14

SLS 1053 : 1995
(ISO 8730 : 1990)

Sri Lanka Standard

BANKING - REQUIREMENTS FOR MESSAGE AUTHENTICATION (WHOLESALE)

Gr. M

SRI LANKA STANDARDS INSTITUTION

SLS 1053 : 1995
ISO 8730 : 1990

Sri Lanka Standard
BANKING - REQUIREMENTS FOR MESSAGES AUTHENTICATION (WHOLESALE)

NATIONAL FOREWORD

This standard was finalized by th Sectoral Committee on Information Technology and was authorized for adoption and publication as a Sri Lanka Standard by the Council of the Sri Lanka Standards Institution on 1995-05-25.

This Sri Lanka Standard is identical with ISO 8730 : 1990 Banking -Requirements for message authentication (wholesale), published by the International Organization for Standardization (ISO).

Terminology and conventions

The text of the International standard has been accepted as suitable for publication, without deviation, as a Sri Lanka Standard. However, certain terminology and conventions are not identical with those used in Sri Lanka Standards, attention is therefore drawn to the following:

a) Wherever the words 'International Standard/publication' appear, referring to this standard they should be interpreted as "Sri Lanka Standard".

Wherever page numbers are quoted, they are ISO page numbers.

CROSS - REFERENCES

International Standards	Corresponding Sri Lanka Standards
ISO 7746 : 1988, Banking - Telex formats for interbank payment messages	SLS 1051 : 1995 Banking - Telex formats for interbank payment messages
ISO 7982 - 1 1987, Bank telecommunication- Fund transfer messages- Part 1, Vocabulary and data	SLS 1045 : 1995 Bank telecommuni-cation - Fund, transfer messages - Part 1 : Vocabulary and data
ISO 8731- 1 1987, Banking - -Approved algorithms for message authentication - -Part 1 : DEA	SLS 1054 : 1995,Banking - Approved algorithms for message authentication - Part 1 : DEA
ISO 8732 : 1988, Banking - Key management (wholesale)	SLS 1055 :1995, Banking - Key management (wholesale)
ISO 10126-1 : 1991, Banking - Procedures for message encipherment (wholesale)- Part 1 : Generazl principles	SLS 1058 : Part 1 : 1995, Banking - Procedures for message encipherment (wholesale) - Part 1 : General principles
SO 10126-2 : 1991, Banking - Procedures for message encipherment (wholesale)- Part 2 : Algorithm	SLS 1058 : Part 2 : 1995, Banking -Procedures for message encipher -ment (wholesale) - Part 2 Algorithm

-/ltf.

INTERNATIONAL STANDARD

ISO 8730

Second edition
1990-05-15

Banking — Requirements for message authentication (wholesale)

Opérations bancaires — Spécifications liées à l'authentification des messages

Reference number
ISO 8730 : 1990 (E)

Contents

Annexes

International Organization for Standardization
Case postale 56 • CH-1211 Genève 20 • Switzerland
Printed in Switzerland

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. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 8730 was prepared by Technical Committee ISO/TC 68, *Banking and related financial services.*

This second edition cancels and replaces the first edition (ISO 8730: 1986), which has been technically revised to provide an enhancement of the facilities provided in that edition.

These enhanced facilities are already available in ANSI X9.9, published in August 1986, and the new text maintains consistency with the published ANSI text.

Specific changes introduced in this edition are

a) Data presented for authentication may be formatted in one of five different ways. This selection process allows users to authenticate messages in the format option most suitable for the transmission process used. Correspondents must now agree upon the format option for authentication of any particular message, but this will generally be no major imposition on these parties since the mode selection will be determined by the choice of transmission process;

b) Introduction of a new field for identifying the authentication key used (IDA field);

c) Several definitions have also been changed to ensure consistency across related TC 68 International Standards.

Four new annexes have also been introduced, all of which are intended to simplify implementation of this International Standard.

a) Annex B describes the risks associated with the unintentional introduction of control characters during a reformatting process, and how such risks may be minimized;

b) Annexes D and E provide examples of authentication calculations using the algorithms specified in ISO 8731: 1987, Parts 1 and 2;

c) Annex F describes a means of applying this International Standard to a telex payment order formatted in accordance with the requirements of ISO 7746.

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

Introduction

A Message Authentication Code (MAC) is a data field transmitted with a financial message passing between correspondent financial institutions. It is derived from the whole message, or from specified data elements in the message which require protection against alteration, whether such alteration arises by accident or with intent to defraud.

For any form of alteration the level of protection provided for a given algorithm is related to the length of the Message Authentication Code and of the authentication key, and to the extent to which the two correspondents are able to keep their authentication key secret. Operation of this International Standard implies acceptance of this responsibility by the correspondent parties. Approved algorithms are listed and specified in ISO 8731. Techniques for wholesale key management are specified in ISO 8732. For fraudulent attack, the mathematical security of a standard algorithm is calculated on the assumption that the potential code breaker has an arbitrary large number of plaintext messages each containing its associated MAC derived from an unchanged authentication key. The security is determined by the computational power required for the authentication key to be determined by the code breaker and by the length of the MAC.

Banking — Requirements for message authentication (wholesale)

1 Scope

This International Standard is designed for use by correspondent institutions exchanging financial messages. It may be used to authenticate messages using any wire service or other mode of communication.

This International Standard specifies methods to be used for protecting the authenticity of wholesale financial messages passing between institutions (e.g. between banks, between a bank and a corporate customer or government), by means of a Message Authentication Code (MAC). It specifies the method by which authentication algorithms are to be approved for inclusion in ISO 8731. Application of this International Standard does not protect against internal fraud by sender or receiver, e.g., forgery of a MAC by the receiver.

This International Standard specifies a technique for protecting either the whole of the message or specified elements within it. Data presented for authentication may be formatted in one of five optional forms. These specifications may be supplemented by a group of financial institutions with a community of interest who have established their own operational arrangements (e.g., a banking consortium, a geographical grouping, an operating network, an industry-wide agreement). Selection of the appropriate option permits the authentication of messages in a manner compatible with the transmission process used.

Integrity protection applies only to the selected authentication elements. Other parts of the message are subject to undetected alterations. Assuring the integrity of the presentation of the data is the responsibility of the users (see annex B). This International Standard provides a means for protection against duplication and loss, and a method is described in annex C.

This International Standard is designed for use with symmetric algorithms where sender and receiver use the same key. It is intended that provision will, in due course, be made to cover the use of asymmetric algorithms. The authentication method is applicable to messages formatted and transmitted both as coded character sets and as binary data.

The standard does not specify methods of protecting against unauthorized reading and monitoring. Such protection may be achieved by encipherment of the message as described in ISO 10126 [1].

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. Member of IEC and ISO maintain registers of currently valid International Standards.

ISO 646:1983, *Information processing — ISO 7-bit coded character set for information interchange.*

ISO 7746:1988, *Banking — Telex formats for inter-bank messages.*

ISO 7982-1:1987, *Bank telecommunication — Funds transfer messages — Part 1: Vocabulary and data.*

ISO 8601:1988, *Data elements and interchange formats — Information interchange — Representation of dates and times.*

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

ISO 8732:1988, *Banking — Key management (wholesale).*

ISO 10126-1: —[1], *Banking — Procedures for message encipherment (wholesale) — Part 1: General principles.*

ISO 10126-2: —[1], *Banking — Procedures for message encipherment (wholesale) — Part 2: Algorithms.*

3 Definitions

For the purpose of this International Standard the following definitions apply. Terms printed in italic in the definitions are defined elsewhere in this clause.

3.1 algorithm: A specified mathematical process for computation; a set of rules which, if followed, will give a prescribed result.

3.2 authentication: A process used, between a sender and a receiver, to ensure *data integrity* and to provide *data origin authentication.*

[1] To be published.

3.3 authentication algorithm: An *algorithm* used, together with an *authentication key*, and one or more *authentication elements*, for *authentication*.

3.4 authentication element: A *message element* that is to be protected by *authentication*.

3.5 authentication key: A cryptographic key used for authentication.

3.6 beneficiary; beneficiary party(ies): The ultimate party (or parties) to be credited or paid as a result of a transfer.

3.7 bias: The condition where, during the generation of random or pseudo- random numbers, the occurrence of some numbers is more likely than others.

3.8 cryptoperiod: A defined period of time during which a specific cryptographic key is authorized for use, or during which time the cryptographic keys in a given system may remain in effect.

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

3.10 Date MAC Computed (DMC): The date on which the *sender* computed the *Message Authentication Code*. This date may be used to synchronize the authentication process through selection of the proper key.

3.11 data origin authentication: The corroboration that the source of data received is as claimed.

3.12 decipherment: The reversal of a corresponding reversible *encipherment*.

3.13 decryption: see *decipherment*.

3.14 delimiter: A group of characters used to delineate the beginning and end of a data field or fields.

3.15 dual control: A process of utilizing two or more separate entities (usually persons), operating in concert, to protect sensitive functions or information whereby no single entity is able to access or utilize the materials, e.g., cryptographic key.

3.16 encipherment: The cryptographic transformation of data to produce ciphertext.

3.17 encryption: see *encipherment*.

