SLS 1054 : 1995
(ISO 8731 - 2 : 1992)

Sri Lanka Standard

BANKING - APPROVED ALGORITHMS FOR MESSAGE AUTHENTICATION - PART - 2 : MESSAGE AUTHENTICATOR ALGORITHM

Gr. K

SRI LANKA STANDARDS INSTITUTION

SLS 1054 : 1995
ISO 8731-2 : 1992

Sri Lanka Standard
BANKING - APPROVED ALGORITHMS FOR MESSAGE AUTHENTICATION
PART 2 : MESSAGE AUTHENTICATOR ALGORITHM

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 8731-2 : 1992 Banking -Approved algorithms for message authentication - Part 2 : Message authenticator algorithm, published by the Internatioanl 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. Howevers, 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 Standard	Corresponding Sri Lanka Standards
ISO 8730:1990, Banking - Requirements for message authentication (wholesale).	SLS 1053 : 1995, Banking Requirements for message authentication (wholesale).

-/ltf.

INTERNATIONAL STANDARD

ISO 8731-2

Second edition
1992-09-15

Banking — Approved algorithms for message authentication —

Part 2:
Message authenticator algorithm

Banque — Algorithmes approuvés pour l'authentification des messages —

Partie 2: Algorithme d'authentification des messages

Reference number
ISO 8731-2:1992(E)

Contents **Page**

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 voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

International Standard ISO 8731-2 was prepared by Technical Committee ISO/TC 68, *Banking and related financial services*, Sub-Committee SC 2, *Operations and procedures*.

This second edition cancels and replaces the first edition (ISO 8731-2:1987), of which it constitutes a technical revision.

ISO 8731 consists of the following parts, under the general title *Banking — Approved algorithms for message authentication*:

— *Part 1: DEA*

— *Part 2: Message authenticator algorithm*

Annexes A and B of this part of ISO 8731 are for information only.

Banking -- Approved algorithms for message authentication --

Part 2 :
Message authenticator algorithm

1 Scope

ISO 8731 specifies, in individual parts, approved authentication algorithms i.e. approved as meeting the authentication requirements specified in ISO 8730. This part of ISO 8731 deals with the Message Authenticator Algorithm for use in the calculation of the Message Authentication Code (MAC).

The Message Authenticator Algorithm (MAA) is specifically designed for high-speed authentication using a mainframe computer. This is a special purpose algorithm to be used where data volumes are high, and efficient implementation by software a desirable characteristic. MAA is also suitable for use with a programmable calculator.

Test examples are given in annex A, which does not form part of this part of ISO 8731. A further test example is given as an Annex in ISO 8730.

A specification of MAA in VDM is given in Annex B, which does not form part of this part of ISO 8731.

2 Normative references

The following standards contain provisions which, through references in this text, constitute provisions of this part of ISO 8731. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this part of ISO 8731 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 7185 : 1990, *Information technology - Programming languages - PASCAL.*

ISO 8730 : 1990, *Banking - Requirements for message authentication (wholesale).*

3 Brief description

3.1 General

The Message Authenticator Algorithm works on the principle of a Message Authentication Code (or MAC), a number sent with a message, so that a check can be made by the receiver of the message that it has not been altered since it left the sender.

3.2 Technical

All numbers manipulated in this algorithm shall be regarded as 32-bit unsigned integers, unless otherwise stated. For such a number N, $0 < N < 2^{32}$. This algorithm can be implemented conveniently and efficiently in a computer with a word length of 32 bits or more.

Messages to be authenticated may originate as a bit string of any length. They shall be input to the algorithm as a sequence of 32 bit numbers, M_1, M_2 -- M_n, of which there are n, called message blocks. The detail of how to pad out the last block M_n to 32 bits is not part of the algorithm but shall be defined in any application. This algorithm shall not be used to authenticate messages with more than 1 000 000 blocks, i.e. $n < 1\ 000\ 000$.

The key shall comprise two 32 bit numbers J and K and thus has a size of 64 bits.

The result of the algorithm is a 32 bit authentication value. The calculation can be performed on messages as short as one block ($n = 1$).

Messages longer than 256 message blocks shall be divided into segments of 256 blocks, except that the last segment may have less than 256 message blocks.

Clause 4 specifies the segment algorithm. If the whole message is within one segment this completes the calculation and its output (Z) is the value of the authenticator. If there are more than 256 message blocks, the mode of operation specified in clause 5 shall be used.

The segment algorithm has three parts.

a) The prelude shall be a calculation made with the key parts (J and K) alone and it shall generate six numbers X_0, Y_0, V_0, W, S and T which shall be used in the subsequent calculations. This part need not be repeated until a new key is installed.

b) The main loop is a calculation which shall be repeated for each message block M, and therefore, for long messages, dominates the calculation.

c) The coda shall consist of two operations of the main loop, using as its message blocks the two numbers S and T in turn, followed by a simple calculation of Z.

The mode of operation (see clause 5) is an essential feature of the implementation of this algorithm.

Figure 1 shows the data flow in schematic form.

4 The segment algorithm

4.1 Definition of the functions used in the algorithm

4.1.1 General definitions

A number of functions are used in the description of the algorithm. In the following, X and Y are 32 bit numbers and the result is a 32 bit number except where stated otherwise.

CYC(X) is the result of a one-bit cyclic left shift of X.

AND(X,Y) is the result of the logical AND operation carried out on each of 32 bits.

OR(X,Y) is the result of the logical OR operation carried out on each of 32 bits.

XOR(X,Y) is the result of the XOR operation (modulo 2 addition) carried out on each of 32 bits.

ADD(X,Y) is the result of adding X and Y discarding any carry from the 32nd bit, that is to say, addition modulo 2^{32}.

CAR(X,Y) is the value of the carry from the 32nd bit when X is added to Y; it has the value of 0 or 1.

MUL1(X,Y), MUL2(X,Y) and MUL2A(X,Y) are three different forms of multiplication, each with a 32 bit result.

[X||Y] is the result of concatenating the binary numbers X and Y, in the left of most significant position. The notation is extended to concatenate more than two numbers and is applied also to 8 bit bytes and numbers longer than 32 bits.

4.1.2 Definition of multiplication functions

To explain the multiplications, let the 64 bit product of X and Y be [U||L]. Hence U is the upper (most significant) half of the product and L the lower (least significant) half.

