

PRACTICAL CRYPTOGRAPHY

Algorithms and Implementations Using C++

OTHER INFORMATION SECURITY BOOKS FROM AUERBACH

Anonymous Communication Networks:

Protecting Privacy on the Web

Kun Peng

ISBN 978-1-4398-8157-6

Conducting Network Penetration and Espionage in a Global Environment

Bruce Middleton

ISBN 978-1-4822-0647-0

Cyberspace and Cybersecurity

George Kostopoulos

ISBN 978-1-4665-0133-1

Developing and Securing the Cloud

Bhavani Thuraisingham

ISBN 978-1-4398-6291-9

Ethical Hacking and Penetration

Testing Guide

Rafay Baloch

ISBN 978-1-4822-3161-8

Guide to the De-Identification of

Personal Health Information

Khaled El Emam

ISBN 978-1-4665-7906-4

Industrial Espionage: Developing a

Counterespionage Program

Daniel J. Benny

ISBN 978-1-4665-6814-3

Information Security Fundamentals,

Second Edition

Thomas R. Peltier

ISBN 978-1-4398-1062-0

Information Security Policy Development for

Compliance: ISO/IEC 27001, NIST SP 800-53, HIPAA Standard, PCI DSS V2.0, and AUP V5.0

Barry L. Williams

ISBN 978-1-4665-8058-9

Investigating Computer-Related Crime,

Second Edition

Peter Stephenson and Keith Gilbert

ISBN 978-0-8493-1973-0

Managing Risk and Security in Outsourcing

IT Services: Onshore, Offshore and the Cloud

Frank Siepmann

ISBN 978-1-4398-7909-2

PRAGMATIC Security Metrics: Applying

Metametrics to Information Security

W. Krag Brotby and Gary Hinson

ISBN 978-1-4398-8152-1

Responsive Security: Be Ready to Be Secure

Meng-Chow Kang

ISBN 978-1-4665-8430-3

Securing Cloud and Mobility:

A Practitioner's Guide

Ian Lim, E. Coleen Coolidge, Paul Hourani

ISBN 978-1-4398-5055-8

Security and Privacy in Smart Grids

Edited by Yang Xiao

ISBN 978-1-4398-7783-8

Security for Service Oriented Architectures

Walter Williams

ISBN 978-1-4665-8402-0

Security without Obscurity:

A Guide to Confidentiality, Authentication, and Integrity

J.J. Stapleton

ISBN 978-1-4665-9214-8

The Complete Book of Data Anonymization:

From Planning to Implementation

Balaji Raghunathan

ISBN 978-1-4398-7730-2

The Frugal CISO: Using Innovation and

Smart Approaches to Maximize

Your Security Posture

Kerry Ann Anderson

ISBN 978-1-4822-2007-0

The Practical Guide to HIPAA Privacy and

Security Compliance, Second Edition

Rebecca Herold and Kevin Beaver

ISBN 978-1-4398-5558-4

Secure Data Provenance and Inference

Control with Semantic Web

Bhavani Thuraisingham, Tyrone Cadenhead,

Murat Kantarcioglu, and Vaibhav Khadilkar

ISBN 978-1-4665-6943-0

Secure Development for Mobile Apps:

How to Design and Code Secure Mobile

Applications with PHP and JavaScript

J. D. Glaser

ISBN 978-1-4822-0903-7

AUERBACH PUBLICATIONS

www.auerbach-publications.com • To Order Call: 1-800-272-7737 • E-mail: orders@crcpress.com

PRACTICAL CRYPTOGRAPHY

Algorithms and Implementations Using C++

Edited by
Saiful Azad
Al-Sakib Khan Pathan



CRC Press

Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
AN AUERBACH BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

© 2015 by Taylor & Francis Group, LLC
CRC Press is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works
Version Date: 20140930

International Standard Book Number-13: 978-1-4822-2890-8 (eBook - PDF)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access www.copyright.com (<http://www.copyright.com/>) or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Visit the Taylor & Francis Web site at
<http://www.taylorandfrancis.com>

and the CRC Press Web site at
<http://www.crcpress.com>

To the Almighty Allah, who has given us the capability to
share our knowledge with other knowledge seekers.

