

Information technology — Security techniques — Hash-functions —

Part 4: Hash-functions using modular arithmetic

ICS 35.040

National foreword

This British Standard is the UK implementation of ISO/IEC 10118-4:1998+A1:2014, incorporating corrigendum July 2014. It supersedes BS ISO/IEC 10118-4:1998, which is withdrawn.

The start and finish of text introduced or altered by corrigendum is indicated in the text by tags. Text altered by ISO/IEC corrigendum July 2014 is indicated in the text by AC1 AC1.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT – Security techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

The publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard, having been prepared under the direction of the DISC Board, was published under the authority of the Standards Committee and comes into effect on 15 March 1999

© The British Standards Institution 2014.
Published by BSI Standards Limited 2014

ISBN 978 0 580 80109 9

Amendments/corrigenda issued since publication

Date	Comments
31 August 2014	Implementation of ISO/IEC corrigendum July 2014
31 December 2014	Implementation of ISO/IEC amendment 1:2014: Annex C replaced and Bibliography added

INTERNATIONAL STANDARD

ISO/IEC 10118-4

First edition
1998-12-15

Information technology — Security techniques — Hash-functions —

Part 4: Hash-functions using modular arithmetic

*Technologies de l'information — Techniques de sécurité — Fonctions
de brouillage —*

Partie 4: Fonctions de hachage utilisant l'arithmétique modulaire



Contents

	Page
Foreword	iii
1 Scope	1
2 Normative reference	1
3 Terms and definitions	1
3.1 From ISO/IEC 10118-1	1
3.2 Unique to this part of ISO/IEC 10118	1
3.3 Conventions	2
4 Symbols and abbreviated terms	2
4.1 From ISO/IEC 10118-1	2
4.2 Unique to this part of ISO/IEC 10118	2
5 Requirements	3
6 Variables and values needed for the hash operation	4
6.1 The length of the hash-code and of the modulus	4
6.2 The modulus of the round-function	4
6.3 Initializing value	4
6.4 Exponent	4
6.5 Reduction-function prime number	4
7 Hashing procedure	4
7.1 Preparation of the data string	4
7.1.1 Padding the data string	4
7.1.2 Appending the length	4
7.1.3 Splitting the data string	4
7.1.4 Expansion	4
7.2 Application of the round-function	5
7.3 The Reduction-function	5
7.3.1 Splitting the block H_q	5
7.3.2 Extending the data string	5
7.3.3 Processing the half-blocks	5
7.3.4 Reduction	5
8 Hash-functions	5
8.1 MASH-1	5
8.2 MASH-2	5
Annex A (informative) Examples	7
Annex B (informative) Additional information	21
Annex C (normative) Object identifiers	21
Bibliography	22
Figure 1 — The MASH hash-function	6

Foreword

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

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

International Standard ISO/IEC 10118-4 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC27, *IT Security techniques*.

ISO/IEC 10118 consists of the following parts, under the general title *Information technology — Security techniques — Hash-functions*:

- *Part 1: General*;
- *Part 2: Hash-functions using an n -bit block cipher algorithm*;
- *Part 3: Dedicated hash-functions*;
- *Part 4: Hash-functions using modular arithmetic*.

Annex A, Annex B and Annex C of this part of ISO/IEC 10118 are for information only.

Foreword to amendment A1

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 10118-4 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security technology*.

Amendment 1 to ISO/IEC 10118-4:1998 was written to serve two purposes.

First, a new normative Annex C is produced for the object identifiers assigned to the hash-functions included in ISO/IEC 10118-4:1998.

Second, the present Annex C for Bibliography is moved to the end of the text, after the new Annex C according to ISO/IEC Directives, Part 2.

1 Scope

This part of ISO/IEC 10118 specifies two hash-functions which make use of modular arithmetic. These hash-functions, which are believed to be collision-resistant, compress messages of arbitrary but limited length to a hash-code whose length is determined by the length of the prime number used in the reduction-function defined in 7.3. Thus, the hash-code is easily scaled to the input length of any mechanism (e.g., signature algorithm, identification scheme).

