INTERNATIONAL STANDARD

ISO/IEC 7064

First edition
2003-02-15

Information technology — Security techniques — Check character systems

Technologies de l'information — Techniques de sécurité — Systèmes de caractères de contrôle

iTeh STANDARD PREVIEW

(standards.iteh.ai)

ISO/IEC 7064:2003
https://standards.iteh.ai/catalog/standards/sist/fb0d41d8-cb12-4ad1-9da2-
6e2876f0f355/iso-iec-7064-2003

Contents

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.

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 7064 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This first edition of ISO/IEC 7064 cancels and replaces ISO 7064:1983, which has been technically revised. Note, however, that implementations which comply with ISO 7064:1983 will be compliant with ISO/IEC 7064:2003.

Introduction

The need for standardization of check character systems was determined by the following considerations:

a) of the multitude of systems in use, many have very similar characteristics, and much of the variety fails to provide any significant benefit;

b) few of the existing systems have been thoroughly verified mathematically and several have serious defects;

c) the variety of systems undermines the economics of products which generate or validate check characters, and frequently prevents the checking of interchanged data.

Therefore a small set of compatible systems were selected to cope with various application needs; they were validated, and within the constraints of each application, offer high protection against typical transcription and keying errors.

Existing check character systems as specified in ISO 2108, ISO 2894 and ISO 6166 are used in special application fields (ISO 2894 has been withdrawn). These do not however, achieve the error detection rate of the systems specified in this International Standard.

Annex A summarizes the criteria to be considered when selecting a check character system specified in this International Standard for a particular application.

Annex B provides an example of a method by which this standard may be applied to an alphabet that has more than 26 characters.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Information technology — Security techniques — Check character systems

1 Scope

1.1 This International Standard specifies a set of check character systems capable of protecting strings against errors which occur when people copy or type data. The strings may be of fixed or variable length and may have character sets which are

a) numeric (10 digits: 0 to 9);

b) alphabetic (26 letters: A to Z); and

c) alphanumeric (letters and digits).

Embedded spaces and special characters are ignored.

1.2 This International Standard specifies conformance requirements for products described as generating check characters or checking strings using the systems given in this International Standard.

1.3 These check character systems can detect:

a) all single substitution errors (the substitution of a single character for another, for example "4234" for "1234)";

b) all or nearly all single (local) transposition errors (the transposition of two single characters, either adjacent or with one character between them, for example "12354" or "12543" for "12345");

c) all or nearly all circular shift errors (circular shifts of the whole string to the left or right);

d) a high proportion of double substitution errors (two separate single substitution errors in the same string, for example "7234587" for "1234567)"; and

e) a high proportion of all other errors.

1.4 This International Standard excludes systems designed specifically to:

a) permit both error detection and automatic correction;

b) detect deliberate falsification; and

c) check strings interchanged solely between machines.

1.5 This International Standard is for use in information interchange between organizations. It is also strongly recommended for use in internal information systems.

2 Terms and definitions

For the purposes of this International Standard, the following terms and definitions apply.

2.1 check character: Added character which may be used to verify the accuracy of the string by a mathematical relationship to that string.

2.2 check character system: Set of rules for generating check characters and checking strings incorporating check characters.

2.3 supplementary check character: Check character which does not belong to the character set of the strings which are to be protected.

2.4 modulus: Integer used as a divisor of an integer dividend in order to obtain an integer remainder.

2.5 congruence: Property of a set of integers which differ from each other by a multiple of the modulus. Congruence is indicated by the symbol $\equiv$. For example, $39 \equiv 6 \pmod{11}$ indicates that 39 and 6 are congruent with respect to the modulus 11, i.e., $39 - 6 = 33$, which is a multiple of 11.

2.6 radix: Base of a geometric progression.

3 Symbols and notation

Throughout ISO/IEC 7064 the following symbols and notation are used.

a_i Numerical value of the character in position i.

i Index of the character position.

M Modulus.

n Number of characters in a string, including the check character.

P_j, S_j, V Integers which are used in the calculation of the check character to store an intermediate result.

r Radix.

w_j Weight for the polynomial method.

