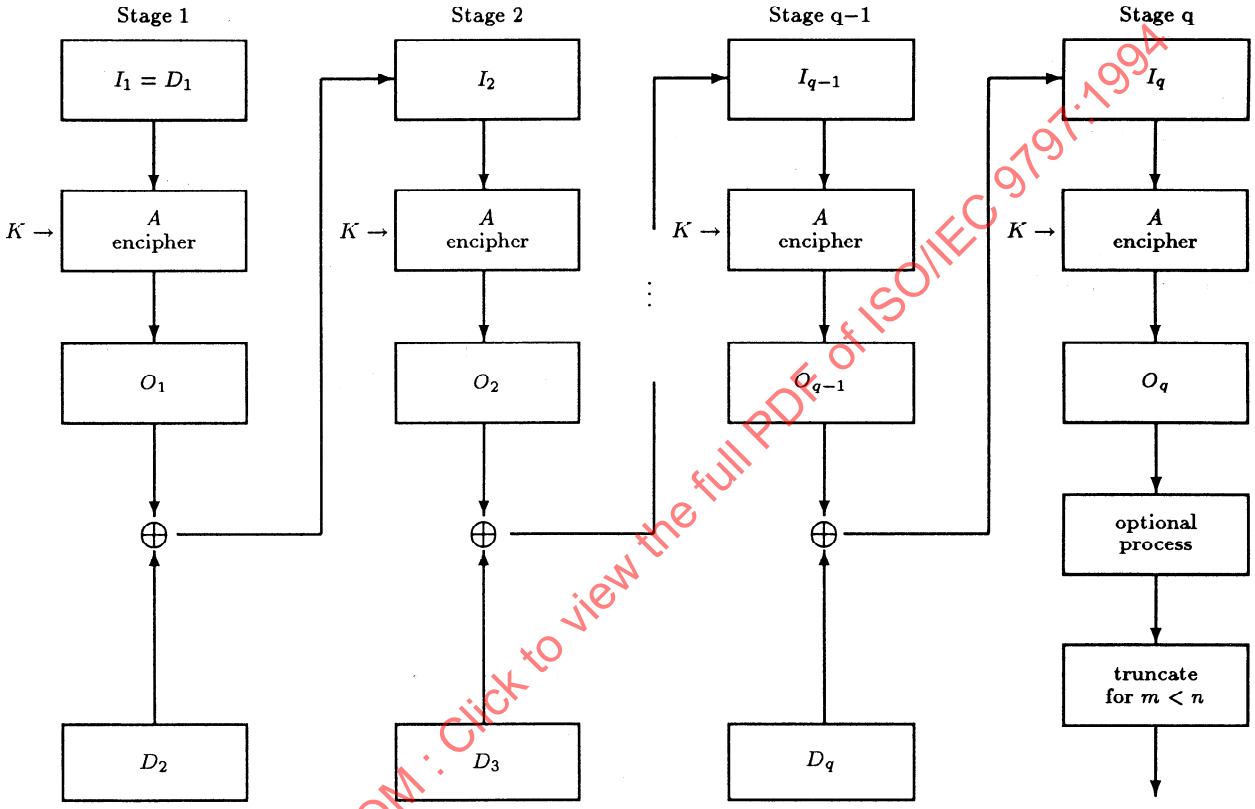
5.5 Optional Process

The final output block (O_q) may be subjected to optional processing to increase the strength of the MAC. The optional process (if used) shall be selected from those specified in normative annex A.

5.6 The MAC

The m leftmost bits of the final n-bit block form the MAC.

NOTE — Use of the optional process specified in A.1 of annex A reduces the threat of exhaustive search attacks. In particular, this optional process is recommended when $m = n$.



Legend:

I_i	input block $(i = 1, \ldots, q)$
A	n-bit block cipher algorithm
O_i	output block $(i = 1, \ldots, q)$
K	key
D_i	data block $(i = 1, \ldots, q)$
$\oplus$	exclusive or

Figure 1 — The MAC calculation

Annex A
(normative)
Optional Processes

A.1 Optional process 1

The following procedure specifies an optional process (see 5.5) which may be used in accordance with a predefined agreement between sender and receiver. This optional process increases the strength of the MAC with respect to exhaustive key search and chosen plaintext attacks.

In this optional process two cryptographic keys are used, which are denoted by (K) and (K_1).

The n-bit block (O_q) is first generated using key (K) in the procedure specified in 5.3 and 5.4.

Two additional steps shall then be performed (see figure A.1):

a) decipher the output (O_q) using key (K_1) to obtain (O'_q);

b) encipher (O'_q) using key (K) to obtain (O''_q).

This completes the optional process. The MAC is obtained as specified in 5.6.

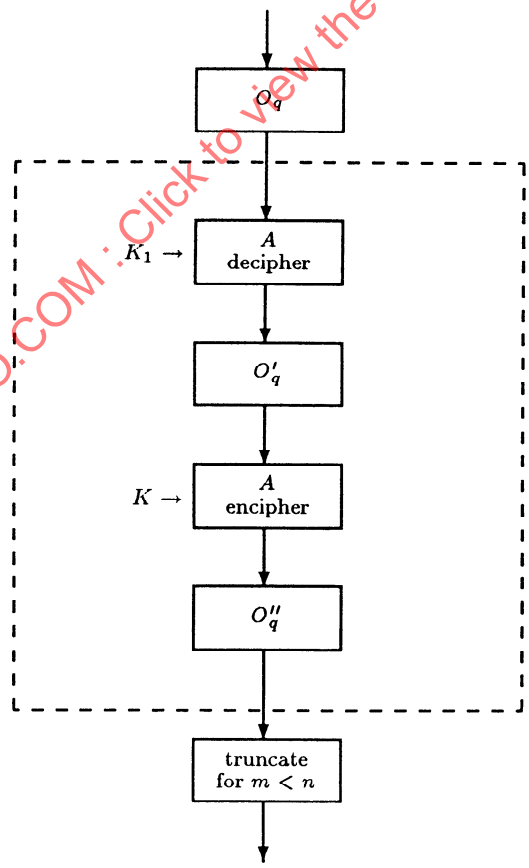


Figure A.1 — Optional process 1

A.2 Optional process 2

The following procedure specifies an optional process (see 5.5) which may be used in accordance with a predefined agreement between sender and receiver. This optional process increases the strength of the MAC with respect to chosen plaintext attacks.