The hash-functions specified in this part of ISO/IEC 10118, known as MASH-1 and MASH-2 (Modular Arithmetic Secure Hash) are particularly suitable for environments in which implementations of modular arithmetic of sufficient length are already available. The two hash-functions differ only in the exponent used in the round-function.

2 Normative reference

The following standard contains provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 10118. At the time of publication, the edition indicated was valid. All standards are subject to revision and parties to agreements based on this part of ISO/IEC 10118 are encouraged to investigate the possibility of applying the most recent edition of the standard indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO/IEC 10118-1:1994, *Information technology — Security techniques — Hash-functions — Part 1: General*.

3 Terms and definitions

For the purposes of this part of ISO/IEC 10118, the following definitions apply.

3.1 From ISO/IEC 10118-1

- collision-resistant hash-function
- data string (data)
- hash-code
- hash-function
- initializing value
- padding.

3.2 Unique to this part of ISO/IEC 10118

3.2.1

block

a string of bits of length L_ϕ , which shall be an integer multiple of 16 (see also clause 6.1)

EXAMPLE The length of the output H_j of the round-function

3.2.2

half-block

a string of bits of length $L_\phi/2$

EXAMPLE Half the length of the block H_j

3.2.3

hash-function identifier

a byte identifying a specific hash-function

3.2.4

modulus

a parameter which is a positive integer and a product of two distinct prime numbers

3.2.5

reduction-function

a function RED that is applied to the block H_q of length L_ϕ to generate the hash-code H of length L_p

3.2.6

round-function

a function $\phi(;)$ that transforms two binary strings of length L_ϕ to a binary string of length L_ϕ

NOTE It is used iteratively as part of a hash-function, where it combines an “expanded” data block of length L_ϕ with the previous output of length L_ϕ .

3.3 Conventions

3.3.1

bit ordering

bit ordering in this part of ISO/IEC 10118 is as described in clause 3 of ISO/IEC 10118-1

3.3.2

converting a number to a string

during computation of the round-function, integers need to be converted to strings of L bits. Where this is required, the string of bits shall be made equal to the binary representation of the integer, with the left-most bit of the string corresponding to the most significant bit of the binary representation. If the resulting string of bits has less than L bits, then the string shall be left-padded with the appropriate number of zeros to make it of length L

3.3.3

converting a string to a number

during computation of the round-function, strings of bits need to be converted into integers. Where this is required, the integer shall be made equal to the number having binary representation equal to the binary string, where the left-most bit of the string is considered as the most significant bit of the binary representation

3.4

hash-function identifier

identifiers are defined for each of the two MASH hash-functions specified in this standard. The hash-function identifiers for the hash-functions specified in clause 8.1 and 8.2 are equal to 41 and 42 (hexadecimal) respectively. The range of values from 43 to 4f (hexadecimal) are reserved for future use as hash-function identifiers by this part of ISO/IEC 10118

4 Symbols and abbreviated terms

Throughout this part of ISO/IEC 10118, the following symbols and abbreviations apply.

4.1 From ISO/IEC 10118-1

D Data

H Hash-code

IV Initializing value

$X \oplus Y$ Exclusive-or of strings of bits X and Y

4.2 Unique to this part of ISO/IEC 10118

B_j The j th block derived from the data string D after the padding, splitting, and expansion process.

D_j The j th half-block derived from the data string D after the padding and the splitting process. D_{q+1} through D_{q+8} are additional data blocks computed in the reduction-function.

e The exponent used in the round-function.

E A constant block equal to four ones (in the left-most position) followed by $L_\phi - 4$ zeros.

H_j The output of the round-function in the j th round. H_j has length L_ϕ .

L_D The length of the input string D in bits.

L_ϕ The length of the output H_j of the round-function ϕ . It shall be an integer multiple of 16.

L_N The length of the modulus N used in the round-function.