$\mathbf{X}$, $*$ Supplementary check characters.

$:=$ A symbol denoting the 'set equal to' operation used in the procedural specifications of check characters, which indicates that the value of the integer on the left side of the symbol shall be made equal to the value of the expression on the right side of the symbol.

$\equiv$ A symbol denoting 'congruence' (see Clause 2.5).

$\|_M$ A symbol denoting the unique integer between 1 and M that is the remainder after dividing by M; if this remainder is zero then the value M shall be substituted.

$|_{M+1}$ A symbol denoting the unique integer between 0 and M that is the remainder after dividing by $M + 1$; the remainder is never zero after this operation.

$(\bmod M)$ A symbol denoting the unique integer between 0 and $M - 1$ that is the remainder after dividing by M.

4 Types of systems

This International Standard specifies two types of systems:

a) pure systems (Clauses 6, 7 and 8) and

b) hybrid systems (Clauses 9 and 10).

4.1 Pure systems

The pure systems are listed in Table 1 and specified in Clauses 6, 7 and 8. They each use a single modulus for all stages of the calculation.

4.2 Hybrid systems

The hybrid systems are listed in Table 2 and specified in Clauses 9 and 10. The hybrid systems each use two moduli in the calculation. One modulus is equal to, and the other is one greater than, the number of characters in the character set of the string to be protected. These hybrid systems always provide a check character within the character set of the string to be protected.

5 Compliance and designation

5.1 Strings

Strings protected by one of the systems specified in this International Standard for the relevant application comply with this International Standard.

5.2 Check character generating products

5.2.1 Products (implemented either in software or hardware) that are described as generating check characters to this International Standard without further qualification shall be capable of generating check characters for all systems in this International Standard.

5.2.2 The description of products which do not generate check characters for all the systems in this International Standard shall specify those systems which they do cover, for example "generates check characters in accordance with ISO/IEC 7064, MOD 11–2".

5.3 Checking products

5.3.1 Products (implemented either in software or hardware) that are described as checking strings to this International Standard without further qualification shall be capable of using all the systems in this International Standard.

5.3.2 The description of products which check strings using only certain of the systems in this International Standard shall specify those systems which they do cover, for example "checks strings using ISO/IEC 7064, MOD 11–2".

5.4 System designation

5.4.1 Normally the full designation of each system as given in Tables 1 and 2 shall be used, for example "ISO/IEC 7064, MOD 11–2".

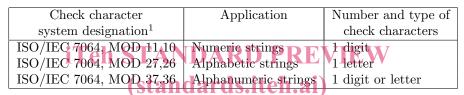> NOTE — Abbreviations to forms such as "MOD 11" will create confusion with the similar systems using modulus 11.

2

Table 1 — Pure systems

Check character system designation[1]	Application	Number and type of check characters[2]
ISO/IEC 7064, MOD 11–2	Numeric strings	1 digit or the supplementary check character "X"
ISO/IEC 7064, MOD 37–2	Alphanumeric strings	1 digit or letter or the supplementary check character "∗"
ISO/IEC 7064, MOD 97–10	Numeric strings	2 digits
ISO/IEC 7064, MOD 661–26	Alphabetic strings	2 letters
ISO/IEC 7064, MOD 1271–36	Alphanumeric strings	2 digits or letters

1 The first number following "MOD" in the designation is the modulus and the second number is the radix.

2 The first two systems may produce a supplementary check character outside the character set of the string to be checked (i.e., ISO/IEC 7064, MOD 11-2 check characters are "0" to "9" plus "X", and ISO/IEC 7064, MOD 37–2 check characters are "0" to "9", and "A" to "Z", plus "∗"). Where the supplementary check character is not acceptable and a single check character is required, it may be possible to avoid issuing those strings which yield the supplementary check character. If neither the supplementary check character can be tolerated nor can the strings yielding it be avoided, then the hybrid systems may be used instead.