4.1.2.1 To calculate MUL1(X,Y)

Multiply X and Y to produce [U||L] with S and C as local variables,

S := ADD(U,L); ... (1)

C := CAR(U,L); ... (2)

MUL1(X,Y) : = ADD(S,C). ... (3)

That is to say, U shall be added to L with end around carry.

Numerically the result is congruent to X*Y, the product of X and Y, modulo (2^{32} - 1). It is not necessarily the smallest residue because it may equal 2^{32} - 1.

4.1.2.2 To calculate MUL2(X,Y)

This form of multiplication shall not be used in the main loop, only in the prelude. With D, E, F, S and C as local variables,

D := ADD(U,U); ... (4)

E := CAR(U,U); ... (5)

F := ADD(D,2E); ... (6)

S := ADD(F,L); ... (7)

C := CAR(F,L); ... (8)

MUL2(X,Y) := ADD(S,2C). ... (9)

Numerically the result is congruent to X*Y, the product of X and Y, modulo (2^{32} - 2). It is not necessarily the smallest residue because it may equal 2^{32} - 1 or 2^{32} - 2.

4.1.2.3 To calculate MUL2A(X,Y)

This is a simplified form of MUL2(X,Y) used in the main loop, which yields the correct result only when at least one of the numbers X and Y has a zero in its most significant bit.

This form of multiplication is employed for economy in processing. D, S, C are local variables,

D := ADD(U,U); ... (10)

S := ADD(D,L); ... (11)

C := CAR(D,L); ... (12)

MUL2A(X,Y):= ADD(S,2C). ... (13)

The result is congruent to X*Y modulo (2^{32} - 2) under the conditions stated because, in the notation of MUL2(X,Y) above, the carry E = 0.

4.1.3 Definition of the functions BYT[X||Y] and PAT[X||Y]

A procedure is used in the prelude to condition both the key parts and the results in order to prevent long strings of ones or zeros. It produces two results which are the conditioned values of X and Y and a number PAT[X,Y] which records the changes that have been made. PAT[X,Y] < 255 so it is essentially an 8 bit number.

X and Y are regarded as strings of bytes.

[X||Y] = [B_0|| B_1|| B_2|| B_3|| B_4|| B_5|| B_6|| B_7]

Thus bytes B_0 to B_3 are derived from X and B_4 to B_7 from Y.

The procedure is best described by a procedure where each byte B_i is regarded as an integer of length 8 bits.

```
begin
   P := 0
   for i := 0 to 7 do
   begin
      P := 2*P;
      if B[i]= 0 then
      begin
         P := P + 1;
         B'[i] := P
      end
      else
         if B[i]= 255 then
         begin
            P : = P + 1;
            B'[i] := 255 - P
         end
         else
            B'[i] := B[i];
   end
end;
```

NOTE 1 The procedure is written in the programming language PASCAL (see ISO 7185), except that the non-standard identifier B′ has been used to maintain continuity with the text. The symbols B[i] and B′[i] correspond to B_i and B'_i in the text.

The results are

$BYT[X||Y] = [B'_0 || B'_1 || B'_2 || B'_3 || B'_4 || B'_5 || B'_6 || B'_7]$

and

$PAT[X||Y] = P$

4.2 Specification of the algorithm

4.2.1 The prelude

$[J_1||K_1] :=$ BYT$[J||K]$;

$P :=$ PAT$[J||K]$;

$Q := (1 + P)*(1 + P)$. ... (14)

First, by means of a calculation using J_1, produce H_4, H_6, and H_8 from which X_0, V_0 and S are derived.

$J1_2$:= MUL1(J_1,J_1); $J2_2$:= MUL2(J_1,J_1);

$J1_4$:= MUL1($J1_2$,$J1_2$); $J2_4$:= MUL2($J2_2$,$J2_2$);

$J1_6$:= MUL1($J1_2$,$J1_4$); $J2_6$:= MUL2($J2_2$,$J2_4$);

$J1_8$:= MUL1($J1_2$,$J1_6$); $J2_8$:= MUL2($J2_2$,$J2_6$). ... (15)

H_4 := XOR($J1_4$,$J2_4$);

H_6 := XOR($J1_6$,$J2_6$);

H_8 := XOR($J1_8$,$J2_8$). ... (16)

From a similar calculation using K_1, produce H_5, H_7 and H_9, from which Y_0, W and T are derived.

$K1_2$:= MUL1(K_1,K_1); $K2_2$:= MUL2(K_1,K_1);

$K1_4$:= MUL1($K1_2$,$K1_2$); $K2_4$:= MUL2($K2_2$,$K2_2$);

$K1_5$:= MUL1(K_1,$K1_4$); $K2_5$:= MUL2(K_1,$K2_4$);

$K1_7$:= MUL1($K1_2$,$K1_5$); K27 := MUL2($K2_2$,$K2_5$);

$K1_9$:= MUL1($K1_2$,$K1_7$); $K2_9$:= MUL2($K2_2$,$K2_7$). ...(17)

H′ := XOR($K1_5$,$K2_5$);

H_5 := MUL2(H′,Q);

H_7 := XOR($K1_7$,$K2_7$);

H_9 := XOR($K1_9$,$K2_9$). ...(19)

Finally, condition the results using the BYT function

$[X_0||Y_0]$:= BYT$[H_4||H_5]$;
$[V_0||W]$:= BYT$[H_6||H_7]$;
$[S||T]$:= BYT$[H_8||H_9]$. ...(20)

4.2.2 The main loop

This loop shall be performed in turn for each of the message blocks M_i. In addition to M_i, the principal values employed shall be X and Y and the main results shall be the new values of X and Y. It shall also use V and W and modify V at each performance. X, Y and V shall be initialized with the values provided by the prelude. In order to use the same keys again, the initial values of X, Y and V shall be preserved, therefore they shall be denoted X_0, Y_0 and V_0 and there shall be an initializing step $X := X_0$, $Y := Y_0$, $V := V_0$, after which the main loop shall be entered for the first time.

NOTE 2 The program is shown in columns to clarify its parallel operation but it should be read in normal reading order, left to right on each line.

