INTERNATIONAL STANDARD

ISO/IEC 9797

First edition
1989-12-01

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

Techniques cryptographiques — Mécanisme d'intégrité des données utilisant une fonction de contrôle cryptographique employant un algorithme d'encodage par blocs

Reference number
ISO/IEC 9797 : 1989 (E)

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) together form a system for worldwide standardization as a whole. 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 approval before their acceptance as International Standards. They are approved in accordance with procedures requiring at least 75 % approval by the national bodies voting.

International Standard ISO/IEC 9797 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*.

Introduction

The calculation described in this International Standard is similar to that used in ISO 8731 – 1 and in the American 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. Thus the calculations of cryptographic check–values described in ISO 8731 and ANSI X9.9 are subsets of this International Standard with $n=64$ and $m=32$ using DEA (see ANSI X3 : 1981).

Data cryptographic 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 $n-bit$ algorithms in block cipher mode to calculate an $m-bit$ cryptographic check value that can be used as a data integrity mechanism to detect that data has not been altered in an unauthorised manner. The degree of integrity of the data 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 listed below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO 8731 – 1 : 1987, *Banking – Approved algorithms for message authentication – Part 01: DEA*

ANSI X3.92 : 1981, *Data Encryption Algorithm.*

ANSI X9.9 : 1986, *Financial Institution Message Authentication.*

3 Terminology

The cryptographic check value is variously described as
- a Message Authentication Code (MAC),
- a Message Integrity Code (MIC), or
- a Modification Detection Code (MDC).

This International Standard refers to the check value as a MAC.

4 Requirements

The value m will be less than or equal to the block size n. The result of the calculation and any optional process is an information block of the size n. The cryptographic check value is the left – most m bits of the final $n-bit$ block. Assuming an adequate strength in the algorithm, the larger the m value, the greater the protection.

5 Calculation of the MAC

5.1 The $n-bit$ cryptographic algorithm

The MAC is calculated as illustrated in figure 1. The data bits on D_1, for which the cryptographic check value is to be calculated, are divided into $n-bit$ blocks, $D_1, D_2, \ldots, D_{q-1}$ followed by a possibly incomplete block D_q.

5.2 The cryptographic key

The key should be randomly or pseudo randomly generated. The key should be changed periodically. 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 input register I_1 is initialised with the first n bits of data D_1 This input I_1 is passed through the algorithm, which uses the key K to produce n bits in the output register O_1.

5.4 Subsequent stages up to the final stage

The second n bits of the data D_2 are bitwise exclusive or'ed with the n bits in the output register O_1 and the result loaded into the input register as I_2. This process continues until n bits or fewer of the data for which the cryptographic check value is being calculated remain.

5.5 The final stage

The remaining bits are left justified and the final block, D_q of n bits is obtained by adding a "1" and as many zero bits as necessary. This block is then bitwise exclusive or'ed with the result in the output register O_{q-1}. The Result I_q is passed through the algorithm to produce the final output block of n bits O_q. If zero bits are added the recipient must either know the number needed beforehand or receive that number in a manner which ensures its integrity.

5.6 Optional Process

At this stage, O_q can be subject to further optional processing. For example, ANSI X9.9, using the same algorithm, deciphers O_q under a different secret key and further enciphers the result under the original key.

5.7 Truncation for $m <= n$

The cryptographic check value is derived by taking the leftmost m – bits of the final n – bit block.

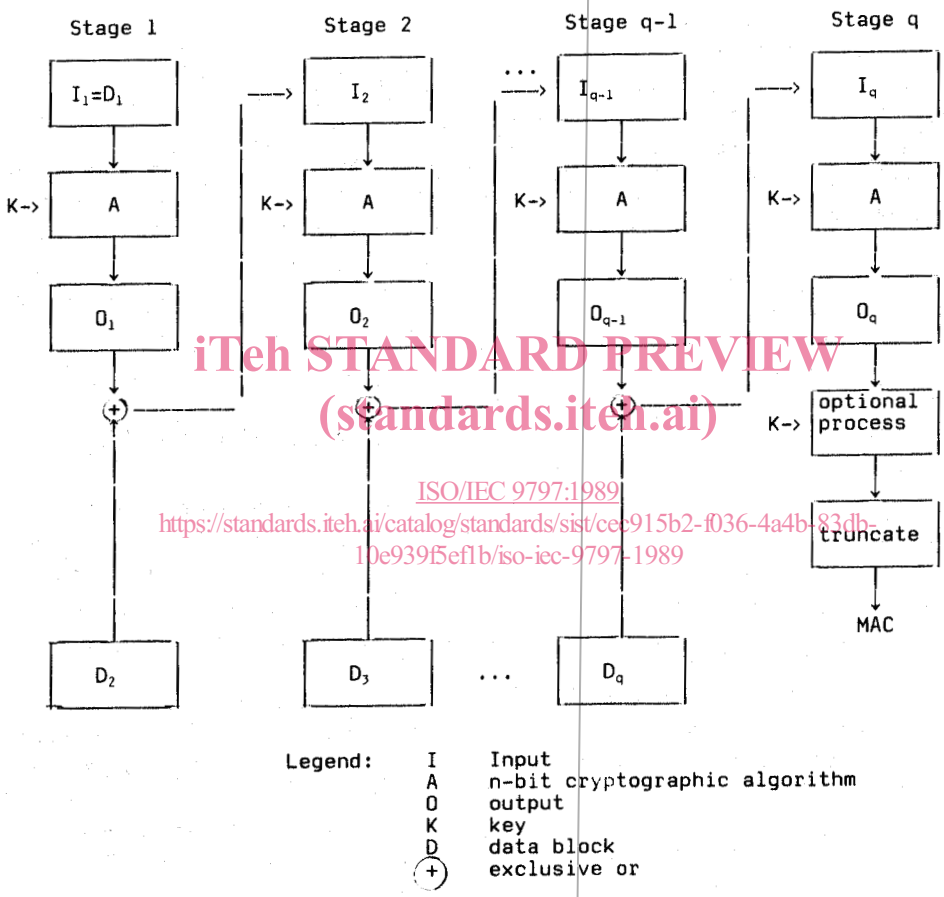

Figure 1 – The MAC calculation

Annex A
(informative)

Bibliography

ISO 2382-9 : 1984, *Data Processing — Vocabulary — Part 09 : Data Communication.*

ISO 7498 : 1984, *Information processing systems— Open Systems Interconnection — Basic Reference Model.*

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

ISO 9979 : —[1)], *Data cryptographic techniques — Procedures for the registration of cryptographic algorithms.*

1) To be published.

UDC 681.3.04 : 003.26

Descriptors : data processing, coded representation, data converting, algorithms, checking functions.

Price based on 3 pages