3.18 hexadecimal digit: A single character in the range 0-9, A-F (upper case), representing a four bit string, as follows:

Binary	Decimal	Hexadecimal
0000	0	0
0001	1	1
0010	2	2
0011	3	3
0100	4	4
0101	5	5
0110	6	6
0111	7	7
1000	8	8
1001	9	9
1010	10	A
1011	11	B
1100	12	C
1101	13	D
1110	14	E
1111	15	F

3.19 Identifier for Authentication Key (IDA): A field that identifies the key to be used in authenticating the message.

3.20 Message Authentication Code (MAC): A code in a message between a sender and a receiver used to validate the source and part or all of the text of the message. The code is the result of an agreed calculation.

3.21 message element: A contiguous group of characters designated for a specific purpose.

3.22 Message Identifier (MID): A field used uniquely to identify a financial message or transaction (e.g., sending bank's transaction reference).

3.23 message text: Information being conveyed or transmitted between *sender* and *receiver*, excluding header and trailer information used for transmission purposes.

3.24 receiver: The institution or other entity responsible for, and authorized to, receive a message.

3.25 sender: The institution or other entity responsible for, and authorized to, send a message.

3.26 value date: Date on which funds are to be at the disposal of the beneficiary.

3.27 wire service: Any telecommunication service over which messages or transmissions may be sent between subscribers.

4 Protection

4.1 Protection of the identity of the sender

To prevent misuse of the sender's identity the authentication key shall both be protected and restricted to use by only the sending and receiving parties (or their authorized agents).

4.2 Authentication elements

4.2.1 The following authentication elements shall always be included in the calculation of the MAC:

a) Date MAC computed (DMC);

b) Message identifier (MID).

4.2.2 The following authentication elements shall be included in the calculation of the MAC whenever they appear in the message:

a) Transaction amount;

b) Currency;

c) Identifier for Authentication Key (IDA);

d) Identification of parties to be credited and debited;

e) Identification of beneficiary party;

f) Value date.

4.3 Protection of total message

Where correspondents wish to protect the whole text of the message the authentication process shall be applied to the whole text (see 6.5 and 6.7).

4.4 Protection against duplication or loss

To protect against duplication or loss, a unique transaction reference (or message identifier) shall be used. The Message Identifier, (MID), is a value that does not repeat before either (i) the change of date (i.e. Date MAC Computed); or (ii) the expiration of the cryptoperiod of the key used for authentication, whichever occurs first, i.e., there must not be more than one message with the same date and the same message identifier that uses the same key. This requirement may be satisfied by the inclusion of a unique sending bank's transaction reference number in a fixed format message as a message identifier. In free format messages, the MID field shall be delimited in accordance with this International Standard (see 6.3.1). A method of protection is described in annex C.

5 Generation and checking of the Message Authentication Code (MAC)

5.1 Generation

The sender of a message shall generate a MAC by processing (in the sequence in which they appear in the message) those authentication elements of the transmitted message that are to be protected by an approved authentication algorithm (see ISO 8731). The algorithm shall be activated by means of an authentication key, which is a secret between the two correspondents. This process creates the MAC, which shall then be included with the original message text as an additional data field.

5.2 Checking

On receipt of the message the receiver shall compute a reference MAC using the authentication elements, an identical authentication key and an identical algorithm. Authenticity of the content of the authentication elements and the message source are confirmed when the receiver's computed reference MAC agrees with that transmitted with the message text.

A received MAC (and its delimiters) shall not be included in the algorithm computation.

When a received MAC does not equal the computed reference MAC, failure to authenticate shall be indicated in accordance with 6.9.2.

The process of generating the MAC is sensitive to the sequence in which the authentication elements are processed, i.e., a change in the sequence of authentication elements after the MAC is generated will result in a failure to authenticate.

Message authentication keys shall not be used as encipherment keys.

6 Procedures for message authentication

6.1 Authentication process

Correspondents shall agree upon the algorithm to be applied and they shall also exchange a secret authentication key. The sender shall calculate a MAC using these elements. This MAC shall be appended to the text of the transmitted message in such a way that it is identifiable by the receiver. (For free format messages see 6.3.3.) The receiver repeats the computation, using the same authentication method as defined in this section. The message authenticates if the received and computed reference MACs are identical.

6.2 Format options

This International Standard provides five options for the format of data to be authenticated:

1) binary data; (6.4);

2) coded characters; (6.5);
entire message
text; no editing

3) coded characters; (6.6);
extracted message
elements; no editing

4) coded characters; (6.7);
entire message
text; editing

5) coded characters; (6.8);
extracted message
elements; editing

Option 1 is designed for the authentication of a binary string of data.

Options 2 and 3 are designed for the authentication of data in coded character sets whenever the transmission medium provides character set transparency, e.g., systems and networks designed in accordance with the open systems interconnection (OSI) model.

Options 4 and 5 are designed for the authentication of data in a restricted coded character set for use whenever the transmission medium is not transparent to the character set being used, e.g., baudot, telex, and store and forward services such as those provided by many international record carriers.

Choice of the format option is the responsibility of the correspondents and shall be subject to bilateral agreement.

6.3 Codes character sets (as used in options 2 to 5)

6.3.1 Defined message element formats

The field formats for Date MAC Computed, Identifier for Authentication Key, Message Authentication Code, and Message Identifier are represented in the form specified in this International Standard. Formats of other message elements are not specified.

The field formats shall be verified as part of the authentication process. If an authentication option that employs editing is used, then the field formats shall be verified prior to editing. If a formatting error occurs, the message will fail to authenticate. The following field formats are defined:

a) Date MAC Computed (DMC). The date on which the sending institution originates the message shall be expressed in accordance with ISO 8601 as year, month, day (preferably compacted, i.e., YYMMDD); for example 851101 for 1 November 1985;

b) Identifier for Authentication Key (IDA). This field is the identifier of the key for authentication which shall conform to the requirements for key identifiers specified in ISO 8732;

c) Message Authentication Code (MAC). The MAC shall be expressed as eight hexadecimal digits written in two groups of four, separated by a space (hhhhbhhhh); for example, 5A6Fb09C3;

d) Message Identifier (MID). The message identifier shall be expressed as one to sixteen printable characters (aaaaaaaaaaaaaaaa). Permitted characters are 0-9, A-Z (upper case), space (b), comma (,), fullstop (.), solidus (/), asterisk (*) and hyphen (-); for example, FN-BC/2.5.

6.3.2 Implicit field delimiters

Implicit delimitation of an authentication element may be achieved if its position in the message is fixed or unambiguously identified by standardized format rules. Field names, numbers, or identifying field tags, where specified by the wire service as implicit delimiters, shall be processed for authentication.

6.3.3 Explicit field delimiters

Explicit delimiters may be used to identify the beginning and end of message elements, including the MAC. They may be used in all coded character set options. The following explicit delimiters are specified:

a) Date MAC computed (DMC): QD- and -DQ, for example, QD-YYMMDD-DQ;

b) Identifier for Authentication Key (IDA) QK- and -KQ, for example, QK-1357BANKATOBANKB-KQ;

c) Message Authentication Code (MAC): QM- and -MQ, for example, QM-hhhhbhhhh-MQ;

d) Message Identifier (MID): QX- and -XQ, for example, QX-aaaaaaaaaaaaaaaa-XQ;

e) Other message elements: QT- and -TQ, for example, QT-text-TQ.

The "text" delimited in QT-text-TQ may be of any length allowed by the wire service.

6.3.4 Use of delimiters

Beginning and ending delimiters, when present, shall occur in complementary pairs without intervening explicit delimiters.

> NOTE - if this condition is not satisfied, the message will fail to authenticate.

The message may contain any number of delimited "text" fields; however, the DMC, MID, IDA, and MAC fields shall not appear more than once each in a message.

The hyphen (-) shall appear in all explicit delimiters.

6.3.5 Character representation

All characters of authentication elements which are input to the algorithm shall be represented as 8-bit characters comprising the 7-bit code of ISO 646 (excluding national character assignments) preceded by a zero (e.g., 0, b7, b6, ...b1). Where this necessitates a code translation, the translation shall be for internal computational purposes only. If the message is transformed into a different character set, the inverse transformation must be applied before beginning the authentication process.

6.3.6 Header and trailer information

Header and trailer message information added (e.g., by a network) for transmission purposes shall be omitted, i.e., shall not be part of the message text nor be included in the algorithm calculation.

6.4 Option 1: Binary data

The authentication algorithm shall be applied to the entire message text, or to parts of the message text, according to a bilateral agreement between the sender and the receiver.

6.5 Option 2: Coded characters; entire message; no editing

Where message processing is automated and the precise content of the body of the message does not change between sender and receiver, the algorithm can be applied to the entire message.

The MAC is computed over the entire message text (see example in annex D).

6.6 Option 3: Coded characters; extracted message elements; no editing

6.6.1 Use

Where authentication of the entire message is impractical, the authentication algorithm shall be applied only to the selected message elements.

The message elements shall be extracted according to the rules of 6.6.2. A MAC shall be computed on the extracted elements, taken in the order in which they appear (see example in annex D).