V := CYC(V);

E := XOR(V,W); ...(21)

X := XOR(X,M_i); Y := XOR(Y,M_i); ...(22)

F := ADD(E,Y); G := ADD(E,X);

F := OR(F,A); G := OR(G,B);

F := AND(F,C); G := AND(G,D); ...(23)

X := MUL1(X,F); Y := MUL2A(Y,G). ...(24)

The numbers A, B, C, D are constants which are, in hexadecimal notation:

Constant A: 0204 0801
Constant B: 0080 4021
Constant C: BFEF 7FDF
Constant D: 7DFE FBFF

NOTE 3 Lines (21) are common to both paths. Line (22) introduces the message block M_i. Lines (23) prepare the multipliers and line (24) generates new X and Y values. Only X, Y and V are modified for use in the next cycle. F and G are local variables. Since the constant D has its most significant digit zero, $G < 2^{31}$ and this ensures that MUL2A in line (24) will give the correct result.

4.2.3 The coda

The coda shall be performed after the last message block of the segment has been processed, by applying the main loop to message block S, then again to message block T. Then the result Z = XOR(X,Y) shall be calculated. This completes the coda. If the message contains no more than 256 message blocks, Z is the value of the MAC. Otherwise the value of Z shall be used in the mode of operation specified in clause 5.

NOTE 4 In order to calculate further Z values without repeating the prelude (key calculation) until the key is changed the values X_0, Y_0, V_0, W, S and T should be retained.

5 Specification of the mode of operation

Messages longer than 256 message blocks shall be divided into segments SEG_1,SEG_2...SEG_5 each of 256 blocks except that the last segment may have from 1 to 256 blocks. The number of segments is s.

The result Z of the segment algorithm specified in clause 4, when applied to key J,K and a message M shall be denoted Z(J,K,M).

The mode of operation for calculating the MAC for a message of more than 256 blocks shall employ the above algorithm once for each segment. The algorithm specified in clause 4 shall be applied to the first segment to produce:

$Z_1 = Z(J,K,SEG_1)$.

Z_1 shall be concatenated with the second segment to produce $[Z_1||SEG_2]$, to which the algorithm shall be applied:

$Z_2 = Z(J,K,[Z_1||SEG_2])$.

Note that Z_1 is treated as a message block which is prefixed to SEG_2 to form a segment of up to 257 blocks.

If there are no more segments, Z_2 shall be the resultant MAC for the whole message, otherwise the procedure shall continue, and for the ith segment:

$Z_i = Z(J,K,[Z_{i-1}||SEG_i])$.

There are in total s segments; then Z_s shall be the resultant MAC for the whole message.

NOTE 5 The prelude need be performed only once and its results (line 20) may be retained for use on each Z_i calculation. The main loop is performed once for each message block, including the prefixed Z_i blocks. The coda is performed at the end of each segment, since it is part of the segment algorithm specified in clause 4.

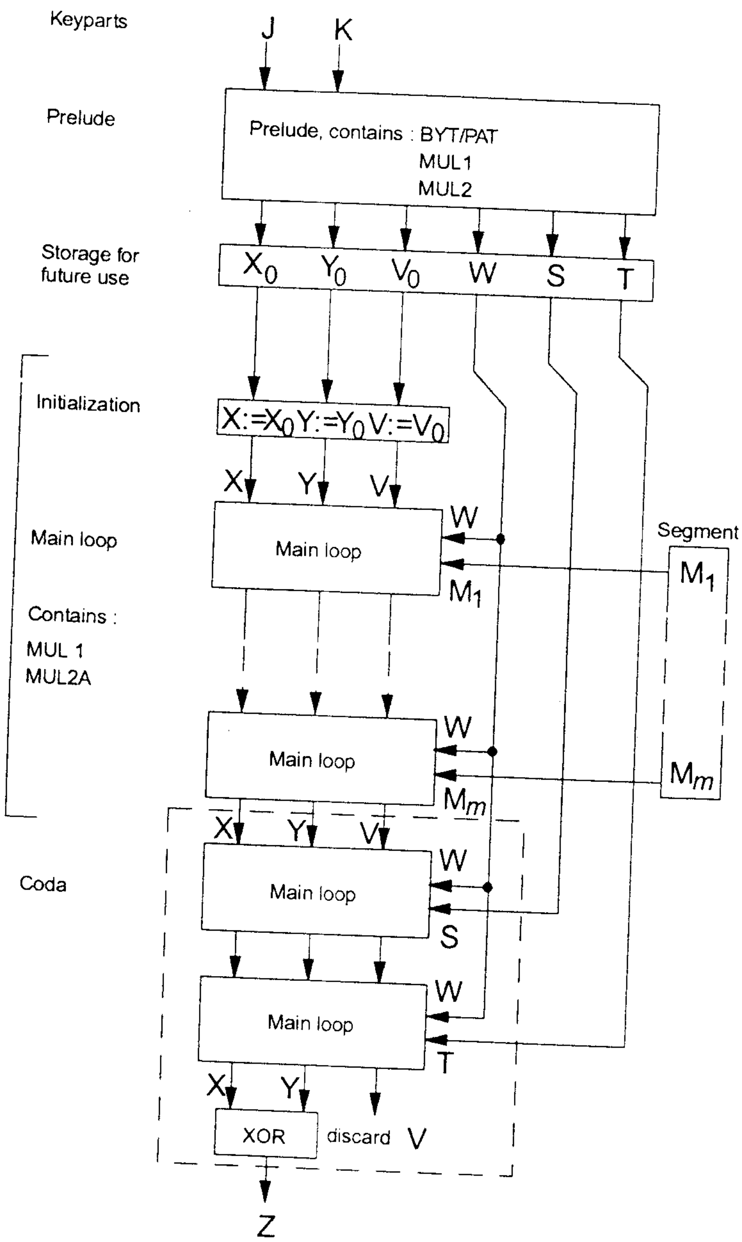

Figure 1 - Schematic showing data flow for the segment algorithm applied to a segment of m message blocks

Annex A

(informative)

Test examples for implementation of the algorithm

A.1 General

For most parts of the algorithm, simple test examples are given. The data used are not always realistic, i.e. they are not values which could be produced by earlier parts of the algorithm, and artificial values of constants are used. This is done to keep the test cases so simple that they can be verified by a pencil and paper calculation and thus the verification of the algorithm's implementations does not consist of comparing one machine implementation with another. The parts thus tested are:

- MUL1, MUL2, MUL2A;
- BYT[X,Y] and PAT[X,Y];
- Prelude, except the initial BYT[J,K] operation;
- Main loop.