—**The Editors**

Contents

PREFACE	ix
ACKNOWLEDGMENTS	xi
ABOUT THE EDITORS	xiii
CONTRIBUTORS	xvii
CHAPTER 1 BASICS OF SECURITY AND CRYPTOGRAPHY	1
AL-SAKIB KHAN PATHAN	
CHAPTER 2 CLASSICAL CRYPTOGRAPHIC ALGORITHMS	11
SHEIKH SHAUGAT ABDULLAH AND SAIFUL AZAD	
CHAPTER 3 ROTOR MACHINE	35
SHEIKH SHAUGAT ABDULLAH AND SAIFUL AZAD	
CHAPTER 4 BLOCK CIPHER	45
TANVEER AHMED, MOHAMMAD ABUL KASHEM, AND SAIFUL AZAD	
CHAPTER 5 DATA ENCRYPTION STANDARD	57
EZAZUL ISLAM AND SAIFUL AZAD	
CHAPTER 6 ADVANCED ENCRYPTION STANDARD	91
ASIF UR RAHMAN, SAEF ULLAH MIAH, AND SAIFUL AZAD	

VIII**CONTENTS**

CHAPTER 7	ASYMMETRIC KEY ALGORITHMS	127
	NASRIN SULTANA AND SAIFUL AZAD	
CHAPTER 8	THE RSA ALGORITHM	135
	SAAD ANDALIB AND SAIFUL AZAD	
CHAPTER 9	ELLIPTIC CURVE CRYPTOGRAPHY	147
	HAFIZUR RAHMAN AND SAIFUL AZAD	
CHAPTER 10	MESSAGE DIGEST ALGORITHM 5	183
	BAYZID ASHIK HOSSAIN	
CHAPTER 11	SECURE HASH ALGORITHM	207
	SADDAM HOSSAIN MUKTA AND SAIFUL AZAD	
CHAPTER 12	FUNDAMENTALS OF IDENTITY-BASED CRYPTOGRAPHY	225
	AYMEN BOUDGUIGA, MARYLINE LAURENT, AND MOHAMED HAMDI	
CHAPTER 13	SYMMETRIC KEY ENCRYPTION ACCELERATION ON HETEROGENEOUS MANY-CORE ARCHITECTURES	251
	GIOVANNI AGOSTA, ALESSANDRO BARENGHI, GERARDO PELOSI, AND MICHELE SCANDALE	
CHAPTER 14	METHODS AND ALGORITHMS FOR FAST HASHING IN DATA STREAMING	299
	MARAT ZHANIKEEV	

Preface

Many books are available on the subject of cryptography. Most of these books focus on only the theoretical aspects of cryptography. Some books that include cryptographic algorithms with practical programming codes are by this time (i.e., at the preparation of this book) outdated. Though cryptography is a classical subject in which often “old is gold,” many new techniques and algorithms have been developed in recent years. These are the main points that motivated us to write and edit this book.

In fact, as students for life, we are constantly learning new needs in our fields of interest. When we were formally enrolled university students completing our undergraduate and postgraduate studies, we felt the need for a book that would not only provide details of the theories and concepts of cryptography, but also provide executable programming codes that the students would be able to try using their own computers. It took us a long time to commit to prepare such a book with both theory and practical codes.

Though some chapters of this book have been contributed by different authors from different countries, we, the editors, have also made our personal contributions in many parts. The content is a balanced mixture of the foundations of cryptography and its practical implementation with the programming language C++.

What This Book Is For

The main objective of this book is not only to describe state-of-the-art cryptographic algorithms (alongside classic schemes), but also to demonstrate how they can be implemented using a programming language, i.e., C++. As noted before, books that discuss cryptographic algorithms do not elaborate on implementation issues. Therefore, a gap between the understanding and the implementation remains unattained to a large extent. The motivation for this book is to bridge that gap and to cater to readers in such a way that they will be capable of developing and implementing their own designed cryptographic algorithm.

What This Book Is Not For

The book is not an encyclopedia-like resource. It is not for those who are completely outside the related fields, for example, readers with backgrounds in arts, business, economics, or other such areas. It may not contain the meanings and details of each technical term mentioned. While many of the technical matters have been detailed for easy understanding, some knowledge about computers, networking, programming, and aspects of computer security may be required. Familiarity with these basic topics will allow the reader to understand most of the materials.

Target Audience

This book is prepared especially for undergraduate or postgraduate students. It can be utilized as a reference book to teach courses such as cryptography, network security, and other security-related courses. It can also help professionals and researchers working in the field of computers and network security. Moreover, the book includes some chapters written in tutorial style so that general readers will be able to easily grasp some of the ideas in relevant areas. Additional material is available from the CRC Press website: <http://www.crcpress.com/product/isbn/9781482228892>.

We hope that this book will be significantly beneficial for the readers. Any criticism, comments, suggestions, corrections, or updates about any portion of the book are welcomed.

Acknowledgments

We are very grateful to the Almighty Allah for allowing us the time to complete this work. Thanks to the contributors who provided the programming codes for different algorithms, as well as the write-ups of various schemes. We express our sincere gratitude to our wives and family members who have been constant sources of inspiration for our works. Last, but not the least, we are grateful to CRC Press for accepting our proposal for this project.

