

Recommendations for

Algorithms for use in banking message authentication —

Part 1: Data Encryption Algorithm
(DEA)

UDC 336.717.131.3:654.073.4:681.3.04:519.688:65.012.8

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

BSI
Documents



Document Sharing Hub

Committees responsible for this British Standard

The preparation of this British Standard was entrusted by the Information Systems Technology Standards Policy Committee (IST/-) to Technical Committee IST/12, upon which the following bodies were represented:

- American Banks Association of London (ABAL)
- Association for Payment Clearing Services
- British Computer Society
- Building Societies Association
- Electronic Components Industry Federation
- Institute of Data Processing Management
- Stock Exchange

This British Standard, having been prepared under the direction of the Information Systems Technology Standards Policy Committee, was published under the authority of the Board of BSI and comes into effect on 31 October 1989

© BSI 11-1999

The following BSI references relate to the work on this standard:
Committee reference IST/12
Draft for comment 85/65694 DC

ISBN 0 580 17611 8

Amendments issued since publication

Amd. No.	Date of issue	Comments

Contents

	Page
Committees responsible	Inside front cover
National foreword	ii
0 Introduction	1
1 Scope and field of application	1
2 References	1
3 Source of algorithm DEA	1
4 Specification of algorithm	1
Figure — Authentication algorithm	2
Publications referred to	Inside back cover