6.6.2 Extraction of message elements

Message elements to be authenticated shall be extracted in accordance with the following rules:

6.6.2.1 Delete all characters other than the message elements and their corresponding delimiters.

6.6.2.2 Insert a single space after each implicitly delimited message element.

6.7 Option 4: Coded characters; entire message; editing

6.7.1 Use

The MAC shall be computed on the message text following editing according to the rules of 6.7.2 (see example in annex D).

6.7.2 Editing

The following editing rules shall apply, in the sequence shown, on all message elements - implicitly and explicitly delimited - before processing by the authentication algorithm:

6.7.2.1 Each carriage return and each line feed shall be replaced by a single space.

6.7.2.2 Lower case alphabetic characters (a-z) shall be translated to upper case (A-Z).

6.7.2.3 Any characters other than the letters A-Z, digits 0-9, space, comma (,), fullstop (.), solidus (/), asterisk (*), open and close parentheses, and hyphen (-) shall be deleted; thus end-of-text, and other formatting and control characters shall be deleted.

6.7.2.4 All leading spaces shall be deleted.

6.7.2.5 Each sequence of consecutive spaces (internal and trailing) shall be replaced by a single space.

6.8 Option 5: Coded characters; extracted message elements; editing

6.8.1 Use

See 6.6.1.

6.8.2 Extraction of message elements

The extraction rules of 6.6.2 shall be applied.

6.8.3 Editing

The editing rules of 6.7.2 shall be applied.

6.9 "Failed" Message Authentication Code (MAC)

6.9.1 Inability to generate MAC

When the MAC is automatically generated, i.e., by automatic extraction of authentication elements, the process may fail because of rule violations (e.g., due to nested delimiters). In that event, where human readability is required (e.g., paper, screen, or microfiche) as a minimum the failure shall be indicated by eight spaces (if available) written in two groups of four, separated by a character that is not a hexadecimal digit, preferably an asterisk, e.g., bbbb*bbbb. Where spaces are not available, zeros shall be substituted (i.e., 0000*0000).

6.9.2 Received MAC does not authenticate

When a received MAC does not equal the reference MAC generated during the authentication process, where human readability is required, failure to authenticate shall be indicated by the insertion of a non-hexadecimal printable character in place of the space in the received MAC. Where available in the character set, an asterisk shall be used, for example, 5A6F*09C3.

6.10 Authentication keys

Authentication keys are secret cryptographic keys that have been previously exchanged by the sender and receiver and are used by the authentication algorithm. Such keys shall be randomly or pseudo-randomly generated (see annex G). Keys used for message authentication shall not be used for any other purpose. Any key used for authentication shall be protected against disclosure to unauthorized parties.

7 Approval procedure for authentication algorithms

Before an authentication algorithm is authorized for inclusion in ISO 8731, it shall satisfy both of the following basic requirements:

a) Be designed to serve a purpose not already covered by ISO 8731 (for example, be suitable for a different operational environment, provide significant cost savings in implementation or in operation, offer a greater degree of protection);

b) Be sufficiently secure to serve its stated purpose.

Annex A describes the way in which these objectives shall be achieved.

Annex A
(normative)

Procedure for review of alternative authentication algorithms

A.1 Origination

An alternative authentication algorithm which is to be proposed for incorporation in ISO 8731 shall be submitted by, or with the approval of, a national standards body, to the Secretariat of ISO/TC 68.

A.2 Justification of proposal

The originator shall justify a proposal by describing

a) The purpose the proposal is designed to serve;

b) How this purpose is better achieved by the proposal than algorithms already in ISO 8731;

c) Additional merits not described elsewhere;

d) Experience in use with the new algorithm.

A.3 Documentation

The proposed algorithm shall be completely documented when submitted for consideration. The documentation shall include:

a) A full description of the algorithm proposed;

b) A clear acknowledgement that the algorithm satisfies, or is compatible with, all the requirements contained in this International Standard;

c) A logic flow diagram showing the processing steps used to compute the MAC;

d) A definition and explanation of any new terms, factors, or variables introduced;

e) Authentication key requirements, usage, and handling;

f) A step-by-step computation example illustrating the computation of the MAC using the standard example message (see annex D);

g) Detailed information on any prior testing to which the proposed algorithm has been subjected, particularly concerning its security, reliability and stability. Such information shall include an outline of the testing procedures used, the results of the tests, and the identity of the agency or group performing the tests and certifying the results (that is, sufficient information shall be provided to enable an independent agency to conduct the same tests and to compare the results achieved).

A.4 Public disclosure

Any algorithm submitted for consideration shall be free from security classification. If copyright patent application has been made on the algorithm, it shall be assessed in accordance with IEC/ISO procedures[1]. All documentation of the algorithm shall be considered public information available to any individual, organization or agency for review and testing.

A.5 Examination of proposals

Each new proposal will be examined by ISO and a report on it prepared within 180 days of receipt (see A.6). The report shall state if the proposal is adequately documented, if it has been properly tested and certified already, and if the proposed algorithm satisfies the conditions and requirements of the International Standard. The examination may also recommend submission of the proposal for public review (A.6).

A.6 Public review

When the report (A.5) recommends that public review is necessary, proposals considered suitable for acceptance shall be forwarded (with the consent of the originator) to selected agencies and institutions with an international reputation in this field. These agencies and institutions will be requested to examine and report on the proposals within 90 days of receipt.

NOTE - This period of public review may extend the 180 days allowed for preparation of the report on the proposal (see A.5).

[1] Currently, the IEC/ISO Directives, part 2, *Methodology for the development of International Standards*, first edition (1989), annex A.

A.7 Appeal procedure

Originators whose proposals are rejected (see A.5) may ask the Secretariat of ISO/TC 68 to have the proposals subjected to public review (see A.6) if this has not already been done. If, following submission of the public review reports, rejection is still recommended, the originator may request the TC 68 Secretariat to circulate the proposal, together with copies of all relevant reports on it, for ballot by the P-members of the technical committee whose ruling in the matter by a simple majority of those voting shall be final.

A.8 Incorporation of new authentication algorithms

New algorithms for authentication recommended for acceptance, together with relevant reports on them, shall be circulated for letter ballot as proposed amendments to ISO 8731.

A.9 Maintenance

An algorithm approved by the method described in this International Standard shall be reviewed by ISO/TC 68 at intervals of not greater than five years.

Annex B

(informative)

Risks associated with communications control characters

B.1 Purpose

As stated in the scope of this International Standard, assuring the integrity of the presentation of the data is the responsibility of the user. Control of the presentation of data (e.g., printing, display) is outside the scope of this standard. It is the purpose of this annex to highlight some of the risks associated with communication control characters and to provide some possible solutions to these problems.

The problem occurs when the message that is presented differs significantly from the message data that is actually passed to the MAC algorithm. Even though the message authenticates correctly, the presentation of the data gives a false impression of the original message. These cases can occur because messages may be presented before editing, parts of the presented message may not be authenticated, and presentation devices do not present data in a consistent manner.

Protection against the variations discussed in B.2 and B.3 below can be provided if the MAC is calculated on unedited text (see 6.5 and 6.6) and no additional editing is done before presentation. However, this option implies that the network does not modify control characters and that the devices are consistent at both ends.

The selection of a format option to protect against the insertion of presentation control characters is an important operational decision. Choices are dependent upon many factors such as manual vs. automated processing, hardware vs. software authentication, formatted vs. unformatted messages, non-intelligent vs. intelligent terminals, one-way vs. two way communications, the availability of an audit trail, and many others.

The final solution must be an individual user decision, based on the characteristics of the given environment.

B.2 Insertion and deletion of characters in authenticated text

The editing rules (see 6.7.2) state that each carriage return and each line feed is replaced by a single space, and each sequence of consecutive spaces is replaced by a single space. Therefore, these characters may be inserted next to other such characters or deleted if next to other such characters without affecting the authentication.

When such modifications are made, the message as presented may appear quite different from the message received. For example, if CR represents a carriage return then "123 456" and "123 CR456" would have the same MAC. The former message would appear as "123 456" while the latter may appear as "456" on some terminals.

B.3 Insertion and deletion of characters in unauthenticated text

This International Standard allows for the authentication of message elements only. In this case, it may be possible to insert or delete characters in any text which is not selected for authentication (including parts of message elements) such that the authenticated text appears different from the same text in the original message. An escape sequence may be placed in unauthenticated text which will cause an authenticated field, such as the transaction value field, to be overwritten when the entire message is displayed. Note that this problem is independent of the editing rules.

For example, on some terminals escape sequences may be inserted at the end of the message to overwrite the authentication text. These escape sequences perform absolute cursor addressing to selectively replace the dollar amount.

```
QD-850327-DQ      QK-KEY1-KQ          QX-MSG1-XQ
QT-$12000-TQ      QM-2EB7 2F98-MQ     -[▬"G99999-[▬"
```

The altered message is authenticated using one of the format options. When displayed on the screen, the dollar amount appears as $99999. Since the escape sequences (-[▬"G) and (-[▬") were inserted into the message outside of the message elements, they are not authenticated and the computed MAC is identical to the MAC computed for the original unaltered message.

B.4 Presentation device inconsistencies

An unaltered message may appear differently on one presentation device than on another. For example, a message of "123CR456" may appear as two lines, the first being "123" and the second being "456" or the message may appear as only the single line of "456".