The coda is not tested separately because it uses only the main loop and one XOR function. For testing the whole algorithm, some results from a trial implementation are given.

A.2 Test examples for MUL1, MUL2, MUL2A

It is suggested that the multiplication operations should be tested with very small numbers and very large numbers. To represent a large number these examples use the ones complement. Thus if *a* is a small number (say less than 4 096) the notation $\bar{a}$ is used to mean its complement, i.e. $2^{32} - 1 - a$.

For small numbers *a* and *b*, all three multiplication functions produce their true product $a*b$. When large numbers are used the functions can give different results. They should be tested both ways round, with MUL(x,y) and MUL(y,x) to verify that these are equal.

A.2.1 Test cases for MUL1

In modulo $(2^{32} - 1)$ arithmetic $\bar{a}$ is effectively $- a$, therefore the results are very simple

$\mathrm{MUL1}(\bar{a},b) = \mathrm{MUL1}(a,\bar{b}) = \overline{a*b}$

$\mathrm{MUL1}(\bar{a},\bar{b}) = a*b$

Examples for testing are given in table 1.

A.2.2 Test cases for MUL2

$\mathrm{MUL2}(\bar{a},b) = \overline{a*b-b+1}$

$\mathrm{MUL2}(a,\bar{b}) = \overline{a*b-a+1}$

$\mathrm{MUL2}(\bar{a},\bar{b}) = a*b-a-b+1$

Examples for testing are given in table 1.

A.2.3 Test cases for MUL2A

This will give the same result as MUL2 when tested with numbers within its range. For testing with large numbers, $\bar{a}$ and $\bar{b} - 2^{31}$ shall be used

$\mathrm{MUL2A}(\bar{a},b) = \overline{a*b-b+1}$

$\mathrm{MUL2A}(a,\bar{b}) = \overline{a*b-a+1}$

$\mathrm{MUL2A}(\bar{a},\bar{b} - 2^{31}) = 2^{31} * (1 - p) + a*b + p - b - 1$

where *p* is the parity of *a*, the value of its least significant bit.

That is, for even values of *a* the result is $2^{31} + a*b - b - 1$ and for odd values of *a* the result is $a*b - b$.

Examples for testing are given in table A.1.

Table A.1 - Test cases for multiplication functions (hexadecimal)

Function	a	b	Result
MUL1	0000 000F	0000 000E	0000 00D2
	FFFF FFF0	0000 000E	FFFF FF2D
	FFFF FFF0	FFFF FFF1	0000 00D2
MUL2	0000 000F	0000 000E	0000 00D2
	FFFF FFF0	0000 000E	FFFF FF3A
	FFFF FFF0	FFFF FFF1	0000 00B6
MUL2A	0000 000F	0000 000E	0000 00D2
	FFFF FFF0	0000 000E	FFFF FF3A
	7FFF FFF0	FFFF FFF1	8000 00C2
	FFFF FFF0	7FFF FFF1	0000 00C4

A.3 Test examples for BYT and PAT

Three cases for testing these functions are listed in table A.2.

Table A.2 - Test cases for the BYT and PAT functions

Function	X	Y
[X||Y]	00 00 00 00	00 00 00 00
BYT[X||Y]	01 03 07 0F	1F 3F 7F FF
PAT[X||Y]	FF	
[X||Y]	FF FF 00 FF	FF FF FF FF
BYT[X||Y]	FE FC 07 F0	E0 C0 80 00
PAT[X||Y]	FF	
[X||Y]	AB 00 FF CD	FF EF 00 01
BYT[X||Y]	AB 01 FC CD	F2 EF 35 01
PAT[X||Y]	6A	

A.4 Test examples for the prelude

An example is given in table A.3. The initial BYT[J||K] operation is not tested. It is assumed that the results from lines (14) are

J_1 = 0000 0100, K_1 = 0000 0080, P = 1.

Table A.3 - Test cases for lines (15) to (20) of the prelude

$J1_2$	0001 0000	$J2_2$	0001 0000
$J1_4$	0000 0001	$J2_4$	0000 0002
$J1_6$	0001 0000	$J2_6$	0002 0000
$J1_8$	0000 0001	$J2_8$	0000 0004
H_4		0000 0003	
H_6		0003 0000	
H_8		0000 0005	
$K1_2$	0000 4000	$K2_2$	0000 4000
$K1_4$	1000 0000	$K2_4$	1000 0000
$K1_5$	•0000 0008	$K2_5$	0000 0010
$K1_7$	0002 0000	$K2_7$	0004 0000
$K1_9$	8000 0000	$K2_9$	0000 0002
H′		0000 0018	
H_5		0000 0060 (Q = 4)	
H_7		0006 0000	
H_9		8000 0002	
[X_0‖Y_0]	0103 0703 1D3B 7760	PAT[X_0‖Y_0]	EE (1110 1110)
[V_0‖W]	0103 050B 1706 5DBB	PAT[V_0‖W]	BB (1011 1011)
[S‖T]	0103 0705 8039 7302	PAT[S‖T]	E6 (1110 0110)

The PAT values obtained from conditioning the results of the prelude are quoted above for checking purposes but are not used in the algorithm.

A.5 Test examples for the main loop

In table A.4, three examples of single block messages are given, using small and large numbers with the convention that $\bar{a}$ *is* $2^{32} - 1 - a$. In the third example there are two cases of large numbers which must have zero in the 32nd bit, shown as $\bar{2} - 2^{31}$ and $\bar{3} - 2^{31}$ respectively. They could have been written $2^{31} - 3$ and $2^{31} - 4$ respectively. In order to keep the numbers small, artificial values of the constants A, B, C and D are used. Three single block examples are followed by a message of three blocks, in order to check that the implementation correctly retains the value of X, Y and W. The final S and T cycles of the coda are not included in this table.

