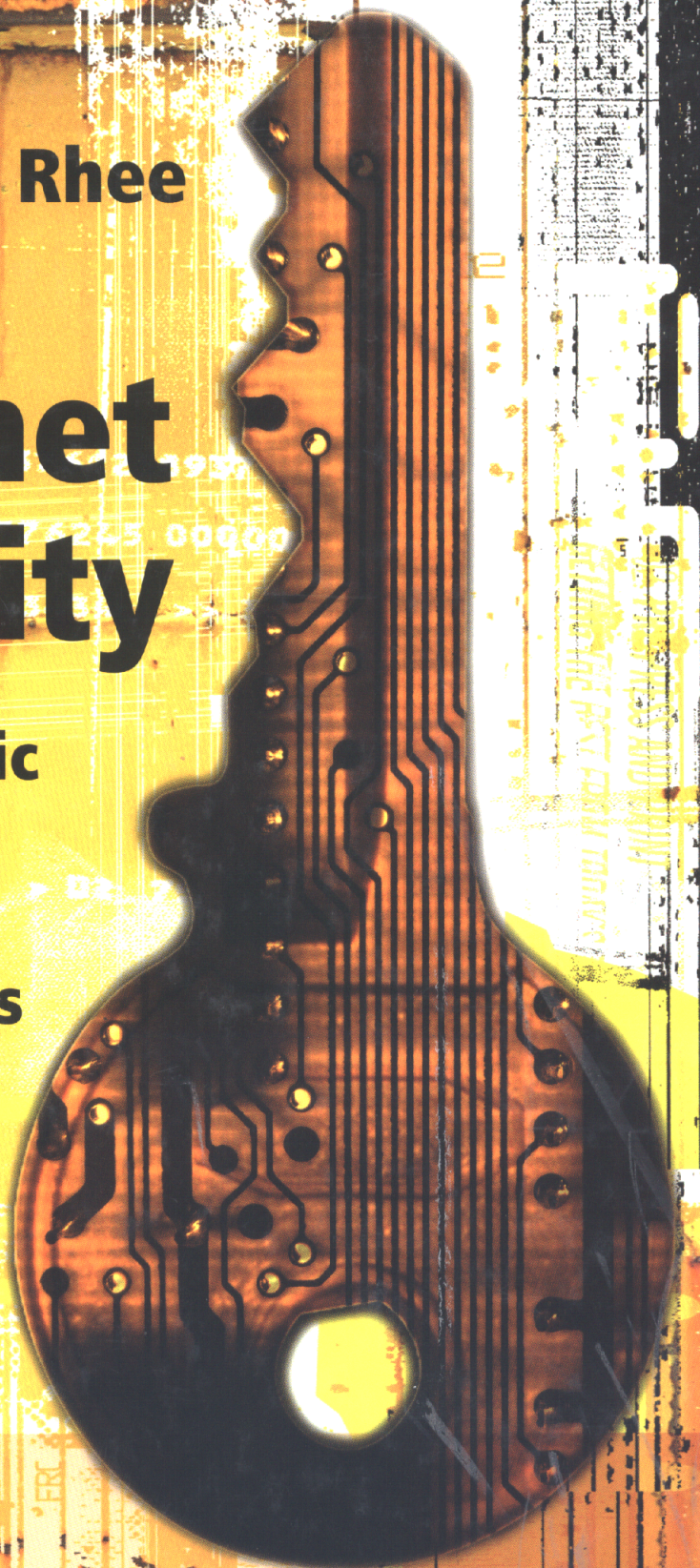


**Man Young Rhee**

# **Internet Security**

**Cryptographic  
principles,  
algorithms  
and protocols**

 **WILEY**





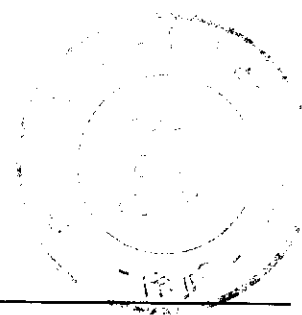
BIBLIOTHEQUE DU CERIST

---

# Internet Security

---

BIBLIOTHEQUE DU CERIST



---

# Internet Security

Cryptographic Principles, Algorithms  
and Protocols

---

**Man Young Rhee**

*School of Electrical and Computer Engineering  
Seoul National University, Republic of Korea*