B.5 Alternative processing solutions

Some (of an unlimited number of) solutions to overcoming display-related problems are dependent upon the conditions in the processing environment.

1) In format options 4 and 5, any characters other than the ones allowed in 6.7.2 will not be present in the transmitted data. The sender should perform the functions of all these characters before passing the data through the algorithm. The resulting message data would then be transmitted without these characters. This rule applies to all data, not just authentication elements;

2) If any implementation requires special characters, such as backspace, to be present in the transmitted data, then the receiver must execute the function of the special characters prior to passing the data through the authentication algorithm;

3) A pre-determined control character set can be defined. Any deviation from this set would trigger an error condition. If certain combinations of characters are required, they could also be validated. For example, if line feed always precedes carriage return, then a line feed alone would cause an error. Similarly, if the escape character is considered dangerous, it could be excluded from the allowable character set;

4) Elements which have been authenticated could be separated from non-authenticated data on different screens or pieces of hard copy;

5) Any format control characters could be ignored if present. The recipient would independently perform all formatting.

Annex C
(informative)

Protection against duplication and loss

C.1 Purpose

This annex describes a method to detect duplication and loss of transmitted messages by using the "Date MAC Computed" (DMC) and "Message Identifier" (MID) as authentication elements.

C.2 Protection against duplication

C.2.1 Duplicated messages may be detected if under normal operation the MID from a given sender does not repeat for a given date and a given key. The receiver must check the MID to ensure that it did not appear in a previous message. This check may be performed in one of the following ways:

a) If MIDs are sent in no predetermined order, thenthe receiver may compare the received MID against a list of the MIDs received for the day;

b) If the MIDs for messages authenticated under a particular key are always sent in increasing order, the receiver need only check that the identifiers are strictly increasing.

Other methods, including variations of those just described, may also be devised. Windows may be necessary, and techniques of window management are given in ISO 8732: 1988, annex D.

C.2.2 When two parties share a common key ("Multi-party operation"), duplication may be detected if each party uses a mutually exclusive portion of the possible MIDs. The receiving party checks that the MID is in the proper range and has not already been received.

C.2.3 When the identities of both the sending and receiving parties are included as authentication elements in each message, the receiving party need check only that it is the intended receiver and that the MID has not appeared previously in a message from the sending party. In this case, the entire range of MIDs may be used by each sending and receiving pair, and MIDs may repeat between different pairs.

C.3 Loss protection

Loss of a transmitted message may be detected if both the sending and receiving parties keep a list of all MIDs used in a given time. One party sends its list (via an authenticated message which has duplication protection) to the party wishing to detect any loss. A comparison of the two lists is then performed. Alternatively, if the MIDs are to be received in sequence, the receiver may detect a lost message as soon as an out-of-sequence MID is received. The last MID for a day may be sent to the loss detecting party by way of an authenticated message which has duplication protection. Other methods, including variations of those just described, may also be devised.

Annex D
(informative)

Example of message authentication for coded character sets: DEA

D.1 Purpose

This annex presents examples of the entire authentication process, including extraction of message elements, editing, and the MAC computation, for each of the four coded character set options in this International Standard, using the algorithm in ISO 8731, Part 1, DEA.

D.2 Example message

The following message will be used as an example for each of the options. The MACs computed in D.4 to D.7 are each substituted in place of "XXXX XXXX" in the MAC field. This demonstrates how the value of the MAC changes, using the different authentication options in this International Standard.

```
TO YOUR BANK
FROM OUR BANK
QD-80 07 14-DQ ///// 1056/  QX-127-XQ
QT-

TRNSFR USD $1234567,89 FRM ACCNT 48020-166
            /////    TO ACCNT 40210-178

-TQ

KEEP ON QT EXPECT VISIT ON FRIDAY OF
NEW DIV VP ON PROJECT QT-QWERT-TQ BE CAREFUL

REGARDS

QUIRTO
QK-1357BANKATOBANKB-KQ
QM-XXXX XXXX-MQ
```

D.3 Example cryptographic key

E6 A1 2F 07 9D 15 C4 37

D.4 OPTION 2: Coded characters; entire message; no editing (see 6.5)

D.4.1 Resulting authentication element

The processing of the example message would result in the following authentication element. It is identical to the original message, except that the MAC and its delimiters are not included, and the parity bit for each character is set to zero.

The explicit delimiters are used to locate and identify particular message elements. Mismatched delimiters, intervening delimiters, or an invalid message element format would result in a failure to compute the MAC.

TO YOUR BANK

FROM OUR BANK

QD-80 07 14-DQ ///// 1056/ QX-127-XQ

QT-

TRNSFR USD $1234567,89 FRM ACCNT 48020-166
///// TO ACCNT 40210-178
-TQ

KEEP ON QT EXPECT VISIT ON FRIDAY OF
NEW DIV VP ON PROJECT QT-QWERT-TQ BE CAREFUL

REGARDS

QUIRTO
QK-1357BANKATOBANKB-KQ

D.4.2 MAC Computation

First Data Block: 0A202020544F2059 (ISO 646 representation of linefeed,space,space,space,T,O,space,Y).

TIME	DES IN	DES OUT	DATA	DATA+OUT=FEEDBACK
1	0A202020544F2059	1CAB5BC75CD5D7D4	4F55522042414E4B	53FE09E71E94999F
2	53FE09E71E94999F	E2C5ED33A60E8594	0A0A20202046524F	E8CFCD138648D7DB
3	E8CFCD138648D7DB	CDCA93439001329C	4D204F5552204241	80EADC16C22170DD
4	80EADC16C22170DD	3AD9ADA97C307C20	4E4B0A0A20202051	7492A7A35C105C71
5	7492A7A35C105C71	656100AA734D9BD6	442D383020303720	214C389A537DACF6
6	214C389A537DACF6	24192F84496F87A3	31342D4451202F2F	152D02C0184FA88C
7	152D02C0184FA88C	D1E5023A78004224	2F2F2F2031303536	FECA2D1A49307712
8	FECA2D1A49307712	C13681C85AC2BE9A	2F202051582D3132	EE16A19902EF8FA8
9	EE16A19902EF8FA8	51FABD3FD07689D6	372D58510A0A2020	66D7E56EDA7CA9F6
10	66D7E56EDA7CA9F6	E6B8C62F2EC43E95	2051542D0A0A0A20	C6E9920224CE34B5
11	C6E9920224CE34B5	0DFF16356E7BCF0B	202054524E534652	2DDF426720288959
12	2DDF426720288959	61D5E796902D5CFE	2055534420243132	4180B4D2B0096DCC
13	4180B4D2B0096DCC	CC8D850C0ECBBAA7	33343536372C3839	FFB9B03A39E7829E
14	FFB9B03A39E7829E	6CA50D0E8FBBCDFC	2046524D20414343	4CE35F43AFFA8EBF
15	4CE35F43AFFA8EBF	9A831A2CC74F4605	4E54203438303230	D4D73A18FF7F7435
16	D4D73A18FF7F7435	57154C9434F4CBA0	2D3136360A202020	7A247AA23ED4EB80
17	7A247AA23ED4EB80	EB9FA8DA67E00543	2020202020202020	CBBF88FA47C02563
18	CBBF88FA47C02563	A5584A610252F65C	20202020202F2F2F	85786A41227DD973
19	85786A41227DD973	1AA40E7F5FC0424C	2F2F202020202020	358B2E5F7FE0626C
20	358B2E5F7FE0626C	98089B143D02BBD4	544F204143434E54	CC47BB557E41F580

TIME	DES I N	DES OUT	DATA	DATA+OUT=FEEDBACK
21	CC47BB557E41F580	9A2FF5301D4D6BC1	2034303231302D31	BA1BC5022C7D46F0
22	BA1BC5022C7D46F0	1594F70B71C95CB1	37380A0A2020202D	22ACFD0151E97C9C
23	22ACFD0151E97C9C	73AB36B9EBBB05FE	54510A0A2020204B	27FA3CB3CB9B25B5
24	27FA3CB3CB9B25B5	DF1C3CEC6D147D2A	454550204F4E2051	9A596CCC225A5D7B
25	9A596CCC225A5D7B	B7B4BB5DB804DC16	5420455850454354	E394FE05E8419F42
26	E394FE05E8419F42	1B59F3C34852E3FD	205649534954204F	3B0FBA900106C3B2
27	3B0FBA900106C3B2	0CF7C6F8129EC7DA	4E20465249444159	42D780AA5BDA8683
28	42D780AA5BDA8683	F6EA0A6E5BFA9248	204F460A2020204E	D6A54C647BDAB206
29	D6A54C647BDAB206	03AF2354BC6CE835	4557204449562056	46F80310F53AC863
30	46F80310F53AC863	9D14737E3B98F5E3	50204F4E2050524F	CD343C301BC8A7AC
31	CD343C301BC8A7AC	EBD090359DB1FC5F	4A4543542051542D	A195D361BDE0A872
32	A195D361BDE0A872	DAC0D52805099102	51574552542D5451	8B97907A5124C553
33	8B97907A5124C553	2130F6C26E02F5B7	2042450A0A202020	0172B3C86422D597
34	0172B3C86422D597	E8325D59A65CD5C2	4361726566756C0A	AB532F3CC029B9C8
35	AB532F3CC029B9C8	8D0BB87D3EDD2035	0A20202052454741	872B985D6C986774
36	872B985D6C986774	970BBFB7EE9039C7	5244530A0A202020	C54FECBDE4B019E7
37	C54FECBDE4B019E7	96AA63E5AC81A3E6	51554952544F0A20	C7FF2AB7F8CEA9C6
38	C7FF2AB7F8CEA9C6	1104BFA8E79586A1	2020514B2D313335	3124EEE3CAA4B594
39	3124EEE3CAA4B594	0763CA7757778C40	3742414E4B41544F	30218B391C36D80F
40	30218B391C36D80F	156C8A2945B76A1B	42414E4B422D4B51	572DC462079A214A
41	572DC462079A214A	717552C795A78FAD	0A2020200A0A0000	7B5572E79FAD8FAD
42	7B5572E79FAD8FAD	4B7C7264DDB22A86		

MAC = 4B7C 7264

Note that the last four digits of DATA, line 41, represent binary zero "pad" characters (see ISO 8731, Part 1).