Table A.4 - Test cases for the main loop (decimal)

		Single block messages						Three-block message						
A	B	4	1	1	4	1	2	2	1	2	1	2	1	
C	D	$\bar{8}$	$\bar{4}$	$\bar{6}$	$\bar{3}$	$\bar{1}$	$\overline{2*}$	$\bar{4}$	$\bar{4}$	$\bar{4}$	$\bar{4}$	$\bar{4}$	$\bar{4}$	
V	W	3	3	3	3	7	7	1	1	2	1	4	1	
X_0	Y_0	2	3	$\bar{2}$	$\bar{3}$	$\bar{2}$	$\bar{3}$	1	2	3	2	20	9	
M		5		1		8		0		1		2		
V		6		6		14		2		4		8		CYC
E		5		5		9		3		5		9		XOR
X	Y	7	6	$\bar{3}$	$\bar{2}$	$\overline{10}$	$\overline{11}$	1	2	2	3	22	11	XOR
F	G	11	12	2	1	$\bar{2}$	$\bar{1}$	5	4	8	7	20	31	ADD
F	G	15	13	3	5	$\bar{2}$	$\bar{1}$	7	5	10	7	22	31	OR
F	G	7	9	1	4	$\bar{3}$	$\overline{3*}$	3	1	10	3	18	27	AND
X	Y	49	54	$\bar{3}$	$\bar{5}$	30	30	3	2	20	9	396	297	MUL
Z		7		6		0		1		29		165		XOR

* $- 2^{31}$

A.6 Test examples for the whole algorithm

Using the original implementation of the algorithm, the four test examples with two block messages given in table A.5 were calculated. For ease of checking, intermediate results are tabulated: the results of the prelude and the X and Y values after each operation of the main loop, that is for M_1, M_2, S and T.

Table A.5 - Test cases for the whole algorithm

J	00FF 00FF	00FF 00FF	5555 5555	5555 5555
K	0000 0000	0000 0000	5A35 D667	5A35 D667
P	FF	FF	00	00
X_0	4A64 5A01	4A64 5A01	34AC F886	34AC F886
Y_0	50DE C930	50DE C930	7397 C9AE	7397 C9AE
V_0	5CCA 3239	5CCA 3239	7201 F4DC	7201 F4DC
W	FECC AA6E	FECC AA6E	2829 040B	2829 040B
M_1	5555 5555	AAAA AAAA	0000 0000	FFFF FFFF
X	48B2 04D6	6AEB ACF8	2FD7 6FFB	8DC8 BBDE
Y	5834 A585	9DB1 5CF6	550D 91CE	FE4E 5BDD
M_2	AAAA AAAA	5555 5555	FFFF FFFF	0000 0000
X	4F99 8E01	270E EDAF	A70F C148	CBC8 65BA
Y	BE9F 0917	B814 2629	1D10 D8D3	0297 AF6F
S	51ED E9C7	51ED E9C7	9E2E 7B36	9E2E 7B36
X	3449 25FC	2990 7CD8	B1CC 1CC5	3CF3 A7D2
Y	DB91 02B0	BA92 DB12	29C1 485F	160E E9B5
T	24B6 6FB5	24B6 6FB5	1364 7149	1364 7149
X	277B 4B25	28EA D8B3	288F C786	D048 2465
Y	D636 250D	81D1 0CA3	9115 A558	7050 EC5E
Z	F14D 6E28	A93B D410	B99A 62DE	A018 C83B

A further set of test cases for the whole algorithm is given in table A.6. The J and K values were chosen to give long strings of zeros after conditioning. The message consists of 20 blocks of zeros. Intermediate values of X and Y are listed as well as the final authenticator value Z.

J = 8001 8001, K = 8001 8000 (all message blocks are zeros)

Table A.6 - Test case for a 20 block message

Block	X	Y	Z
1	303F F4AA	1277 A6D4	
2	55DD 063F	4C49 AAE0	
3	51AF 3C1D	5BC0 2502	
4	A44A AAC0	63C7 0DBA	
5	4D53 901A	2E80 AC30	
6	5F38 EEF1	2A60 91AE	
7	F023 9DD5	3DD8 1AC6	
8	EB35 B97F	9372 CDC6	
9	4DA1 24A1	C6B1 317E	
10	7F83 9576	74B3 9176	
11	11A9 D254	D786 34BC	
12	D880 4CA5	FDC1 A8BA	
13	3F6F 7248	11AC 46B8	
14	ACBC 13DD	33D5 A466	
15	4CE9 33E1	C21A 1846	
16	C1ED 90DD	CD95 9B46	
17	3CD5 4DEB	613F 8E2A	
18	BBA5 7835	07C7 2EAA	
19	D784 3FDC	6AD6 E8A4	
20	5EBA 06C2	9189 6CFA	
S	1D9C 9655	98D1 CC75	
T	7BC1 80AB	A0B8 7B77	DB79 FBDC

Annex B

(informative)

Specification of MAA in VDM

B.1 General

In the following section is a complete specification of the MAA in the specification language called the Vienna Development Method (VDM). The notation for the VDM is that of the emerging standard for VDM as described in *VDM Specification Language Proto-Standard, ISO/IEC JTC1/SC22/WG19, Document Reference IN9.*

It demonstrates how it is possible to write a standard in an unambiguous formal language. The style of the VDM has been guided by the following:

- It has been written in a functional way so that it could be implemented easily although not necessarily efficiently in a functional, logic or imperative programming language.
- It retains as much of the naming, structure etc. used in the main part of this standard.

The VDM in the next section is written purely in VDM, including the comments. The comments point to sections of the main text of the standard from which the VDM is derived. The VDM models a message as a sequence of natural numbers 0 and 1 (*Bits*).