Table 2 — Hybrid systems

Check character system designation[1]	Application	Number and type of check characters
ISO/IEC 7064, MOD 11,10	Numeric strings	1 digit
ISO/IEC 7064, MOD 27,26	Alphabetic strings	1 letter
ISO/IEC 7064, MOD 37,36	Alphanumeric strings	1 digit or letter

1 The two numbers following "MOD" in the designation are the two moduli.

5.4.2 Where there is a special need for brevity, for example when it is necessary to accompany a transmitted data element by an indication of the system used to protect it, the single digit designations indicated in Table 3 may be used.

Table 3 — Single digit designations

Check character system	Designation
ISO/IEC 7064, MOD 11–2	1
ISO/IEC 7064, MOD 37–2	2
ISO/IEC 7064, MOD 97–10	3
ISO/IEC 7064, MOD 661–26	4
ISO/IEC 7064, MOD 1271–36	5
ISO/IEC 7064, MOD 11,10	6
ISO/IEC 7064, MOD 27,26	7
ISO/IEC 7064, MOD 37,36	8
No check character or non-standard system	0

6 Specification of pure systems

6.1 Formula

A character string satisfies the check when:

$$\sum_{i=1}^{n} a_i \cdot r^{i-1} \equiv 1 \ (\mathrm{mod}\, M),$$

where

n is the number of characters in the string, including check character(s);

i is the index of the character position starting from the right (i.e., for the rightmost character, $i = 1$), disregarding spaces and special characters;

a_i is the value of the character in position i as defined in Table 4;

r is the radix (i.e., the basis for the geometric progression); and

M is the modulus.

6.2 Calculation

Any calculation procedure which satisfies the formula may be used.

6.3 Check character position

The check character(s) shall be placed at the right-most end of the string.

7 Computational methods for pure systems with one check character

Two basic computational methods for the pure systems are defined in this International Standard. These are the *pure system recursive method* and the *pure system polynomial method.* Both yield the same result and require the same number of multiplications and additions. The polynomial method requires more memory, as the system weights need to be stored.

7.1 Pure system recursive method

7.1.1 Computation

In the recursive method the string is processed character by character from left to right.

The algorithm for generating the check character a_1 can be described as follows. With the index $j = 1 \ldots (n-1)$, where n is the number of characters in the string including the check character, and defining $P_j = 0$ for $j = 1$, calculate:

$$
\begin{aligned}
S_j &:= P_j + a_{n-j+1} \\
P_{j+1} &:= S_j \cdot r\,,
\end{aligned}
$$

where

a_{n-j+1} is the character value;

r is the radix.

Next a_1 shall be chosen so that

$$P_n + a_1 \equiv 1 \ (\mathrm{mod}\, M)$$

or

$$a_1 := (1 - P_n) \ (\mathrm{mod}\, M)\,.$$

The algorithm for verifying the check character a_1 can be described as follows. With the index $j = 1 \ldots n$, where n is the number of characters in the string including the check character, and defining $P_j = 0$ for $j = 1$, calculate:

$$
\begin{aligned}
S_j &:= P_j + a_{n-j+1} \\
P_{j+1} &:= S_j \cdot r\,,
\end{aligned}
$$

Table 4 — Values assigned to characters

Character	Value in systems for numeric strings	Value in systems for alphabetic strings	Value in systems for alpha-numeric strings
0	0		0
1	1		1
2	2		2
3	3		3
4	4		4
5	5		5
6	6		6
7	7		7
8	8		8
9	9		9
X[1]	10		
A		0	10
B		1	11
C		2	12
D		3	13
E		4	14
F		5	15
G		6	16
H		7	17
I		8	18
J		9	19
K		10	20
L		11	21
M		12	22
N		13	23
O		14	24
P		15	25
Q		16	26
R		17	27
S		18	28
T		19	29
U		20	30
V		21	31
W		22	32
X		23	33
Y		24	34
Z		25	35
*[2]			36

1 for ISO/IEC 7064 MOD 11–2.

2 for ISO/IEC 7064 MOD 37–2.

