

Information technology — Security techniques — Check character systems

ICS 35.040

National foreword

This British Standard reproduces verbatim ISO/IEC 7064:2003 and implements it as the UK national standard. It supersedes BS 6541:1985 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33, Security techniques, which has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible international/European committee any enquiries on the interpretation, or proposals for change, and keep the UK interests informed;
- monitor related international and European developments and promulgate them in the UK.

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

Cross-references

The British Standards which implement international publications referred to in this document may be found in the *BSI Catalogue* under the section entitled “International Standards Correspondence Index”, or by using the “Search” facility of the *BSI Electronic Catalogue* or of British Standards Online.

This 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 does not of itself confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 21 March 2003

Summary of pages

This document comprises a front cover, an inside front cover, the ISO/IEC title page, pages ii to v, a blank page, pages 1 to 13 and a back cover.

The BSI copyright date displayed in this document indicates when the document was last issued.

Amendments issued since publication

Amd. No.	Date	Comments

© BSI 21 March 2003

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*



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.