BIBLIOTHEQUE DU CERIST



WILEY

Copyright © 2003

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](mailto:cs-books@wiley.co.uk)

Visit our Home Page on [www.wiley-europe.com](http://www.wiley-europe.com) or [www.wiley.com](http://www.wiley.com)

Reprinted July 2003

All Rights Reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except under the terms of the Copyright, Designs and Patents Act 1988 or under the terms of a licence issued by the Copyright Licensing Agency Ltd, 90 Tottenham Court Road, London W1T 4LP, UK, without the permission in writing of the Publisher. Requests to the Publisher should be addressed to the Permissions Department, John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England, or emailed to [permreq@wiley.co.uk](mailto:permreq@wiley.co.uk), or faxed to (+44) 1243 770620.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold on the understanding that the Publisher is not engaged in rendering professional services. If professional advice or other expert assistance is required, the services of a competent professional should be sought.

#### *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

#### *British Library Cataloguing in Publication Data*

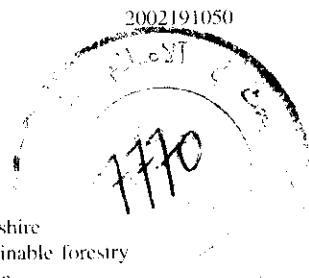
A catalogue record for this book is available from the British Library

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

<b>Author biography</b>	<b>xi</b>
<b>Preface</b>	<b>xiii</b>
<b>1 Internetworking and Layered Models</b>	<b>1</b>
1.1 Networking Technology	2
1.1.1 Local Area Networks (LANs)	2
1.1.2 Wide Area Networks (WANs)	3
1.2 Connecting Devices	5
1.2.1 Switches	5
1.2.2 Repeaters	6
1.2.3 Bridges	6
1.2.4 Routers	7
1.2.5 Gateways	8
1.3 The OSI Model	8
1.4 TCP/IP Model	12
1.4.1 Network Access Layer	13
1.4.2 Internet Layer	13
1.4.3 Transport Layer	13
1.4.4 Application Layer	13
<b>2 TCP/IP Suite and Internet Stack Protocols</b>	<b>15</b>
2.1 Network Layer Protocols	15
2.1.1 Internet Protocol (IP)	15
2.1.2 Address Resolution Protocol (ARP)	28
2.1.3 Reverse Address Resolution Protocol (RARP)	31
2.1.4 Classless Interdomain Routing (CIDR)	32
2.1.5 IP Version 6 (IPv6, or IPng)	33
2.1.6 Internet Control Message Protocol (ICMP)	41
2.1.7 Internet Group Management Protocol (IGMP)	41
2.2 Transport Layer Protocols	42
2.2.1 Transmission Control Protocol (TCP)	42
2.2.2 User Datagram Protocol (UDP)	45



2.3	World Wide Web	47
2.3.1	Hypertext Transfer Protocol (HTTP)	48
2.3.2	Hypertext Markup Language (HTML)	48
2.3.3	Common Gateway Interface (CGI)	49
2.3.4	Java	49
2.4	File Transfer	50
2.4.1	File Transfer Protocol (FTP)	50
2.4.2	Trivial File Transfer Protocol (TFTP)	50
2.4.3	Network File System (NFS)	50
2.5	Electronic Mail	51
2.5.1	Simple Mail Transfer Protocol (SMTP)	51
2.5.2	Post Office Protocol Version 3 (POP3)	52
2.5.3	Internet Message Access Protocol (IMAP)	52
2.5.4	Multipurpose Internet Mail Extension (MIME)	52
2.6	Network Management Service	53
2.6.1	Simple Network Management Protocol (SNMP)	53
2.7	Converting IP Addresses	54
2.7.1	Domain Name System (DNS)	54
2.8	Routing Protocols	54
2.8.1	Routing Information Protocol (RIP)	54
2.8.2	Open Shortest Path First (OSPF)	55
2.8.3	Border Gateway Protocol (BGP)	55
2.9	Remote System Programs	56
2.9.1	TELNET	56
2.9.2	Remote Login (Rlogin)	56
<b>3</b>	<b>Symmetric Block Ciphers</b>	<b>57</b>
3.1	Data Encryption Standard (DES)	57
3.1.1	Description of the Algorithm	58
3.1.2	Key Schedule	60
3.1.3	DES Encryption	62
3.1.4	DES Decryption	67
3.1.5	Triple DES	71
3.1.6	DES-CBC Cipher Algorithm with IV	73
3.2	International Data Encryption Algorithm (IDEA)	75
3.2.1	Subkey Generation and Assignment	76
3.2.2	IDEA Encryption	77
3.2.3	IDEA Decryption	82
3.3	RC5 Algorithm	84
3.3.1	Description of RC5	85
3.3.2	Key Expansion	86
3.3.3	Encryption	91
3.3.4	Decryption	92
3.4	RC6 Algorithm	95
3.4.1	Description of RC6	95

