ENCYCLOPEDIA OF CRYPTOGRAPHY AND SECURITY

Editor-in-chief

Henk C.A. van Tilborg

Eindhoven University of Technology
The Netherlands

Springer

Library of Congress Cataloging-in-Publication Data

A C.I.P. Catalogue record for this book is available from the Library of Congress.

Encyclopedia of Cryptography and Security, Edited by Henk C. A. van Tilborg

p. cm.

ISBN-10: (HB) 0-387-23473-X
ISBN-13: (HB) 978-0387-23473-1
ISBN-10: (eBook) 0-387-23483-7
ISBN-13: (eBook) 978-0387-23483-0
Printed on acid-free paper.

Printed in the United States of America

9 8 7 6 5 4 3 2 1 SPIN 11327875 (HC) / 151464 (eBook)

springeronline.com

Dedicated to the ones I love

List of Advisory Board Members

List of Contributors

Carlisle Adams
Sacha Barg
Friedrich Bauer
Olivier Benoît
Eli Biham
Alex Biryukov
John Black
Robert Blakley
Gerrit Bleumer
Sharon Boeyen
Dan Boneh
Antoon Bosselaars
Gerald Brose
Marco Bucci
Mike Burmester
Christian Cachin
Tom Caddy
Ran Canetti
Anne Canteaut
Claude Carlet
Pascale Charpin
Hamid Choukri
Scott Contini
Claude Crépeau
Eric Cronin
Joan Daemen
Christophe De Canniere
Yvo Desmedt
Marijke de Soete
Yevgeniy Dodis
Glen Durfee
Cynthia Dwork
Carl Ellison
Toni Farley
Caroline Fontaine
Matthew Franklin
Martin Gagné
Daniel M. Gordon
Jorge Guajardo
Stuart Haber
Helena Handschuh
Darrel Hankerson
Clemens Heinrich
Tor Helleseth
Russ Housley
Hideki Imai
Anil Jain
Jill Joseph
Marc Joye
Mike Just
Gregory Kabatiansky
Burt Kaliski
Lars Knudsen
Çetin Kaya Koç
François Koeune
Hugo Krawczyk
Markus Kuhn
Peter Landrock
Kerstin Lemke
Arjen K. Lenstra
Paul Leyland
Benoît Libert
Moses Liskov
Steve Lloyd
Henri Massias
Patrick McDaniel
Alfred Menezes
Daniele Micciancio
Bodo Möller
François Morain
Dalit Naor
Kim Nguyen
Phong Q. Nguyen
Francis Olivier
Lukasz Opyrchal
Christof Paar
Pascal Paillier
Joe Pato
Sachar Paulus
Torben Pedersen
Benny Pinkas
David Pointcheval
Bart Preneel
Niels Provos
Jean-Jacques Quisquater
Vincent Rijmen
Ronald L. Rivest
Matt Robshaw
Arun Ross
Randy Sabett

Kazue Sako
David Samyde
Bruce Schneier
Berry Schoenmakers
Matthias Schunter
Nicolas Sendrier
Adi Shamir
Igor Shparlinski
Robert D. Silverman
Miles Smid
Jerome Solinas
Anton Stiglic
François-Xavier Standaert
Berk Sunar
Laurent Sustek
Henk van Tilborg
Assia Tria
Eran Tromer
Salil Vadhan
Pavan Verma
Colin Walter
Michael Ward
Andre Weimerskirch
William Whyte
Michael Wiener
Atsuhiro Yamagishi
Paul Zimmermann
Robert Zuccherato

Preface

The need to protect valuable information is as old as history. As far back as Roman times, Julius Caesar saw the need to encrypt messages by means of cryptographic tools. Even before then, people tried to hide their messages by making them "invisible." These hiding techniques, in an interesting twist of history, have resurfaced quite recently in the context of digital rights management. To control access or usage of digital contents like audio, video, or software, information is secretly embedded in the data!

Cryptology has developed over the centuries from an art, in which only few were skillful, into a science. Many people regard the "Communication Theory and Secrecy Systems" paper, by Claude Shannon in 1949, as the foundation of modern cryptology. However, at that time, cryptographic research was mostly restricted to government agencies and the military. That situation gradually changed with the expanding telecommunication industry. Communication systems that were completely controlled by computers demanded new techniques to protect the information flowing through the network.

In 1976, the paper "New Directions in Cryptography," by Whitfield Diffie and Martin Hellman, caused a shock in the academic community. This seminal paper showed that people who are communicating with each other over an insecure line can do so in a secure way with no need for a common secret key. In Shannon's world of secret key cryptography this was impossible, but in fact there was another cryptologic world of public-key cryptography, which turned out to have exciting applications in the real world. The 1976 paper and the subsequent paper on the RSA cryptosystem in 1978 also showed something else: mathematicians and computer scientists had found an extremely interesting new area of research, which was fueled by the ever-increasing social and scientific need for the tools that they were developing. From the notion of public-key cryptography, information security was born as a new discipline and it now affects almost every aspect of life.

As a consequence, information security, and even cryptology, is no longer the exclusive domain of research laboratories and the academic community. It first moved to specialized consultancy firms, and from there on to the many places in the world that deal with sensitive or valuable data; for example the financial world, the health care sector, public institutions, nongovernmental agencies, human rights groups, and the entertainment industry.

A rich stream of papers and many good books have been written on information security, but most of them assume a scholared reader who has the time to start at the beginning and work his way through the entire text. The time has come to make important notions of cryptography accessible to readers who have an interest in a particular keyword related to computer security or cryptology, but who lack the time to study one of the many books on computer and information security or cryptology. At the end of 2001, the idea to write an easily accessible encyclopedia on cryptography and information security was proposed. The goal was to make it possible to become familiar with a particular notion, but with minimal effort. Now, 4 years later, the project is finished, thanks to the help of many contributors, people who are all very busy in their professional life. On behalf of the Advisory Board, I would like to thank each of those contributors for their work. I would also like to acknowledge the feedback and help given by Mihir Bellare, Ran Canetti, Oded Goldreich, Bill Heelan, Carl Pomerance, and Samuel S. Wagstaff, Jr. A person who was truly instrumental for the success of this project is Jennifer Evans at Springer Verlag. Her ideas and constant support are greatly appreciated. Great help has been given locally by Anita Klooster and Wil Kortsmit. Thank you very much, all of you.

Henk van Tilborg