D.5 Option 3: Coded characters; extracted message elements; no editing (see 6.6)

D.5.1 Resulting authentication element

The processing of the example message would result in the following authentication element. The MAC and its delimiters are not included, and the parity bit for each character is set to zero. Only the extraction rules of 6.6.2 are applied. All characters other than message elements and their corresponding delimiters are deleted.

The explicit delimiters are used to locate and identify particular message elements. Mismatched delimiters, intervening delimiters, or an invalid message element format would result in a failure to compute the MAC.

```
QD-80 07 14-DQQX-127-XQQT-

TRNSFR USD $1234567,89 FRM ACCNT 48020-166
        /////   TO ACCNT 40210-178

-TQQT-QWERT-TQQK-1357BANKATOBANKB-KQ
```

The explicit delimiters are used to locate and identify particular message elements. Mismatched delimiters, intervening delimiters, or an invalid message element format would result in a failure to compute the MAC.

```
TO YOUR BANK

FROM OUR BANK

QD-80 07 14-DQ ///// 1056/  QX-127-XQ

QT-

TRNSFR USD $1234567,89 FRM ACCNT 48020-166
           /////    TO ACCNT 40210-178
-TQ

KEEP ON QT EXPECT VISIT ON FRIDAY OF
NEW DIV VP ON PROJECT QT-QWERT-TQ BE CAREFUL

REGARDS

QUIRTO
QK-1357BANKATOBANKB-KQ
```

D.4.2 MAC Computation

First Data Block: 0A202020544F2059 (ISO 646 representation of linefeed,space,space,space,T,O,space,Y).

TIME	DES IN	DES OUT	DATA	DATA+OUT=FEEDBACK
1	0A202020544F2059	1CAB5BC75CD5D7D4	4F55522042414E4B	53FE09E71E94999F
2	53FE09E71E94999F	E2C5ED33A60E8594	0A0A20202046524F	E8CFCD138648D7DB
3	E8CFCD138648D7DB	CDCA93439001329C	4D204F5552204241	80EADC16C22170DD
4	80EADC16C22170DD	3AD9ADA97C307C20	4E4B0A0A20202051	7492A7A35C105C71
5	7492A7A35C105C71	656100AA734D9BD6	442D383020303720	214C389A537DACF6
6	214C389A537DACF6	24192F84496F87A3	31342D4451202F2F	152D02C0184FA88C
7	152D02C0184FA88C	D1E5023A78004224	2F2F2F2031303536	FECA2D1A49307712
8	FECA2D1A49307712	C13681C85AC2BE9A	2F202051582D3132	EE16A19902EF8FA8
9	EE16A19902EF8FA8	51FABD3FD07689D6	372D58510A0A2020	66D7E56EDA7CA9F6
10	66D7E56EDA7CA9F6	E6B8C62F2EC43E95	2051542D0A0A0A20	C6E9920224CE34B5
11	C6E9920224CE34B5	0DFF16356E7BCF0B	202054524E534652	2DDF426720288959
12	2DDF426720288959	61D5E796902D5CFE	2055534420243132	4180B4D2B0096DCC
13	4180B4D2B0096DCC	CC8D850C0ECBBAA7	33343536372C3839	FFB9B03A39E7829E
14	FFB9B03A39E7829E	6CA50D0E8FBBCDFC	2046524D20414343	4CE35F43AFFA8EBF
15	4CE35F43AFFA8EBF	9A831A2CC74F4605	4E54203438303230	D4D73A18FF7F7435
16	D4D73A18FF7F7435	57154C9434F4CBA0	2D3136360A202020	7A247AA23ED4EB80
17	7A247AA23ED4EB80	EB9FA8DA67E00543	2020202020202020	CBBF88FA47C02563
18	CBBF88FA47C02563	A5584A610252F65C	202020202F2F2F	85786A41227DD973
19	85786A41227DD973	1AA40E7F5FC0424C	2F2F202020202020	358B2E5F7FE0626C
20	358B2E5F7FE0626C	98089B143D02BBD4	544F204143434E54	CC47BB557E41F580

D.5.2 MAC computation

First Data Block: 51442D3830203037 (ISO 646 representation of Q,D,-,8,0,space,0,7).

TIME	DES IN	DES OUT	DATA	DATA+OUT = FEEDBACK
1	51442D3830203037	0EC117F76ECCE2B9	2031342D44515158	2EF023DA2A9DB3E1
2	2EF023DA2A9DB3E1	D6531B3A58CAEF2F	2D3132372D585151	FB62290D7592BE7E
3	FB62290D7592BE7E	8926CE3C31026A4D	542D0A0A0A202020	DD0BC4363B224A6D
4	DD0BC4363B224A6D	3961E3E5113F6CD4	54524E5346522055	6D33ADB6576D4C81
5	6D33ADB6576D4C81	E34C49C658B5A5B3	5344202431323334	B00869E269879687
6	B00869E269879687	50BC1AD3B25A6F3C	3536372C38392046	658A2DFF8A634F7A
7	658A2DFF8A634F7A	B2E87E1A107E4CFC	524D204143434E54	E0A55E5B533D02A8
8	E0A55E5B533D02A8	71A060DA8E1E43CC	2034383032302D31	519458EABC2E6EFD
9	519458EABC2E6EFD	A48D3F27941BAF93	36360A2020202020	92BB3507B43B8FB3
10	92BB3507B43B8FB3	4DB726E7EB2781A3	2020202020202020	6D9706C7CB07A183
11	6D9706C7CB07A183	AC657F09B68B9007	2020202F2F2F2F2F	8C455F2699A4BF28
12	8C455F2699A4BF28	FA530E3092423F58	202020202020544F	DA732E10B2626B17
13	DA732E10B2626B17	74854F134964AA63	204143434E542034	54C40C5007308A57
14	54C40C5007308A57	F29B647B7BCA9084	303231302D313738	C2A9554B56FBA7BC
15	C2A9554B56FBA7BC	7AB659B4C55764C3	0A0A2020202D5451	70BC7994E57A3092
16	70BC7994E57A3092	2FA8C903E7C21E6C	51542D5157455254	7EFCE452B0874C38
17	7EFCE452B0874C38	D5357FE17DDD2EDD	2D5451514B2D3133	F8612EB036F01FEE
18	F8612EB036F01FEE	4327709A75D45C7D	353742414E4B4154	761032DB3B9F1D29
19	761032DB3B9F1D29	DB7EE3766594E6C5	4F42414E4B422D4B	943CA2382ED6CB8E
20	943CA2382ED6CB8E	5CBE516997D8343A	5100000000000000	0DBE516997D8343A
21	0DBE516997D8343A	56C3B8DCFFCF09DC		

MAC = 56C3 B8DC

Note that the last fourteen digits of DATA, line 20, represent binary zero "pad" characters.

D.6 Option 4: Coded characters; entire message; editing (see 6.7)

D.6.1 Resulting authentication element

The processing of the message would result in the following authentication element. The MAC and its delimiters are not included, and the parity bit for each character is set to zero. Only the editing rules of 6.7.2 are applied. Each carriage return and each line feed is replaced by a single space, lower case alphabetics are translated to upper case, any characters other than the upper case letters, digits, space, comma, full stop, hyphen, solidus, asterisk, and open and close parentheses are deleted, leading spaces of the message are deleted, and each sequence of consecutive spaces is replaced by a single space.

The explicit delimiters are used to locate and identify particular message elements. Mismatched delimiters, intervening delimiters, or an invalid message element format would result in a failure to compute the MAC.

```
TO YOUR BANK FROM OUR BANK QD-80 07 14-DQ ///// 1056/ QX-1
27-XQ QT- TRNSFR USD 1234567,89 FRM ACCNT 48020-166 /////
TO ACCNT 40210-178 -TQ KEEP ON QT EXPECT VISIT ON FRIDAY O
F NEW DIV VP ON PROJECT QT-QWERT-TQ BE CAREFUL REGARDS QUI
RTO QK-1357BANKATOBANKB-KQ
```

D.6.2 MAC computation

First Data Block: 544F20594F555220 (ISO 646 representation of T,O,space,Y,O,U,R,space).