B.2 The specification

definitions

values

-- **3.2 Technical**

$Word\text{-}length = 32;$

$Maximum\text{-}Number\text{-}Size = (2 \uparrow Word\text{-}length) - 1;$

$Maximum\text{-}Number\text{-}Size\text{-}plus\text{-}1 = Maximum\text{-}Number\text{-}Size + 1;$

$Maximum\text{-}Number\text{-}Size\text{-}plus\text{-}1\text{-}div\text{-}2 = Maximum\text{-}Number\text{-}Size\text{-}plus\text{-}1 \text{ div } 2;$

$Maximum\text{-}No\text{-}of\text{-}Message\text{-}blocks = 1000000;$

-- **4.2.2 The main loop**

$A = 2 \times 2 \uparrow 24 + 4 \times 2 \uparrow 16 + 8 \times 2 \uparrow 8 + 1;$

$B = 0 \times 2 \uparrow 24 + 128 \times 2 \uparrow 16 + 64 \times 2 \uparrow 8 + 33;$

$C = 191 \times 2 \uparrow 24 + 239 \times 2 \uparrow 16 + 127 \times 2 \uparrow 8 + 223;$

$D = 125 \times 2 \uparrow 24 + 254 \times 2 \uparrow 16 + 251 \times 2 \uparrow 8 + 255;$

-- **5 Specification of the mode of operation**

$\mathit{Maximum\text{-}No\text{-}of\text{-}blocks\text{-}for\text{-}SEG} = 256;$

$\mathit{Maximum\text{-}No\text{-}of\text{-}blocks\text{-}for\text{-}SEG\text{-}plus\text{-}1} = \mathit{Maximum\text{-}No\text{-}of\text{-}blocks\text{-}for\text{-}SEG} + 1;$

types

-- **3.2 Technical**

$\mathit{Number} = \mathbf{N}$

inv $N \triangleq N < \mathit{Maximum\text{-}Number\text{-}Size\text{-}plus\text{-}1};$

$\mathit{Bit} = \mathbf{N}$

inv $B \triangleq B \in \{0, 1\};$

$\mathit{Message\text{-}in\text{-}bits} = \mathit{Bit}^*$

inv $M \triangleq$
if (len M mod $\mathit{Word\text{-}length}) = 0$
then ((len M div $\mathit{Word\text{-}length}) \leq \mathit{Maximum\text{-}No\text{-}of\text{-}Message\text{-}blocks}) \wedge$
(len $M > 0$)
else ((len M div $\mathit{Word\text{-}length}) + 1) \leq \mathit{Maximum\text{-}No\text{-}of\text{-}Message\text{-}blocks};$

$\mathit{Message\text{-}in\text{-}blocks\text{-}plus\text{-}empty\text{-}Message} = \mathit{Number}^*$

inv $M \triangleq$ len $M \leq \mathit{Maximum\text{-}No\text{-}of\text{-}Message\text{-}blocks};$

$\mathit{Message\text{-}in\text{-}blocks} = \mathit{Message\text{-}in\text{-}blocks\text{-}plus\text{-}empty\text{-}Message}$

inv $M \triangleq 1 \leq$ len $M;$

– – **3.2 Technical**
– – **4.1.1 General definitions**

$Double\text{-}Number = Number^*$

inv $D \triangleq$ len $D = 2$;

$Key = Double\text{-}Number$;

– – **4.2.1 The prelude**

$$\begin{aligned}Key\text{-}Constant :: X0 &: Number\\ Y0 &: Number\\ V0 &: Number\\ W &: Number\\ S &: Number\\ T &: Number;\end{aligned}$$

functions

– – **3.2 Technical**

$Pad\text{-}out\text{-}Message : Message\text{-}in\text{-}bits \rightarrow Message\text{-}in\text{-}bits$

$Pad\text{-}out\text{-}Message\ (M) \triangleq$
let $No\text{-}Extra\text{-}bits = Word\text{-}length -$ (len M mod $Word\text{-}length$) in
if $No\text{-}Extra\text{-}bits = Word\text{-}length$
then M
else $M \frown Get\text{-}Application\text{-}defined\text{-}bits(M, No\text{-}Extra\text{-}bits)$;

$Get\text{-}Application\text{-}defined\text{-}bits\ (M : Message\text{-}in\text{-}bits, No\text{-}bits : \mathbb{N})\ E : Message\text{-}in\text{-}bits$
pre $No\text{-}bits < Word\text{-}length$
post len $E = No\text{-}bits$;

$Form\text{-}Message\text{-}into\text{-}blocks : Message\text{-}in\text{-}bits \rightarrow Message\text{-}in\text{-}blocks$

$Form\text{-}Message\text{-}into\text{-}blocks\ (M) \triangleq$
if len $M = Word\text{-}length$
then $[Form\text{-}Number(M)]$
else $[Form\text{-}Number(Get\text{-}head\text{-}in\text{-}bits(M, Word\text{-}length))] \frown$
$Form\text{-}Message\text{-}into\text{-}blocks(Get\text{-}tail\text{-}in\text{-}bits(M, Word\text{-}length))$
pre (len $M \geq Word\text{-}length$) $\wedge$ (len M mod $Word\text{-}length = 0$);

$Form\text{-}Number : Message\text{-}in\text{-}bits \rightarrow Number$

$Form\text{-}Number\,(M) \triangleq$
  if len $M = 1$
  then hd M
  else hd $M + 2 \times (Form\text{-}Number(\text{tl } M))$
pre len $M \leq Word\text{-}length$;

-- **4 The segment algorithm**
-- **4.1 Definition of the functions used in the algorithm**
-- **4.1.1 General definitions**

$CYC : Number \rightarrow Number$

$CYC\,(X) \triangleq$
  $ADD(X, X) + CAR(X, X)$;

$AND : Number \times Number \rightarrow Number$

$AND\,(X, Y) \triangleq$
  if $(X = 0) \vee (Y = 0)$
  then 0
  else $(X \text{ mod } 2) \times (Y \text{ mod } 2) + 2 \times (AND(X \text{ div } 2, Y \text{ div } 2))$;

$OR : Number \times Number \rightarrow Number$

$OR\,(X, Y) \triangleq$
  if $(X = 0) \vee (Y = 0)$
  then $X + Y$
  else $max(X \text{ mod } 2, Y \text{ mod } 2) + 2 \times (OR(X \text{ div } 2, Y \text{ div } 2))$;

$max : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$

$max\,(X, Y) \triangleq$
  if $X \geq Y$
  then X
  else Y;

$XOR : Number \times Number \rightarrow Number$

$XOR\,(X, Y) \triangleq$
  if $(X = 0) \vee (Y = 0)$
  then $X + Y$
  else $((X + Y) \text{ mod } 2) + 2 \times (XOR(X \text{ div } 2, Y \text{ div } 2))$;

$ADD : Number \times Number \rightarrow Number$

$ADD\,(X, Y) \triangleq$
$(X + Y) \bmod (Maximum\text{-}Number\text{-}Size\text{-}plus\text{-}1);$

