Primality Testing and Integer Factorization in Public-Key Cryptography

Second Edition

by

Song Y.Yan

Harvard University
and
Massachusetts Institute of Technology
USA

Springer

Author:
Dr. Song Y. Yan
Visiting Professor
Department of Mathematics
Harvard University
One Oxford Street
Cambridge, MA 02138-2901
syan@math.harvard.edu

and

Department of Mathematics
Massachusetts Institute of Technology
77 Massachusetts Avenue
Cambridge, MA 02139-4307
syan@math.mit.edu

Library of Congress Control Number: 2008935407

ISBN-13: 978-0-387-77267-7 e-ISBN-13: 978-0-387-77268-4

Printed on acid-free paper

springer.com

In Memory of Prof Shiing-Shen Chern (1911–2004)

Founding Director, Mathematical Sciences Research Institute, Berkeley

Table of Contents