The string is assumed to be correct if

$$S_n \equiv 1 \;(\mathrm{mod}\, M).$$

Alternatively, the procedure for generating the check character a_1 can be repeated. This string is assumed to be correct if the generated check character corresponds to the existing character a_1.

7.1.2 Example

Assume that the string "0794" is to be provided with a check character using the check character system ISO/IEC 7064, MOD 11–2.

Here $M = 11$, $r = 2$ and $n = 5$ (i.e., 4 characters plus 1 check character).

The calculation may then be as set out in Table 5.

In this example, the final product P_n is equal to 100. This value plus the check character is to be congruent to $1\,(\mathrm{mod}\,11)$. As 100 is itself congruent to $1\,(\mathrm{mod}\,11)$, the check character value must be zero, and the full protected string is "07940", as the check character is appended to the right of the string.

To check the string, the steps $j = 1$ to 5 above are computed as shown, but with the check character value, 0, being included in the calculation; if the result is congruent to $1\,(\mathrm{mod}\,11)$, the string is accepted as valid.

NOTES

1 If at any stage the product P_{j+1} or the sum S_j is greater than the modulus M, multiples of the modulus may be discarded and the integer remainder be used for further calculations. In the calculations in Table 5:

$$
\begin{aligned}
P_3 &= 14 \quad \text{but could be} \quad 14 - 11 = 3 \\
S_3 &= 23 \quad \text{but could be} \quad 23 - 22 = 1 \\
P_4 &= 46 \quad \text{but could be} \quad 46 - 44 = 2
\end{aligned}
$$

2 The valid check character values in the system ISO/IEC 7064, MOD11-2 are 0 to 10. If the value of the check character is 10, it is represented by the supplementary check character "X". If the original string had been the shorter string "079", then at the end of step 3 the value is 46:

$$46 \equiv 2 \;(\mathrm{mod}\,11);$$

as $2 + 10 \equiv 1 \;(\mathrm{mod}\,11)$ the complete string is "079X".

To verify the string after step 3 we would have $46 + 10 = 56$, which is congruent to $1\,(\mathrm{mod}\,11)$, thus satisfying the check.

7.2 Pure system polynomial method

7.2.1 Computation

The polynomial method for the pure systems is computed by multiplying the value for each character in the string by r^{i-1} or by $r^{i-1} \;(\mathrm{mod}\, M)$, which is denoted by the weight w_i. A list of the first fifteen values of $r^{i-1} \;(\mathrm{mod}\, M)$ for all the pure systems is given in Table 6.

Multiply the character values by their weights, and then add the products. Strings including the check character are valid if the sum of these products is congruent to $1\,(\mathrm{mod}\, M)$.

7.2.2 Example

The computation to generate the check character by the polynomial method for the same string used in the example of Clause 7.1.2, i.e., "0794", is:

Character position i:	5	4	3	2	1
Weight $2^{i-1} \;(\mathrm{mod}\,11)$:	5	8	4	2	1
Character value a_i:	0	7	9	4	
Products:	0	56	36	8	
Sum of products:		$0{+}56{+}36{+}8$			$= 100$

The sum, which in this case is 100, plus the check character must be congruent to $1\,(\mathrm{mod}\,11)$. As 100 itself is congruent to $1\,(\mathrm{mod}\,11)$, the check character value must be zero, and the full protected string is "07940". Note that the check character is appended to the right of the string.

To check the string with this method, multiply each character value (including the check character value) by the weight associated with its position; sum the products and divide by 11 to get the remainder. If the remainder equals 1 the check is satisfied. The computation to check the full protected string is:

Character position i:	5	4	3	2	1
Weight $2^{i-1} \;(\mathrm{mod}\,11)$:	5	8	4	2	1
Character value a_i:	0	7	9	4	0
Products:	0	56	36	8	0
Sum of products:		$0{+}56{+}36{+}8{+}0$			$= 100$
					$\equiv 1 \;(\mathrm{mod}\,11)$

thus satisfying the check.

NOTE — The rightmost position, i.e., the position with the weight $r^0 = 1$, is reserved for the check character, so the rightmost position of the original string (*without* the check character) is associated with a weight of r, here 2.