3.4.2	Key Schedule	96
3.4.3	Encryption	97
3.4.4	Decryption	100
3.5	AES (Rijndael) Algorithm	107
3.5.1	Notational Conventions	107
3.5.2	Mathematical Operations	108
3.5.3	AES Algorithm Specification	111
<b>4</b>	<b>Hash Function, Message Digest and Message Authentication Code</b>	<b>123</b>
4.1	DMDC Algorithm	123
4.1.1	Key Schedule	124
4.1.2	Computation of Message Digests	128
4.2	Advanced DMDC Algorithm	133
4.2.1	Key Schedule	133
4.2.2	Computation of Message Digests	136
4.3	MD5 Message-digest Algorithm	138
4.3.1	Append Padding Bits	138
4.3.2	Append Length	138
4.3.3	Initialise MD Buffer	138
4.3.4	Define Four Auxiliary Functions (F, G, H, I)	139
4.3.5	FF, GG, HH and II Transformations for Rounds 1, 2, 3 and 4	139
4.3.6	Computation of Four Rounds (64 Steps)	140
4.4	Secure Hash Algorithm (SHA-1)	149
4.4.1	Message Padding	149
4.4.2	Initialise 160-Bit Buffer	150
4.4.3	Functions Used	150
4.4.4	Constants Used	150
4.4.5	Computing the Message Digest	151
4.5	Hashed Message Authentication Codes (HMAC)	155
<b>5</b>	<b>Asymmetric Public-key Cryptosystems</b>	<b>161</b>
5.1	Diffie–Hellman Exponential Key Exchange	161
5.2	RSA Public-key Cryptosystem	165
5.2.1	RSA Encryption Algorithm	165
5.2.2	RSA Signature Scheme	170
5.3	ElGamals Public-key Cryptosystem	172
5.3.1	ElGamal Encryption	173
5.3.2	ElGamal Signatures	175
5.3.3	ElGamal Authentication Scheme	177
5.4	Schnorr’s Public-key Cryptosystem	179
5.4.1	Schnorr’s Authentication Algorithm	179
5.4.2	Schnorr’s Signature Algorithm	181
5.5	Digital Signature Algorithm	184

5.6	The Elliptic Curve Cryptosystem (ECC)	187
5.6.1	Elliptic Curves	187
5.6.2	Elliptic Curve Cryptosystem Applied to the ElGamal Algorithm	195
5.6.3	Elliptic Curve Digital Signature Algorithm	196
5.6.4	ECDSA Signature Computation	198
<b>6</b>	<b>Public-key Infrastructure</b>	<b>201</b>
6.1	Internet Publications for Standards	202
6.2	Digital Signing Techniques	203
6.3	Functional Roles of PKI Entities	210
6.3.1	Policy Approval Authority	210
6.3.2	Policy Certification Authority	212
6.3.3	Certification Authority	213
6.3.4	Organisational Registration Authority	214
6.4	Key Elements for PKI Operations	215
6.4.1	Hierarchical Tree Structures	216
6.4.2	Policy-making Authority	217
6.4.3	Cross-certification	218
6.4.4	X.500 Distinguished Naming	221
6.4.5	Secure Key Generation and Distribution	222
6.5	X.509 Certificate Formats	222
6.5.1	X.509 v1 Certificate Format	223
6.5.2	X.509 v2 Certificate Format	225
6.5.3	X.509 v3 Certificate Format	226
6.6	Certificate Revocation List	233
6.6.1	CRL Fields	234
6.6.2	CRL Extensions	235
6.6.3	CRL Entry Extensions	237
6.7	Certification Path Validation	238
6.7.1	Basic Path Validation	239
6.7.2	Extending Path Validation	240
<b>7</b>	<b>Network Layer Security</b>	<b>243</b>
7.1	IPsec Protocol	243
7.1.1	IPsec Protocol Documents	244
7.1.2	Security Associations (SAs)	246
7.1.3	Hashed Message Authentication Code (HMAC)	248
7.2	IP Authentication Header	250
7.2.1	AH Format	251
7.2.2	AH Location	253
7.3	IP ESP	253
7.3.1	ESP Packet Format	254
7.3.2	ESP Header Location	256
7.3.3	Encryption and Authentication Algorithms	258