TIME	DES IN	DES OUT	DATA	DATA+OUT = FEEDBACK
1	544F20594F555220	B6391DE0AC3D11B6	42414E4B2046524F	F47853AB8C7B43F9
2	F47853AB8C7B43F9	73E2EDF58F1BCC21	4D204F5552204241	3EC2A2A0DD3B8E60
3	3EC2A2A0DD3B8E60	D8A81E3F4B6C6A97	4E4B2051442D3830	96E33E6E0F4152A7
4	96E33E6E0F4152A7	B6AADF11B3A74067	2030372031342D44	969AE83182936D23
5	969AE83182936D23	A856C5896EA8467E	51202F2F2F2F2F20	F976EAA64187695E
6	F976EAA64187695E	F37AD3830B2CA19F	313035362F205158	C24AE6B5240CF0C7
7	C24AE6B5240CF0C7	A3A8BFF8CB90E692	2D3132372D585120	8E998DCFE6C8B7B2
8	8E998DCFE6C8B7B2	B46F0318F100893D	51542D2054524E53	E53B2E38A552C76E
9	E53B2E38A552C76E	E408D7F3BBD9A468	4652205553442031	A25AF7A6E89D8459
10	A25AF7A6E89D8459	FD39B6A3CD702922	3233343536372C38	CF0A8296FB47051A
11	CF0A8296FB47051A	C47824BD5BC1BA0F	392046524D204143	FD5862EF16E1FB4C
12	FD5862EF16E1FB4C	B6279783724FE2A7	434E542034383032	F569C3A34677D295
13	F569C3A34677D295	BF824A0CD2539444	302D313636202F2F	8FAF7B3AE473BB6B
14	8FAF7B3AE473BB6B	37F3E9514E4BA191	2F2F2F20544F2041	18DCC6711A0481D0
15	18DCC6711A0481D0	32CBF3B631D9BD02	43434E5420343032	7188BDE211ED8D30
16	7188BDE211ED8D30	F678CEB605675216	31302D313738202D	C748E387325F723B
17	C748E387325F723B	937BEBF7F0B9C7B4	5451204B45455020	C72ACBBCB5FC9794
18	C72ACBBCB5FC9794	260D3D329F7BAA64	4F4E205154204558	69431D63CB5BEF3C
19	69431D63CB5BEF3C	B4A50AC5BBC67D6E	5045435420564953	E4E049919B90343D
20	E4E049919B90343D	36DE8418A69CE22A	4954204F4E204652	7F8AA457E8BCA478
21	7F8AA457E8BCA478	0E21FDF8BCB3E2DC	49444159204F4620	4765BCA19CFCA4FC
22	4765BCA19CFCA4FC	E97345AC8034E556	4E45572044495620	A736128CC47DB376
23	A736128CC47DB376	584058D3878152D7	5650204F4E205052	0E10789CC9A10285
24	0E10789CC9A10285	FAB603A0040A229C	4F4A454354205154	B5FC46E3502A73C8
25	B5FC46E3502A73C8	CB419F935F0D9B7D	2D51574552542D54	E610C8D60D59B629
26	E610C8D60D59B629	A8628086EFDB9000	5120424520434152	F942C2C3CF98D152
27	F942C2C3CF98D152	F5DAC4502C948287	4546554C20524547	B09C911C0CC6C7C0
28	B09C911C0CC6C7C0	66E0BDF9441DFE30	4152445320515549	27B2F9AA644CAB79
29	27B2F9AA644CAB79	BF3F763FC455FDCD	52544F20514B2D31	ED6B391F951ED0FC
30	ED6B391F951ED0FC	A63E14DE1F9B23C2	33353742414E4B41	950B239C5ED56883
31	950B239C5ED56883	BE9D592B1FF558E2	544F42414E4B422D	EAD21B6A51BE1ACF
32	EAD21B6A51BE1ACF	3A9C28638D37EFE7	4B51200000000000	71CD08638D37EFE7
33	71CD08638D37EFE7	BDFFB4BCC189D2D5		

MAC = BDFF B4BC

Note that the last ten digits of DATA, line 32, represent binary zero "pad" characters.

D.7 Option 5: Coded characters; extracted message elements; editing (see 6.8)

D.7.1 Resulting authentication element

The processing of the message would result in the following authentication element. The MAC and its delimiters are not included, and the parity bit for each character is set to zero. The extraction rules of 6.6.2 and the editing rules of 6.7.2 are applied. All characters other than message elements and their corresponding delimiters are deleted. Each carriage return and each line feed is replaced by a single space, lower case alphabetics are translated to upper case, any characters other than the upper case letters, digits, space, comma, full stop, hyphen, solidus, asterisk, and open and close parentheses are deleted, leading spaces of the message elements are deleted, and each sequence of consecutive spaces is replaced by a single space.

The explicit delimiters are used to locate and identify particular message elements. Mismatched delimiters, intervening delimiters, or an invalid message element format would result in a failure to compute the MAC.

```
QD-80 07 14-DQQX-127-XQQT-TRNSFR USD 1234567,89 FRM ACCNT
48020-166 ///// TO ACCNT 40210-178 -TQQT-QWERT-TQQK-1357BA
NKATOBANKB-KQ
```

D.7.2 MAC computation

First Data Block: 51442D3830203037 (ISO 646 representation of Q,D,-,8,0,space,0,7).

TIME	DES IN	DES OUT	DATA	DATA+OUT=FEEDBACK
1	51442D3830203037	0EC117F76ECCE2B9	2031342D44515158	2EF023DA2A9DB3E1
2	2EF023DA2A9DB3E1	D6531B3A58CAEF2F	2D3132372D585151	FB62290D7592BE7E
3	FB62290D7592BE7E	8926CE3C31026A4D	542D54524E534652	DD0B9A6E7F512C1F
4	DD0B9A6E7F512C1F	0725C3BE7D2D6C9B	2055534420313233	277090FA5D1C5EA8
5	277090FA5D1C5EA8	986FB578F853DABD	343536372C383920	AC5A834FD46BE39D
6	AC5A834FD46BE39D	91FC3D80505A6B62	46524D204143434E	D7AE70A01119282C
7	D7AE70A01119282C	4B89E2109D7DFC42	542034383032302D	1FA9D628AD4FCC6F
8	1FA9D628AD4FCC6F	5A8DE28524DAA77A	313636202F2F2F2F	6BBBD4A50BF58855
9	6BBBD4A50BF58855	E6136AD53FA28BA1	2F20544F20414343	C9333E9A1FE3C8E2
10	C9333E9A1FE3C8E2	0A085E34EE67BD74	4E54203430323130	445C7E00DE558C44
11	445C7E00DE558C44	4376D8D6FF65F864	2D313738202D5451	6E47EFEEDF48AC35
12	6E47EFEEDF48AC35	AF95B4E1C19F4A72	51542D5157455254	FEC199B096DA1826
13	FEC199B096DA1826	FFD81B5AB127C06E	2D5451514B2D3133	D28C4A0BFA0AF15D
14	D28C4A0BFA0AF15D	1B119F10BBE0104E	353742414E4B4154	2E26DD51F5AB511A
15	2E26DD51F5AB511A	6A43C2D831FA7026	4F42414E4B422D4B	250183967AB85D6D
16	250183967AB85D6D	1259B0715E1CABDA	5100000000000000	4359B0715E1CABDA
17	4359B0715E1CABDA	A5F227FC2B161D9C		

MAC = A5F2 27FC

Note that the last fourteen digits of DATA, line 16, represent binary zero "pad" characters.

Annex E
(informative)

Example of message authentication for coded character sets: MAA

E.1 Purpose

This annex presents examples of the entire authentication process, using similar data to that contained in annex D, but using the algorithm of ISO 8731, Part 2, Message Authenticator Algorithm.

E.2 .. Text of example

The text of the unedited message is

```
TO YOUR BANK

FROM OUR BANK

QD-80 07 14-DQ ///// 1056/  QX-127-XQ

QT-

TRNSFR USD $1234567,89 FRM ACCNT 48020-166
          /////    TO ACCNT 40210-178

-TQ

KEEP ON QT EXPECT VISIT ON FRIDAY OF
NEW DIV VP ON PROJECT QT-QWERT-TQ BE CAREFUL

REGARDS

QUIRTO
QK-1357BANKATOBANKB-KQ
```

E.3 ..MAC computation using entire message no editing

E.3.1 Example cryptographic key interpreted as

J = E6 A1 2F 07   K = 9D 15 C4 37

E.3.2 Text for input to algorithm.