$CAR : Number \times Number \rightarrow Number$

$CAR\,(X, Y) \triangleq$
$(X + Y)\ \mathrm{div}\ (Maximum\text{-}Number\text{-}Size\text{-}plus\text{-}1);$

- - 4.1.2 Definition of multiplication functions

- - 4.1.2.1 To calculate MUL1(X,Y)

$MUL1 : Number \times Number \rightarrow Number$

$MUL1\,(X, Y) \triangleq$
let $L = (X \times Y) \bmod (Maximum\text{-}Number\text{-}Size\text{-}plus\text{-}1)$,
$U = (X \times Y)\ \mathrm{div}\ (Maximum\text{-}Number\text{-}Size\text{-}plus\text{-}1)$ in
let $S = ADD(U, L)$,
$C = CAR(U, L)$ in
$ADD(S, C);$

- - 4.1.2.2 To calculate MUL2(X,Y)

$MUL2 : Number \times Number \rightarrow Number$

$MUL2\,(X, Y) \triangleq$
let $L = (X \times Y) \bmod (Maximum\text{-}Number\text{-}Size\text{-}plus\text{-}1)$,
$U = (X \times Y)\ \mathrm{div}\ (Maximum\text{-}Number\text{-}Size\text{-}plus\text{-}1)$ in
let $D = ADD(U, U)$,
$E = CAR(U, U)$ in
let $F = ADD(D, 2 \times E)$ in
let $S = ADD(F, L)$,
$C = CAR(F, L)$ in
$ADD(S, 2 \times C);$

– – 4.1.2.3 To calculate MUL2A(X,Y)

$MUL2A : Number \times Number \rightarrow Number$

$MUL2A(X, Y) \triangleq$

let $L = (X \times Y)$ mod $(Maximum\text{-}Number\text{-}Size\text{-}plus\text{-}1)$,
  $U = (X \times Y)$ div $(Maximum\text{-}Number\text{-}Size\text{-}plus\text{-}1)$ in
let $D = ADD(U, U)$ in
let $S = ADD(D, L)$,
  $C = CAR(D, L)$ in
$ADD(S, 2 \times C)$
pre $((X$ div $Maximum\text{-}Number\text{-}Size\text{-}plus\text{-}1\text{-}div\text{-}2) = 0) \vee$
  $((Y$ div $Maximum\text{-}Number\text{-}Size\text{-}plus\text{-}1\text{-}div\text{-}2) = 0)$;

– – 4.1.3 Definitions of the functions BYT[X,Y] and PAT[X,Y]

$BYT : Double\text{-}Number \rightarrow Double\text{-}Number$

$BYT(K) \triangleq$

let $X =$ hd K,
  $Y =$ hd tl K in
let $X' = [Byte(X,3), Byte(X,2), Byte(X,1), Byte(X,0)]$,
  $Y' = [Byte(Y,3), Byte(Y,2), Byte(Y,1), Byte(Y,0)]$ in
let $XY = X' \curvearrowright Y'$,
  $P = 0$ in
let $XY' = Condition\text{-}Sequence(XY, P)$ in
let $X'' = Get\text{-}head\text{-}in\text{-}blocks(XY', 4)$,
  $Y'' = Get\text{-}tail\text{-}in\text{-}blocks(XY', 4)$ in
$[Convert\text{-}Bytes\text{-}to\text{-}Number(X'')] \curvearrowright [Convert\text{-}Bytes\text{-}to\text{-}Number(Y'')]$;

$Byte : Number \times \mathbf{N} \rightarrow Number$

$Byte(N, B) \triangleq$

if $B = 0$
then N mod $2 \uparrow 8$
else $Byte((N$ div $2 \uparrow 8), B - 1)$
pre $(B \geq 0) \wedge (B \leq 3)$;

$Condition\text{-}Sequence : Message\text{-}in\text{-}blocks \times Number \rightarrow Message\text{-}in\text{-}blocks$

$Condition\text{-}Sequence(M, P) \triangleq$

if len $M = 1$
then $[Condition\text{-}value($hd $M, P)]$
else $[Condition\text{-}value($hd $M, P)] \curvearrowright Condition\text{-}Sequence($tl $M, Changes($hd $M, P))$;

$Condition\text{-}value : Number \times Number \rightarrow Number$

$Condition\text{-}value\ (B, P) \triangleq$
let $P' = 2 \times P$ in
let $P'' = P' + 1$ in
if $B = 0$
then P''
else if $B = 2 \uparrow 8 - 1$
then $(2 \uparrow 8 - 1) - P''$
else B;

$Changes : Number \times Number \rightarrow Number$

$Changes\ (B, P) \triangleq$
let $P' = 2 \times P$ in
let $P'' = P' + 1$ in
if $(B = 0) \vee (B = 2 \uparrow 8 - 1)$
then P''
else P';

$Convert\text{-}Bytes\text{-}to\text{-}Number : Message\text{-}in\text{-}blocks \rightarrow Number$

$Convert\text{-}Bytes\text{-}to\text{-}Number\ (M) \triangleq$
if len $M = 1$
then hd M
else $Convert\text{-}Bytes\text{-}to\text{-}Number(\text{tl } M) + (\text{hd } M) \times 2 \uparrow 8 \times (\text{len } M - 1)$;

$PAT : Double\text{-}Number \rightarrow Number$

$PAT\ (D) \triangleq$
let $X = \text{hd } D$,
$Y = \text{hd tl } D$ in
let $X' = [Byte(X,3), Byte(X,2), Byte(X,1), Byte(X,0)]$,
$Y' = [Byte(Y,3), Byte(Y,2), Byte(Y,1), Byte(Y,0)]$ in
let $XY = X' \frown Y'$,
$P = 0$ in
$Record\text{-}Changes(XY, P)$;

$Record\text{-}Changes : Message\text{-}in\text{-}blocks \times Number \rightarrow Number$

$Record\text{-}Changes\ (M, P) \triangleq$
if len $M = 1$
then $Changes(\text{hd } M, P)$
else $Record\text{-}Changes(\text{tl } M, Changes(\text{hd } M, P))$;