L_p The length of the prime number p used in the reduction-function.

mod If Z_1 is an integer and Z_2 is a positive integer, then $Z_1 \bmod Z_2$ denotes the unique integer Z_3 which satisfies

- a) $0 \leq Z_3 < Z_2$, and
- b) $Z_1 - Z_3$ is an integer multiple of Z_2 .

N A composite integer, used as the modulus in the round-function.

NOTE For the determination of the value of N , see clause 5.

p A prime number used in the reduction-function.

NOTE For the determination of the value of p , see clause 5.

q The number of half-blocks in the data string D after the padding and splitting processes, also the number of blocks after the padding, splitting, and expansion process.

RED The reduction-function, that is applied as the last operation of the hashing procedure to reduce the block H_q of length L_ϕ to the hash-code H of length L_p .

Y_j The j th sub-string of length $L_\phi/4$ bits used in the reduction-function.

ϕ A round-function. If X and Y denote strings of L_ϕ bits, then $\phi(X, Y)$ denotes a string of L_ϕ bits obtained by applying ϕ to X and Y .

$\vee$ The bit-wise inclusive OR operation on strings of bits, i.e., if X and Y are strings of the same length, then $X \vee Y$ denotes the string obtained as the bit-wise inclusive OR of X and Y .

$\sim$ A symbol denoting the truncate operation. If X is a bitstring then $X \sim j$ denotes the bitstring obtained by taking the right-most j bits of X .

$:=$ A symbol denoting the “set equal to” operation. It is used in the procedural specification of the round-function and of the reduction-function, where it indicates that the block on the left side of the symbol shall be changed to equal the value of the expression on the right side of the symbol.

$X||Y$ Concatenation of bit-strings X and Y in the indicated order.

5 Requirements

5.1 To employ either of the hash-functions specified in this part of ISO/IEC 10118, two integers shall be selected: the modulus N used in the round-function and the prime p used in the reduction-function.

Both integers, N and p , are determined by the security requirements of the application for which these hash-functions are used.

5.1.1 The modulus N shall be chosen so that factoring it is computationally infeasible.

5.1.2 The modulus N shall be generated in a way that the factors remain secret. This can be accomplished by a trusted third party or by a secure multiparty computation.

NOTE 1 Generating a modulus N with the property that its factors remain secret can be accomplished by using a trusted third party, trusted hardware, and/or a secure multiparty computation. Examples can be found in Boneh [1], Cocks [2], and Frankel [3].

NOTE 2 If the factors of the modulus are kept secret, and if the size of the prime p is sufficiently large, then the best known algorithm to find a collision takes approximately $2^{L_p/2}$ evaluations of the round-function, and the best known algorithm to find a (2nd) pre-image requires approximately 2^{L_p} evaluations of the round-function. Thus in these circumstances MASH-1 and MASH-2 are believed to be collision-free hash-functions.

5.1.3 The reduction-function prime p shall not be a factor of the modulus N of the round-function.

5.1.4 The length L_p of the prime p shall be at most half of the length of the modulus N , $L_p \leq L_\phi/2$.

5.1.5 The three high order bits of prime p shall consist of ones.

AC1 5.1.6 The modulus N of the MASH-1 round-function shall not satisfy either of the following two conditions:

The left-most bit of N is equal to 1, and the next L_ϕ bits are equal to 0.

$L_N = L_\phi + 1$, $N \neq 31 \pmod{32}$, the 4 left-most bits of N are equal to 1, the bits of N at positions $8t_1 + t_2$, $t_1 = 0, 1, \dots, L_\phi/8$, $t_2 \in \{5, 6, 7\}$ are equal to 1, and every 5-tuple $8t_1, 8t_1 + 1, \dots, 8t_1 + 4$, $t_1 = 1, 2, \dots, L_\phi/8$ contains at least one bit equal to 1. **AC1**

5.2 To employ one of the hash-functions, MASH-1 or MASH-2, the user has to select one of the two exponents e used in the round-function ϕ .

5.3 MASH-1 and MASH-2 can be applied to all data strings D containing at most $2^{L_\phi/2} - 1$ bits.