About the Editors



Saiful Azad earned his PhD in information engineering from the University of Padova, Italy, in 2013. He completed his BSc in computer and information technology at the Islamic University of Technology (IUT) in Bangladesh, and his MSc in computer and information engineering at the International Islamic University Malaysia (IIUM). After the completion of his PhD, he joined the Department of Computer Science at the American International University–Bangladesh (AIUB) as a faculty member. His work on underwater acoustic networks began during his PhD program and remains his main research focus. Dr. Azad’s interests also include the design and implementation of communication protocols for different network architectures, QoS issues, network security, and simulation software design. He is one of the developers of the DESERT underwater simulator. He is also the author of more than 30 scientific papers published in international peer-reviewed journals or conferences. Dr. Azad also serves as a reviewer for some renowned peer-reviewed journals and conferences.



Al-Sakib Khan Pathan earned his PhD degree (MS leading to PhD) in computer engineering in 2009 from Kyung Hee University in South Korea. He earned his BS degree in computer science and information technology from IUT, Bangladesh, in 2003. He is currently an assistant professor in the Computer Science Department of IIUM. Until June 2010 he served as an assistant professor in the Computer Science and Engineering Department of BRAC University, Bangladesh. Prior to holding this position, he worked as a researcher at the networking lab of Kyung Hee University, South Korea, until August 2009. Dr. Pathan's research interests include wireless sensor networks, network security, and e-services technologies. He has been a recipient of several awards/best paper awards and has several publications in these areas. He has served as chair, an organizing committee member, and a technical program committee member in numerous international conferences/workshops, including GLOBECOM, GreenCom, HPCS, ICA3PP, IWCMC, VTC, HPCC, and IDCS. He was awarded the IEEE Outstanding Leadership Award and Certificate of Appreciation for his role in the IEEE GreenCom 2013 conference. He is currently serving as area editor of *International Journal of Communication Networks and Information Security*, editor of *International Journal of Computational Science and Engineering*, *Inderscience*, associate editor of IASTED/ACTA Press *International Journal of Computer Applications*, guest editor of many special issues of top-ranked journals, and editor/author of 12 books. One of his books has twice been included in Intel Corporation's Recommended Reading List for Developers, the second half of 2013 and the first half of 2014; three other books are included in IEEE Communications Society's (IEEE ComSoc) Best Readings in Communications and Information Systems Security, 2013; and a fifth book is in the process of being translated to simplified Chinese language from the English version. Also, two of his journal papers and one conference paper are included under different categories in IEEE Communications Society's Best Readings Topics on Communications

and Information Systems Security, 2013. Dr. Pathan also serves as a referee of numerous renowned journals. He is a senior member of the Institute of Electrical and Electronics Engineers (IEEE), United States; IEEE ComSoc Bangladesh Chapter; and several other international professional organizations.

Contributors

Sheikh Shaugat Abdullah

Department of Computer
Science

American International
University–Bangladesh
(AIUB)

Dhaka, Bangladesh

Giovanni Agosta

Politecnico di Milano
Milano, Italy

Tanveer Ahmed

Dhaka University of
Engineering and Technology
(DUET)

Gazipur, Bangladesh

Saad Andalib

Department of Computer
Science

American International
University–Bangladesh (AIUB)

Dhaka, Bangladesh

Saiful Azad

Department of Computer
Science

American International
University–Bangladesh (AIUB)

Dhaka, Bangladesh

Alessandro Barenghi

Politecnico di Milano
Milano, Italy

XVIII**CONTRIBUTORS****Aymen Boudguiga**

ESME Engineering School
Paris, France

Mohamed Hamdi

Sup'Com
Technopark El Ghazala
Ariana, Tunisia

Bayzid Ashik Hossain

Department of Computer
Science
American International
University–Bangladesh (AIUB)
Dhaka, Bangladesh

Ezazul Islam

Department of Computer
Science
American International
University–Bangladesh (AIUB)
Dhaka, Bangladesh

Mohammad Abul Kashem

Dhaka University of Engineering
and Technology (DUET)
Gazipur, Bangladesh

Maryline Laurent

Telecom SudParis
Evry, France

Saef Ullah Miah

Department of Computer
Science
American International
University–Bangladesh (AIUB)
Dhaka, Bangladesh

Saddam Hossain Mukta

Department of Computer Science
American International
University–Bangladesh
(AIUB)
Dhaka, Bangladesh

Al-Sakib Khan Pathan

Department of Computer Science
Kulliyah (Faculty)
of Information and
Communication Technology
International Islamic University
Malaysia (IIUM)
Gombak, Malaysia

Gerardo Pelosi

Politecnico di Milano
Milano, Italy

Asif Ur Rahman

Department of Computer Science
American International
University–Bangladesh
(AIUB)
Dhaka, Bangladesh

Hafizur Rahman

Department of Computer
Science
American International
University–Bangladesh
(AIUB)
Dhaka, Bangladesh

Michele Scandale

Politecnico di Milano
Milano, Italy

Nasrin Sultana

Department of Computer
Science

American International
University–Bangladesh
(AIUB)

Dhaka, Bangladesh

Marat Zhanikeev

Department of Artificial
Intelligence

Computer Science and Systems
Engineering

Kyushu Institute of Technology
Fukuoka, Japan

