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

Reference number
ISO/IEC 7064:2003(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

1 Scope 1

2 Terms and definitions 1

3 Symbols and notation 2

4 Types of systems 2
4.1 Pure systems . . . 2
4.2 Hybrid systems . . . 2

5 Compliance and designation 2
5.1 Strings . . . 2
5.2 Check character generating products . . . 2
5.3 Checking products . . . 2
5.4 System designation . . . 2

6 Specification of pure systems 3
6.1 Formula . . . 3
6.2 Calculation . . . 4
6.3 Check character position . . . 4

7 Computational methods for pure systems with one check character 4
7.1 Pure system recursive method . . . 4
7.1.1 Computation . . . 4
7.1.2 Example . . . 5
7.2 Pure system polynomial method . . . 5
7.2.1 Computation . . . 5
7.2.2 Example . . . 5

8 Computational methods for pure systems with two check characters 6
8.1 Computation . . . 6
8.2 Example using recursive method . . . 6
8.3 Example using polynomial method . . . 7
8.4 Simplified procedure for ISO/IEC 7064, MOD 97–10 . . . 7

9 Specification for hybrid systems 7
9.1 Formula . . . 7
9.2 Check character position . . . 8

10 Computational method for hybrid systems 8
10.1 Hybrid system recursive method . . . 8
10.1.1 Computation . . . 8
10.1.2 Example . . . 8

Annex A (informative) **Criteria for the selection of check character systems for applications** . . . 10

Annex B (informative) **Check character systems for other alphabets** . . . 12

Bibliography . . . 13

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.

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.