– – 4.2 Specification of the algorithm

– – 4.2.1 The prelude

$Prelude : Key \rightarrow Key\text{-}Constant$

$Prelude\,(K) \triangleq$
let $J1K1 = BYT(K)$ in
let $J1 =$ hd $J1K1$,
$K1 =$ hd tl $J1K1$,
$P = PAT(K)$,
$Q = (1 + P) \times (1 + P)$ in
let $J12 = MUL1(J1, J1)$,
$J22 = MUL2(J1, J1)$ in
let $J14 = MUL1(J12, J12)$,
$J24 = MUL2(J22, J22)$ in
let $J16 = MUL1(J12, J14)$,
$J26 = MUL2(J22, J24)$ in
let $J18 = MUL1(J12, J16)$,
$J28 = MUL2(J22, J26)$ in
let $H4 = XOR(J14, J24)$,
$H6 = XOR(J16, J26)$,
$H8 = XOR(J18, J28)$ in
let $K12 = MUL1(K1, K1)$,
$K22 = MUL2(K1, K1)$ in
let $K14 = MUL1(K12, K12)$,
$K24 = MUL2(K22, K22)$ in
let $K15 = MUL1(K1, K14)$,
$K25 = MUL2(K1, K24)$ in
let $K17 = MUL1(K12, K15)$,
$K27 = MUL2(K22, K25)$ in
let $K19 = MUL1(K12, K17)$,
$K29 = MUL2(K22, K27)$ in
let $H' = XOR(K15, K25)$ in
let $H5 = MUL2(H', Q)$,
$H7 = XOR(K17, K27)$,
$H9 = XOR(K19, K29)$ in
let $X0Y0 = BYT([H4, H5])$,
$V0W = BYT([H6, H7])$,
$ST = BYT([H8, H9])$ in
$mk\text{-}Key\text{-}Constant($hd $X0Y0$, hd tl $X0Y0$, hd $V0W$, hd tl $V0W$, hd ST, hd tl $ST)$;

– – **4.2.2 The main loop**

Main-loop : *Message-in-blocks-plus-empty-Message* × *Key-Constant* → *Number*

Main-loop $(M, KC) \triangleq$
  let $mk\text{-}Key\text{-}Constant(X, Y, V, W, S, T) = KC$ in
  if len $M = 0$
  then $XOR(X, Y)$
  else let $Mi =$ hd M in
    let $V' = CYC(V)$ in
    let $E = XOR(V', W)$,
      $X' = XOR(X, Mi)$,
      $Y' = XOR(Y, Mi)$ in
    let $F = ADD(E, Y')$,
      $G = ADD(E, X')$ in
    let $F' = OR(F, A)$,
      $G' = OR(G, B)$ in
    let $F'' = AND(F', C)$,
      $G'' = AND(G', D)$ in
    let $X'' = MUL1(X', F'')$,
      $Y'' = MUL2A(Y', G'')$ in
    $Main\text{-}loop($tl $M, mk\text{-}Key\text{-}Constant(X'', Y'', V', W, S, T))$;

– – **4.2.3 The coda**

Z : *Message-in-blocks* × *Key* → *Number*

$Z\,(M, K) \triangleq$
  let $KC = Prelude(K)$ in
  let $S = KC.S$,
    $T = KC.T$ in
  let $M' = M \frown [S] \frown [T]$ in
  $Main\text{-}loop(M', KC)$;

-- 5 Specification of the mode of operation

```
MAC : Message-in-bits × Key → Number
MAC(M,K) △
  let M' = Pad-out-Message(M) in
  let M'' = Form-Message-into-blocks(M') in
  if len M'' ≤ Maximum-No-of-blocks-for-SEG
  then Z(M'',K)
  else let M''' =
          [Z(Get-head-in-blocks(M'', Maximum-No-of-blocks-for-SEG), K)]
          ⁀ Get-tail-in-blocks(M'', Maximum-No-of-blocks-for-SEG) in
      Z-of-SEG(M''', K, Maximum-No-of-blocks-for-SEG-plus-1);

Z-of-SEG : Message-in-blocks × Key × N → Number
Z-of-SEG (M, K, No-blocks) △
  if len M ≤ No-blocks
  then Z(M,K)
  else let M' = [Z(Get-head-in-blocks(M, No-blocks), K)] ⁀
                Get-tail-in-blocks(M, No-blocks) in
      Z-of-SEG(M', K, No-blocks);
```

-- Auxiliary functions

-- (These are not directly derived from the main text of the standard)

```
Get-tail-in-bits : Message-in-bits × N → Message-in-bits
Get-tail-in-bits (M, No-bits) △
  if No-bits = 0
  then M
  else Get-tail-in-bits(tl M, No-bits − 1)
pre len M ≥ No-bits;

Get-head-in-bits : Message-in-bits × N → Message-in-bits
Get-head-in-bits (M, No-bits) △
  if No-bits = 1
  then [hd M]
  else [hd M] ⁀ Get-head-in-bits(tl M, No-bits − 1)
pre (len M ≥ No-bits) ∧ (No-bits ≥ 1);
```

$Get\text{-}tail\text{-}in\text{-}blocks : Message\text{-}in\text{-}blocks \times \mathbf{N} \rightarrow Message\text{-}in\text{-}blocks$

$Get\text{-}tail\text{-}in\text{-}blocks\ (M, No\text{-}blocks) \triangleq$
  if $No\text{-}blocks = 0$
  then M
  else $Get\text{-}tail\text{-}in\text{-}blocks(\mathsf{tl}\ M, No\text{-}blocks - 1)$
pre len $M \geq No\text{-}blocks$;

$Get\text{-}head\text{-}in\text{-}blocks : Message\text{-}in\text{-}blocks \times \mathbf{N} \rightarrow Message\text{-}in\text{-}blocks$

$Get\text{-}head\text{-}in\text{-}blocks\ (M, No\text{-}blocks) \triangleq$
  if $No\text{-}blocks = 1$
  then $[\mathsf{hd}\ M]$
  else $[\mathsf{hd}\ M] \frown Get\text{-}head\text{-}in\text{-}blocks(\mathsf{tl}\ M, No\text{-}blocks - 1)$
pre $(\mathsf{len}\ M \geq No\text{-}blocks) \wedge (No\text{-}blocks \geq 1)$;