In this optional process two cryptographic keys are used, which are denoted by (K) and (K_1), where (K_1) may be derived from (K).

NOTE — An example of how to derive (K_1) from (K) is to complement alternate blocks of four bits of (K) commencing with the first four bits.

The n-bit block (O_q) is first generated using key (K) in the procedure specified in 5.3 and 5.4.

An additional step shall then be performed (see figure A.2):

encipher the output (O_q) using key (K_1) to obtain (O'_q).

This completes the optional process. The MAC is obtained as specified in 5.6.

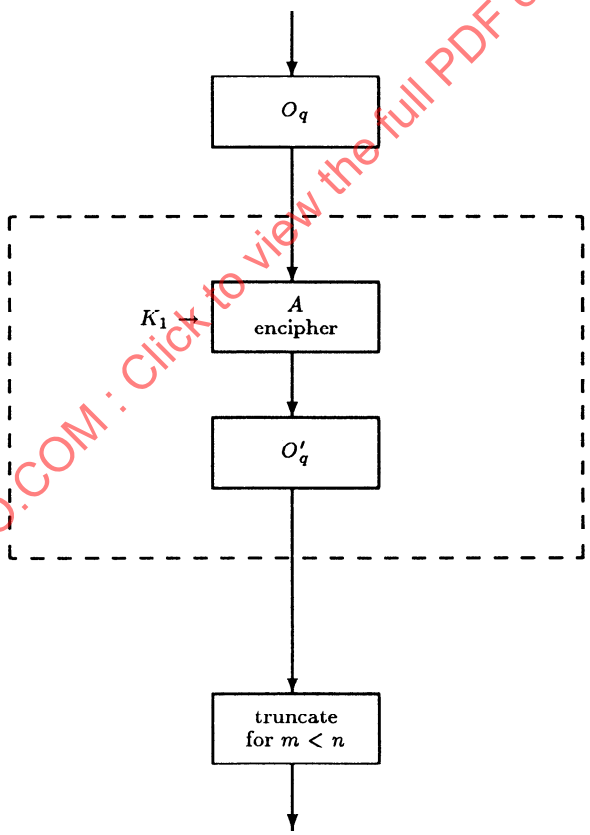


Figure A.2 — Optional process 2

Annex B
(informative)
Examples

This annex presents examples of the generation of a MAC employing the DEA (see ANSI X3.92) for padding methods 1 and 2 as well as optional processes 1 and 2. The plaintexts are the 7-bit ASCII codes (no parity) for "`Now␣is␣the␣time␣for␣all␣`" and "`Now␣is␣the␣time␣for␣it`", where "␣" denotes a blank. The first plaintext does not require any padding if padding method 1 is chosen. The key (K) is 0123456789ABCDEF. The key (K_1) in optional process 1 was chosen to be FEDCBA9876543210, while the key (K_1) in optional process 2 was derived according to the note in annex A.2.

B.1 Padding method 1

Example 1: `Now␣is␣the␣time␣for␣all␣`

key (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
$I_2 = O_1 \oplus D_2$	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

If no optional process is used the MAC consists of the m leftmost bits of (O_3).

Optional process 1

key (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

The MAC consists of the m leftmost bits of (O''_3).

Optional process 2

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

The MAC consists of the m leftmost bits of (O'_3).

Example 2: `Now␣is␣the␣time␣for␣it`

key (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	08	56

If no optional process is used the MAC consists of the m leftmost bits of (O_3).

Optional process 1

key (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

The MAC consists of the m leftmost bits of (O''_3).

Optional process 2

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

The MAC consists of the m leftmost bits of (O'_3).

B.2 Padding method 2

Example 1: `Now␣is␣the␣time␣for␣all␣`

key (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

If no optional process is used the MAC consists of the m leftmost bits of (O_4).

Optional process 1

key (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

The MAC consists of the m leftmost bits of (O''_4).

Optional process 2

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

The MAC consists of the m leftmost bits of (O'_4).

Example 2: `Now␣is␣the␣time␣for␣it`

key (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

If no optional process is used the MAC consists of the m leftmost bits of (O_3).

Optional process 1

key (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

The MAC consists of the m leftmost bits of (O''_3).

Optional process 2

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

The MAC consists of the m leftmost bits of (O'_3).

Annex C

(informative)

Bibliography

[1] ISO 8731–1: 1987, *Banking - Approved algorithms for message authentication - Part 1: DEA.*

[2] ISO 9807: 1991, *Banking and related financial services - Requirements for message authentication (retail).*

[3] ISO/IEC 9979: 1991, *Data cryptographic techniques - Procedures for the registration of cryptographic algorithms.*

[4] ISO/IEC 10181–5:—[1], *Information technology - Open Systems Interconnection - Security Frameworks for Open Systems: Integrity Framework.*

[5] ANSI X3.92: 1981, *Data Encryption Algorithm.*

[6] ANSI X9.9: 1986, *Financial Institution Message Authentication (Wholesale).*

[7] ANSI X9.19: 1986, *Financial Institution Retail Message Authentication.*

[1)] To be published