Table of Contents

Preface xi

Cryptology and Computational Number Theory—An Introduction
CARL POMERANCE 1

Primality Testing
ARJEN K. LENSTRA 13

Factoring
CARL POMERANCE 27

The Discrete Logarithm Problem
KEVIN S. MCCURLEY 49

The Rise and Fall of Knapsack Cryptosystems
A. M. ODLYZKO 75

The Search for Provably Secure Cryptosystems
SHAFI GOLDWASSER 89

Pseudorandom Number Generators in Cryptography and Number Theory
J. C. LAGARIAS 115

Odds and Ends from Cryptology and Computational Number Theory
KEVIN S. MCCURLEY 145

Index 167