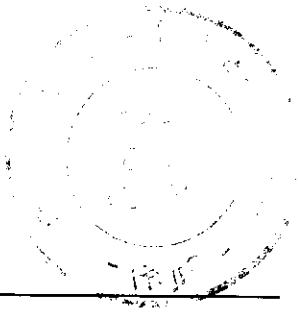
Man Young Rhee

Internet Security

Cryptographic principles, algorithms and protocols

WILEY

Internet Security



Internet Security

Cryptographic Principles, Algorithms and Protocols

Man Young Rhee

School of Electrical and Computer Engineering

Seoul National University, Republic of Korea

WILEY

John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester,
West Sussex PO19 8SQ, England

Telephone (+44) 1243 779777

Email (for orders and customer service enquiries): cs-books@wiley.co.uk
Visit our Home Page on www.wileyeurope.com or www.wiley.com

Reprinted July 2003

Other Wiley Editorial Offices

John Wiley & Sons Inc., 111 River Street, Hoboken, NJ 07030, USA

Jossey-Bass, 989 Market Street, San Francisco, CA 94103-1741, USA

Wiley-VCH Verlag GmbH, Boschstr. 12, D-69469 Weinheim, Germany

John Wiley & Sons Australia Ltd, 33 Park Road, Milton, Queensland 4064, Australia

John Wiley & Sons (Asia) Pte Ltd, 2 Clementi Loop #02-01, Jin Xing Distripark, Singapore 129809

John Wiley & Sons Canada Ltd, 22 Worcester Road, Etobicoke, Ontario, Canada M9W 1L1

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

Library of Congress Cataloging-in-Publication Data

Rhee, Man Young.
Internet security : cryptographic principles, algorithms, and protocols / Man Young Rhee.
p. cm.
Includes bibliographical references and index.
ISBN 0-470-85285-2 (alk. paper)
1. Internet – Security measures. 2. Data encryption (Computer Science) 3. Public key cryptography.
I. Title.

TK5105.875.I57 .R447 2003-02-05
005'8.2 – dc21

2002191050

British Library Cataloguing in Publication Data

A catalogue record for this book is available from the British Library

ISBN 0-470-85285-2

Typeset in 10/12pt Times by Laserwords Private Limited, Chennai, India
Printed and bound in Great Britain by Antony Rowe Ltd, Chippenham, Wiltshire
This book is printed on acid-free paper responsibly manufactured from sustainable forestry in which at least two trees are planted for each one used for paper production.

Contents