This text is treated as 86 numbers of 4 hex (32 bits) each. Each number has the left most character in the most significant end, e.g., the word BANK will read as 42 41 4E 4B in hex and 42 is the most significant byte in the word.

```
0A  20  20  20  54  4F  20  59
4F  55  52  20  42  41  4E  4B
0A  0A  20  20  20  46  52  4F
4D  20  4F  55  52  20  42  41
4E  4B  0A  0A  20  20  20  51
44  2D  38  30  20  30  37  20
31  34  2D  44  51  20  2F  2F
2F  2F  2F  20  31  30  35  36
2F  20  20  51  58  2D  31  32
37  2D  58  51  0A  0A  20  20
20  51  54  2D  0A  0A  0A  20
20  20  54  52  4E  53  46  52
20  55  53  44  20  24  31  32
33  34  35  36  37  2C  38  39
20  46  52  4D  20  41  43  43
4E  54  20  34  38  30  32  30
2D  31  36  36  0A  20  20  20
20  20  20  20  20  20  20  20
20  20  20  20  20  2F  2F  2F
2F  2F  20  20  20  20  20  20
54  4F  20  41  43  43  4E  54
20  34  30  32  31  30  2D  31
37  38  0A  0A  20  20  20  2D
54  51  0A  0A  20  20  20  4B
45  45  50  20  4F  4E  20  51
54  20  45  58  50  45  43  54
20  56  49  53  49  54  20  4F
4E  20  46  52  49  44  41  59
20  4F  46  0A  20  20  20  4E
45  57  20  44  49  56  20  56
50  20  4F  4E  20  50  52  4F
4A  45  43  54  20  51  54  2D
51  57  45  52  54  2D  54  51
20  42  45  0A  0A  20  20  20
43  61  72  65  66  75  6C  0A
0A  20  20  20  52  45  47  41
52  44  53  0A  0A  20  20  20
51  55  49  52  54  4F  0A  20
20  20  51  4B  2D  31  33  35
37  42  41  4E  4B  41  54  4F
42  41  4E  4B  42  2D  4B  51
0A  20  20  20  0A  0A  00  00
```

E.3.3 Steps of the algorithm for the first message block 0A 20 20 20.

This details the steps of the algorithm for the first message block 0A 20 20 20. After the key is given the output of the Prelude, then the message block, then the results of each intermediate step of the main loop. The successive F,G values result from the operations ADD, OR, AND respectively. The last X,Y values are the results from the first message block.

```
J = E6 A1 2F  07     K =  9D 15 C4 37           Key

X = 21  D8 69  BA    Y =  77  92  F9 D4   )     Result of Prelude
V = C4 EB 1A  EB     W =  F6  A0  96 67   )     see 4.2.1 (ISO 8731-2)
S = 6D 67  E8  84    T =  A5  11  98 7A   )

M = 0A 20 20 20                                 First message block

V = 89 D6 35  D7     E =  7F  76  A3 B0         (21)          ) Main loop with
X = 2B F8 49  9A     Y =  7D  B2  D9 F4         (22)          ) reference to
F = FD 29 7D  A4     G =  AB  6E  ED 4A         ADD)          ) lines of text
F = FF 2D 7D  A5     G =  AB  EE  ED 6B         OR) (27)      ) in ISO 8731-2,
F = BF 2D 7D  85     G =  29  EE  E9 6B         AND)          ) 4.2.2.
X = 0A D6 7E  20     Y =  30  26  14 92         (24)          )
```

E.3.4 X and Y values for an 86 block message.

The X,Y values for an 86 block message corresponding to D.4.2 with the example key are given. For each block of the message, the resultant X and Y and the message block number (1-86) are shown. Finally, the S and T steps are shown and the final Z value.

```
M =  0A 20  20  20      X =  0A  D6 7E  20      Y =  30 26  14 92    N  =1
M =  54 4F  20  59      X =  EC  E5 07  4A      Y =  30 24  B3 7F    N  =2
M =  4F 55  52  20      X =  60  5E F7  B2      Y =  56 E0  9C AF    N  =3
M =  42 41  4E  4B      X =  11  25 12  0E      Y =  23 46  22 DC    N  =4
M =  0A 0A  20  20      X =  62  00 C5  82      Y =  48 15  25 92    N  =5
M =  20 46  52  4F      X =  80  AB 2C  AA      Y =  E0 FD  BA A9    N  =6
M =  4D 20  4F  55      X =  DA  F1 22  72      Y =  22 35  84 1E    N  =7
M =  52 20  42  41      X =  33  E5 22  43      Y =  05 5E  A2 CB    N  =8
M =  4E 4B  0A  0A      X =  0B  06 9C  3B      Y =  28 A7  F3 83    N  =9
M =  20 20  20  51      X =  B4  A7 E9  23      Y =  0C FA  0D 42    N  =10
M =  44 2D  38  30      X =  DC  D3 50  A7      Y =  43 A9  DC A2    N  =11
M =  20 30  37  20      X =  EF  80 8A  05      Y =  85 E0  84 3E    N  =12
M =  31 34  2D  44      X =  D1  4F 04  01      Y =  E3 BA  7D 70    N  =13
M =  51 20  2F  2F      X =  9B  DB 76  A8      Y =  BA D7  BC 43    N  =14
M =  2F 2F  2F  20      X =  97  D0 7C  43      Y =  A6 CC  DC 57    N  =15
M =  31 30  35  36      X =  B6  CF E1  B5      Y =  7C E8  61 07    N  =16
M =  2F 20  20  51      X =  AE  E1 DD  D3      Y =  6C BD  66 D8    N  =17
M =  58 2D  31  32      X =  2A  44 7E  AB      Y =  EB 1F  4F FC    N  =18
M =  37 2D  58  51      X =  3D  2A BC  46      Y =  34 0C  3A C7    N  =19
M =  0A 0A  20  20      X =  95  9E 51  A7      Y =  FC A0  4E 9B    N  =20
M =  20 51  54  2D      X =  AE  66 EC  B5      Y =  51 BB  EC 9C    N  =21
M =  0A 0A  0A  20      X =  E5  29 5C  CD      Y =  24 B1  E3 AA    N  =22
M =  20 20  54  52      X =  E5  05 09  F1      Y =  FF 34  68 76    N  =23
M =  4E 53  46  52      X =  04  40 0A  38      Y =  EC 7C  21 48    N  =24
M =  20 55  53  44      X =  8E  CE CB  40      Y =  0C 84  65 D0    N  =25
M =  20 24  31  32      X =  C7  10 4A  8F      Y =  BF 2A  3E 8C    N  =26
M =  33 34  35  36      X =  E7  F2 D9  C6      Y =  80 11  BF AE    N  =27
M =  37 2C  38  39      X =  71  AE 6F  FC      Y =  42 EC  EF C9    N  =28
M =  20 46  52  4D      X =  A7  A3 7A  AE      Y =  49 39  1C 52    N  =29
M =  20 41  43  43      X =  16  32 B3  DB      Y =  49 C5  34 71    N  =30
M =  4E 54  20  34      X =  DD  BE 75  C6      Y =  48 ED  8B DF    N  =31
M =  38 30  32  30      X =  CE  10 C0  89      Y =  94 2B  21 CF    N  =32
M =  2D 31  36  36      X =  15  72 15  74      Y =  A2 43  0B CF    N  =33
M =  0A 20  20  20      X =  76  63 15  89      Y =  88 07  91 EB    N  =34
M =  20 20  20  20      X =  7C  8F B0  D9      Y =  E3 5E  65 2B    N  =35
M =  20 20  20  20      X =  39  EA B0  94      Y =  FF FF  E3 29    N  =36
M =  20 20  20  20      X =  1E  A1 77  1A      Y =  71 70  0F 37    N  =37
M =  20 2F  2F  2F      X =  87  3F 74  88      Y =  66 F6  00 02    N  =38
M =  2F 2F  20  20      X =  DA  BD 9B  E5      Y =  25 8C  05 E6    N  =39
M =  20 20  20  20      X =  D7  AA 38  11      Y =  21 9F  F3 2C    N  =40
M =  54 4F  20  41      X =  B3  8D 8D  16      Y =  57 33  84 37    N  =41
M =  43 43  4E  54      X =  F9  C1 36  F3      Y =  52 39  55 D9    N  =42
M =  20 34  30  32      X =  A6  66 E6  B0      Y =  A8 23  50 5B    N  =43
M =  31 30  2D  31      X =  41  B3 72  86      Y =  D2 95  5D AC    N  =44
M =  37 38  0A  0A      X =  02  59 B9  06      Y =  4B A6  5A 7E    N  =45
M =  20 20  20  2D      X =  A4  34 28  35      Y =  86 08  17 0D    N  =46
M =  54 51  0A  0A      X =  00  DB 50  C4      Y =  BO E9  C1 E7    N  =47
M =  20 20  20  4B      X =  92  D9 0F  51      Y =  7C 0A  5C AE    N  =48
M =  45 45  50  20      X =  4C  69 F1  A0      Y =  E3 45  F7 28    N  =49
M =  4F 4E  20  51      X =  F9  42 09  75      Y =  57 98  56 97    N  =50
M =  54 20  45  58      X =  14  B4 9B  2C      Y =  3B 08  0B 6F    N  =51
M =  50 45  43  54      X =  DE  B0 04  B7      Y =  20 03  33 13    N  =52
M =  20 56  49  53      X =  BC  88 F7  17      Y =  6B 6D  79 90    N  =53
M =  49 54  20  4F      X =  3E  EE 66  54      Y =  E0 1A  AE 31    N  =54
M =  4E 20  46  52      X =  0A  B8 A3  92      Y =  A2 A0  6F 8D    N  =55
```

```
M = 49 44 41 59     X = 0A 42 BE D2     Y = 54 07 21 70     N =56
M = 20 4F 46 0A     X = EB F6 CA 1C     Y = 5E C5 1B 88     N =57
M = 20 20 20 4E     X = E6 74 52 43     Y = E6 16 59 4E     N =58
M = 45 57 20 44     X = 5A C6 8F 40     Y = AA A8 82 AC     N =59
M = 49 56 20 56     X = 19 AF C8 50     Y = 2E 06 55 4A     N =60
M = 50 20 4F 4E     X = C1 26 B8 6E     Y = DF F2 FC 9E     N =61
M = 20 50 52 4F     X = 1A 90 98 9E     Y = 0B BF BC 41     N =62
M = 4A 45 43 54     X = 98 03 D3 5D     Y = 5B 8A 1D A3     N =63
M = 20 51 54 2D     X = 76 73 20 E0     Y = FB 70 1B 0C     N =64
M = 51 57 45 52     X = 0C 7F BE 3D     Y = 34 56 77 D0     N =65
M = 54 2D 54 51     X = A0 DA C4 CB     Y = 47 2B F5 39     N =66
M = 20 42 45 0A     X = 8D 2E 5F 0E     Y = C9 ED 6A 8D     N =67
M = 0A 20 20 20     X = F6 CA 14 AD     Y = EA 41 90 4F     N =68
M = 43 61 72 65     X = B9 50 1E A7     Y = FA 62 27 D8     N =69
M = 66 75 6C 0A     X = 8A 13 5B F0     Y = FE BB C3 24     N =70
M = 0A 20 20 20     X = 3C C8 82 78     Y = E0 07 24 2C     N =71
M = 52 45 47 41     X = 63 01 C3 05     Y = 24 33 7B 11     N =72
M = 52 44 53 0A     X = 3F DE B2 2B     Y = 59 40 9A 59     N =73
M = 0A 20 20 20     X = FB C8 46 EB     Y = 5A 51 58 07     N =74
M = 51 55 49 52     X = 59 03 67 F7     Y = AB 17 8D AB     N =75
M = 54 4F 0A 20     X = 8F EF E7 27     Y = 4E 6B 6B CD     N =76
M = 20 20 51 4B     X = 46 B2 14 AD     Y = 7B A1 69 94     N =77
M = 2D 31 33 35     X = BF 69 AE 4C     Y = C4 18 00 F7     N =78
M = 37 42 41 4E     X = CB 41 32 66     Y = 12 29 0F 39     N =79
M = 4B 41 54 4F     X = 59 EF 2A 8A     Y = 8E 7C CE 02     N =80
M = 42 41 4E 4B     X = 36 8F B9 8D     Y = 29 06 F1 E1     N =81
M = 42 2D 4B 51     X = 7D 42 1C 92     Y = F6 3A 85 6E     N =82
M = 0A 20 20 20     X = D2 72 89 3B     Y = 0A C1 CC 1C     N =83
M = 0A 0A 00 00     X = BA 17 32 96     Y = 6B A2 22 26     N =84

S = 6D 67 E8 84     X = D1 E8 F8 FC     Y = 3C 3F 17 5A
T = A5 11 98 7A     X = 24 E3 C0 E1     Y = FA E3 A7 92

Z = DE 00 67 73
```