7.4	Key Management Protocol for IPsec	260
7.4.1	OAKLEY Key Determination Protocol	260
7.4.2	ISAKMP	261
<b>8</b>	<b>Transport Layer Security: SSLv3 and TLSv1</b>	<b>277</b>
8.1	SSL Protocol	277
8.1.1	Session and Connection States	278
8.1.2	SSL Record Protocol	279
8.1.3	SSL Change Cipher Spec Protocol	282
8.1.4	SSL Alert Protocol	283
8.1.5	SSL Handshake Protocol	284
8.2	Cryptographic Computations	290
8.2.1	Computing the Master Secret	290
8.2.2	Converting the Master Secret into Cryptographic Parameters	291
8.3	TLS Protocol	293
8.3.1	HMAC Algorithm	293
8.3.2	Pseudo-random Function	296
8.3.3	Error Alerts	300
8.3.4	Certificate Verify Message	302
8.3.5	Finished Message	302
8.3.6	Cryptographic Computations (For TLS)	302
<b>9</b>	<b>Electronic Mail Security: PGP, S/MIME</b>	<b>305</b>
9.1	PGP	305
9.1.1	Confidentiality via Encryption	306
9.1.2	Authentication via Digital Signature	307
9.1.3	Compression	308
9.1.4	Radix-64 Conversion	309
9.1.5	Packet Headers	313
9.1.6	PGP Packet Structure	315
9.1.7	Key Material Packet	319
9.1.8	Algorithms for PGP 5.x	323
9.2	S/MIME	324
9.2.1	MIME	325
9.2.2	S/MIME	331
9.2.3	Enhanced Security Services for S/MIME	335
<b>10</b>	<b>Internet Firewalls for Trusted Systems</b>	<b>339</b>
10.1	Role of Firewalls	339
10.2	Firewall-Related Terminology	340
10.2.1	Bastion Host	341
10.2.2	Proxy Server	341
10.2.3	SOCKS	342
10.2.4	Choke Point	343

10.2.5	De-militarised Zone (DMZ)	343
10.2.6	Logging and Alarms	343
10.2.7	VPN	344
10.3	Types of Firewalls	344
10.3.1	Packet Filters	344
10.3.2	Circuit-level Gateways	349
10.3.3	Application-level Gateways	349
10.4	Firewall Designs	350
10.4.1	Screened Host Firewall (Single-homed Bastion Host)	351
10.4.2	Screened Host Firewall (Dual-homed Bastion Host)	351
10.4.3	Screened Subnet Firewall	352
<b>11</b>	<b>SET for E-commerce Transactions</b>	<b>355</b>
11.1	Business Requirements for SET	355
11.2	SET System Participants	357
11.3	Cryptographic Operation Principles	358
11.4	Dual Signature and Signature Verification	359
11.5	Authentication and Message Integrity	363
11.6	Payment Processing	366
11.6.1	Cardholder Registration	366
11.6.2	Merchant Registration	371
11.6.3	Purchase Request	373
11.6.4	Payment Authorisation	374
11.6.5	Payment Capture	376
	<b>Acronyms</b>	<b>379</b>
	<b>Bibliography</b>	<b>383</b>
	<b>Index</b>	<b>391</b>