INTERNATIONAL STANDARD

ISO
8731-1

First edition
1987-06-01

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
ORGANISATION INTERNATIONALE DE NORMALISATION
МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ

Banking — Approved algorithms for message authentication —

Part 1 : DEA

Banque — Algorithmes approuvés pour l'authentification des messages —

Partie 1 : DEA

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work.

Draft International Standards adopted by the technical committees are circulated to the member bodies for approval before their acceptance as International Standards by the ISO Council. They are approved in accordance with ISO procedures requiring at least 75 % approval by the member bodies voting.

International Standard ISO 8731-1 was prepared by Technical Committee ISO/TC 68, *Banking.*

Users should note that all International Standards undergo revision from time to time and that any reference made herein to any other International Standard implies its latest edition, unless otherwise stated.

Printed in Switzerland

Banking — Approved algorithms for message authentication —

Part 1 : DEA

0 Introduction

ISO 8731 specifies, in individual parts, approved authentication algorithms. Every algorithm has been approved as meeting the authentication requirements specified in ISO 8730.

1 Scope and field of application

This part of ISO 8731 deals with the Data Encryption Algorithm (DEA) as a method for use in the calculation of the Message Authentication Code (MAC).

While it may be implemented in software, hardware implementations of DEA operate at substantially higher speeds.

2 References

ISO 8730, *Banking — Requirements for message authentication (wholesale).*

ANSI X3.92-1981, *American National Standard for Information Systems — Data Encryption Algorithm.*

ANSI X3.106-1983, *American National Standard for Information Systems — Data Encryption Algorithm — Mode of operation.*

ANSI X9.9-1982, *Financial Institution Message Authentication (Wholesale).*

3 Source of algorithm DEA

DEA is published as ANSI X3.92.

ANSI X3.92 specifies that key bits 8, 16, 24, 32, 40, 48, 56 and 64 shall be used as odd-parity bits for the octets in which they occur. For the purposes of this International Standard the use of these bits is not specified.

4 Specification of algorithm

4.1 DEA cryptographic key

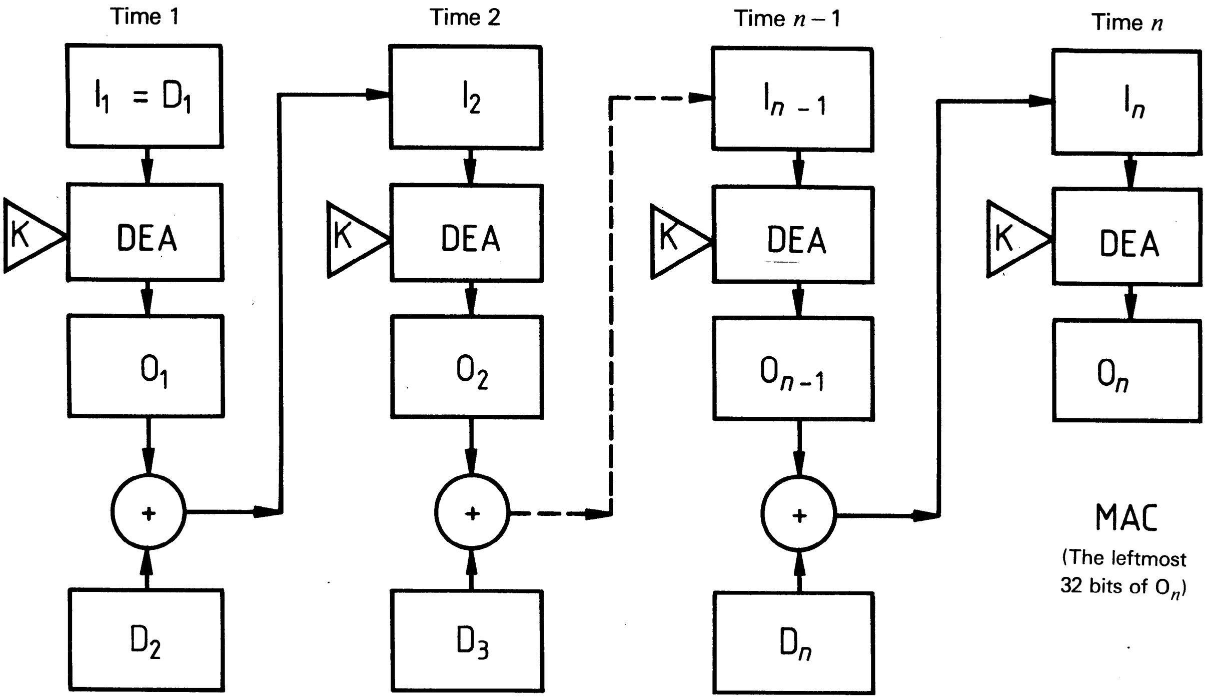
A DEA cryptographic key consists of 64 bits, 56 of which are used by the authentication algorithm (forming the active key) and 8 of which are available to detect errors within the key. If the 64 bits are numbered from left to right (1, 2, ..., 64), bits 8, 16, 24, ..., 64 are for odd parity checking.

When a DEA key is written, it shall be represented by eight pairs of hexadecimal characters with each pair separated by a space (hh hh hh hh hh hh hh hh).

The active key shall be randomly or pseudo-randomly generated. The entire 64-bit key shall be protected from all unauthorized parties throughout its active life. Keys shall be changed from time to time.

4.2 Generating the Message Authentication Code (MAC) using the DEA

The MAC is generated as illustrated in the figure. The DEA shall be used in the cipher block chaining modes of operation with the initialization vector set at zero as specified in ANSI X3.106-1983. The input register (I_1) (see the figure) is initialized with the first 64 bits of data (D_1) to be authenticated. This input is passed through the DEA which uses an authentication key (K) to produce 64 bits in the output register (O_1). The second 64 bits of data (D_2) to be authenticated are modulo-2 added with the 64 bits in the output register, the result being loaded into the input register (I_2). This process continues until 64 or fewer bits remain to be authenticated. These remaining bits shall be left-justified and zeros shall be appended to form a 64 bit data block (D_n). This block is then modulo-2 added with the 64 bits in the output register. The result (I_n) is passed through the DEA producing the final 64 bit output block (O_n). The leftmost 32 bits of final output (O_n) shall be taken as the MAC. An example of the MAC computation is given in ANSI X9.9.1982.



Legend

I	: Input
DEA	: Data Encryption Algorithm (encryption mode)
O	: Output
K	: DEA key
D	: Data block
+	: modulo-2 addition

Figure — Authentication algorithm

UDC 681.3.04 : 336.717

Descriptors : banking, banking documents, messages, data processing, authentication.

Price based on 2 pages