E.4 Example of 516 block message made by repeating the 86 block message six times.

This must be partitioned into sets of 256 blocks (1 024 bytes each) and forms 2 full sets and one of 4 blocks (516 = 256 + 256 + 4). The results are shown below, where the start and finish of the first two sets is shown, the rest, having been calculated, is simply shown as dashes "-- -- -- --". The third set is shown in full and the final Z value.

```
M = 0A 20 20 20     X = 0A D6 7E 20     Y = 30 26 14 92     N =1
M = 54 4F 20 59     X = EC E5 07 4A     Y = 30 24 B3 7F     N =2
    -- -- -- --         -- -- -- --         -- -- -- --
    -- -- -- --         -- -- -- --         -- -- -- --
M = 4F 55 52 20     X = F3 B6 AD 89     Y = 56 05 11 C9     N =255
M = 42 41 4E 4B     X = CB 89 B4 4B     Y = EB E6 7D 68     N =256

S = 6D 67 E8 84     X = AF D7 8F CB     Y = FC B8 AC D6
T = A5 11 98 7A     X = B2 8C F0 69     Y = A8 A9 BA D2

Z = 1A 25 4A BB
```

```
Z = 1A 25 4A BB      X = 55 DF 84 D3      Y = 99 97 11 D7
M = 0A 0A 20 20      X = 00 1B AC 56      Y = A1 6E B6 FD      N =257
M = 20 46 52 4F      X = C7 3B 90 0E      Y = 29 E8 77 02      N =258
    -- -- -- --          -- -- -- --          -- -- -- --
    -- -- -- --          -- -- -- --          -- -- -- --
M = 4D 20 4F 55      X = 68 11 F8 C9      Y = 46 E2 CB CD      N =511
M = 52 20 42 41      X = F1 77 71 B2      Y = 7C E5 C7 62      N =512

S = 6D 67 E8 84      X = 80 A9 29 22      Y = 52 58 DA 00
T = A5 11 98 7A      X = 41 EA 12 4F      Y = 93 BD 1A B6

Z = D2 57 08 F9

Z = D2 57 08 F9      X = 03 33 1A C3      Y = 84 C3 CB F7
M = 4E 4B 0A 0A      X = 7E 10 C7 D3      Y = 53 D9 DD E3      N =513
M = 20 20 20 51      X = 18 8D 1D 75      Y = 4F 92 F7 2A      N =514
    -- -- -- --          -- -- -- --          -- -- -- --
    -- -- -- --          -- -- -- --          -- -- -- --
M = 0A 20 20 20      X = 10 EF 37 A1      Y = B6 1B 50 82      N =587
M = 0A 0A 00 00      X = C4 4A 8C 7C      Y = BC 0E B0 C8      N =588

S = 6D 67 E8 84      X = DE 40 F9 D3      Y = 4B C9 31 0A
T = A5 11 98 7A      X = 82 22 58 08      Y = 44 C1 88 08

Z = C6 E3 D0 00
```

Annex F
(informative)

Framework for message authentication of standard telex formats

F.1 Purpose

This annex presents a framework for structuring the additional data required for authenticating telex messages in accordance with the formats defined in this International Standard.

The example used is example 1 of ISO 7746 (1988): *Telex formats for inter-bank messages.*

Sender and receiver must agree upon the format option for authentication to be selected, to enable the message to be authenticated.

Message authentication can be applied in lieu of test key calculation to any of the formats contained in ISO 7746 which require or provide for a test key. When message authentication in accordance with this International Standard is selected for securing a message structured in accordance with this standard, the test key field and related content are not mandatory.

F.2 Message authentication data elements

F.2.1 IDA:

The identifier for authentication key is an optional data element. This field, when present, should be placed following the start of *text indicator YZYZ, preceded and followed by one blank line.*

Format: Up to 16 characters

F.2.2 DATE MAC COMPUTED:

The date MAC computed (DMC) is equivalent to the instruction date as specified in the DATE: field of all standard telex format messages. This data element is required.

Format: 6 digits - YYMMDD (ISO 8601)

F.2.3 20 SENDERS REF:

The message identifier (MID) is equivalent to the sending bank's transaction reference as specified in field :20 SENDERS REF: of all standard telex format messages. This data element is required.

Format: Up to 16 characters

F.2.4 MAC:

The message authentication code is a required data element. This field should be placed following the last line of the last field specified in the message, preceded and followed by one blank line.

Format: 8 hexadecimal characters (0-9, A-F), expressed as two groups of four separated by a space (hhhhbhhhh).

F.3 Example Message Incorporating Message Authentication Framework Customer Transfer: Standard Format (example 1B, from ISO 7746)

```
45678 LONCOM G
54321 BANFIC CH
YZYZ


:IDA:6666            (IDENTIFIER FOR AUTHENTICATION KEY)


FROM:BANQUE FICTITIOUS,
   GENEVA
TO  :LONDON COMMERCIAL BANK,
   BIRMINGHAM
DATE:801201          (DATE MAC  COMPUTED)

::100 CUSTOMER TRANSFER

PLEASE PAY

:15 TEST KEY:
:20 SENDERS REF:A4760       (MESSAGE IDENTIFIER)
:30 VALUE DATE:801201
:32 AMOUNT:CHF1.000,00
:50 ORIGINATOR:FRANZ HOLZAPFEL
:52 ORIGINATORS BANK:BANQUE DE ZUG, BAHNHOFSTRASSE,
ZUG
:53 REIMBURSEMENT:WE HAVE INSTRUCTED BANQUE ANON SA,
CHIASSO TO PAY BANQUE FORTUITOUS
SA, ZUG FOR YOUR LONDON'S ACCOUNT
UNDER TELEGRAPHIC ADVICE TO YOU
:57 PAY THRU:NIDWAY BANK LTD, GREEN STREET,
WARGRAVE
:59 BENEFICIARY:/122689-443
H.F. JANSSEN, WALLFLOWER HOTEL,
WARGRAVE
:70 BENEF INFO:SALARY SETTLEMENT
:72 RECEIVER INFO:PHONE PAY THRU BANK
:82 PAY THRU INFO:PHONE BEN ON WARGAVE 4725336

:MAC:1773 1044          (MESSAGE AUTHENTICATION CODE)

45678 LONCOM G
54321 BANFIC CH

NNNN
```