

INTERNATIONAL STANDARD

ISO
11166-2

First edition
1994-11-15

ANSI Internat Doc Sec

Banking — Key management by means of asymmetric algorithms —

Part 2:

Approved algorithms using the RSA
cryptosystem

*Banque — Gestion des clés au moyen d'algorithmes asymétriques —
Partie 2: Algorithmes approuvés utilisant le système de chiffrement RSA*



Reference number
ISO 11166-2 1994(E)

Contents

	Page
Introduction	i v
1 Scope.....	1
2 Normative references	1
3 Definitions and notation.....	1
4 Symbols and abbreviations.....	1
5 RSA key generation.....	2
6 RSA encipherment and decipherment.....	2
7 Modes of operation for RSA signature.....	2
8 Application of algorithms	4
Annexes	
A Assigned values of Function and Format Code (FFC).....	7
B Choice of primes.....	10
C Bibliography.....	12

© ISO 1994

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

International Organization for Standardization
Case Postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland