Table of Contents

About the Authors xiii

About the Technical Reviewer xv

Acknowledgments xvii

Part I: Foundations 1

Chapter 1: Getting Started in Cryptography and Cryptanalysis 3

Cryptography and Cryptanalysis 4

Book Structure 5

Internet Resources 9

Forums and Newsgroups 10

Standards 11

Conclusion 12

References 13

Chapter 2: Cryptography Fundamentals 15

Information Security and Cryptography 16

Cryptography Goals 19

Cryptographic Primitives 20

Background of Mathematical Functions 22

Functions: One-to-One, One-Way, Trapdoor One-Way 22

Permutations 28

Involutions 28

Concepts and Basic Terminology 29

Domains and Codomains Used for Encryption 29

Encryption and Decryption Transformations 30

The Participants in the Communication Process 31

Digital Signatures...32
Signing Process...33
Verification Process...33
Public-Key Cryptography...33
Hash Functions...36
Case Studies...53
Caesar Cipher Implementation in C++20...53
Vigenére Cipher Implementation in C++20...55
Conclusions...58
References...58
Chapter 3: Mathematical Background and Its Applicability...65
Preliminaries...66
Conditional Probability...67
Random Variables...68
Birthday Problem...69
Information Theory...70
Entropy...70
Number Theory...71
Integers...71
Algorithms in $\mathbb{Z}$...72
The Integer Modulo *n*...74
Algorithms $\mathbb{Z}_m$...75
The Legendre and Jacobi Symbols...76
Finite Fields...78
Basic Notions...78
Polynomials and the Euclidean Algorithm...79
Case Study 1: Computing the Probability of an Event Taking Place...80
Case Study 2: Computing the Probability Distribution...82
Case Study 3: Computing the Mean of the Probability Distribution...84
Case Study 4: Computing the Variance...85
Case Study 5: Computing the Standard Deviation...87

Case Study 6: Birthday Paradox 89
Case Study 7: (Extended) Euclidean Algorithm 91
Case Study 8: Computing the Multiplicative Inverse Under Modulo *q* 93
Case Study 9: Chinese Remainder Theorem 96
Case Study 10: The Legendre Symbol 98
Conclusion 101
References 102

Chapter 4: Large Integer Arithmetic 105
Big Integers 106
Big Integer Libraries 112
Conclusion 114
References 114

Chapter 5: Floating-Point Arithmetic 117
Why Floating-Point Arithmetic? 117
Displaying Floating Point Numbers 118
The Range of Floating Point Numbers 119
Floating Point Precision 119
Next Level for Floating-Point Arithmetic 122
Conclusions 123
References 123

Chapter 6: New Features in C++20 125
Feature Testing 125
carries_dependency 125
no_unique_address 127
New Headers in C++20 128
<concepts> Header 128
<compare> Header 131
<format> Header 132
Conclusion 133
References 133

Chapter 7: Secure Coding Guidelines 135

Secure Coding Checklist 136

CERT Coding Standards 140

Identifiers 141

Noncompliant Code Examples and Compliant Solutions 141

Exceptions 141

Risk Assessment 142

Automated Detection 143

Related Guidelines 143

Rules 144

Rule 1 - Declarations and Initializations (DCL) 144

Rule 2 - Expressions (EXP) 145

Rule 3 - Integers (INT) 146

Rule 5 - Characters and Strings (STR) 146

Rule 6 - Memory Management (MEM) 147

Rule 7 - Input/Output (FIO) 148

Conclusion 148

References 149

Chapter 8: Cryptography Libraries in C/C++20 151

Overview of Cryptography Libraries 151

Hash Functions 152

Public Key Cryptography 153

Elliptic-Curve Cryptography (ECC) 155

OpenSSL 158

Configuration and Installing OpenSSL 158

Botan 177

CrypTool 177

Conclusion 185

References 186

Part II: Pro Cryptography 187

Chapter 9: Elliptic-Curve Cryptography 189

Theoretical Fundamentals 190

Weierstrass Equation 192

Group Law 194

Practical Implementation 195

Conclusion 222

References 223

Chapter 10: Lattice-Based Cryptography 225

Mathematical Background 225

Example 227

Conclusion 237

References 237

Chapter 11: Searchable Encryption 239

Components 240

Entities 240

Types 241

Security Characteristics 243

An Example 244

Conclusion 255

References 256

Chapter 12: Homomorphic Encryption 259

Fully Homomorphic Encryption 261

Practical Example of Using FHE 263

Conclusion 283

References 283

Chapter 13: Ring Learning with Errors Cryptography 287
Mathematical Background 288
Learning with Errors 288
Ring Learning With Errors 290
Practical Implementation 291
Conclusion 299
References 299

Chapter 14: Chaos-Based Cryptography 303
Security Analysis 306
Chaotic Maps for Plaintexts and Images Encryption 307
Rössler Attractor 308
Complex Numbers – Short Overview 309
Practical Implementation 310
Secure Random Number Generator Using a Chaos Rössler Attractor 312
Cipher Using Chaos and Fractals 319
Conclusion 334
References 334

Chapter 15: Big Data Cryptography 337
Verifiable Computation 341
Conclusion 348
References 349

Chapter 16: Cloud Computing Cryptography 353
A Practical Example 354
Conclusion 360
References 361

Part III: Pro Cryptanalysis 363

Chapter 17: Getting Started with Cryptanalysis 365
Third Part Structure 367
Cryptanalysis Terms 367

A Little Bit of Cryptanalysis History....369
Penetration Tools and Frameworks....371
Conclusion....373
References....374

Chapter 18: Cryptanalysis Attacks and Techniques....377
Standards....377
FIPS 140-2, FIPS 140-3, and ISO 15408....378
Validation of Cryptographic Systems....378
Cryptanalysis Operations....380
Classification of Cryptanalytics Attacks....381
Attacks on Cipher Algorithms....381
Attacks on Cryptographic Keys....383
Attacks on Authentication Protocols....384
Conclusion....385
References....385

Chapter 19: Linear and Differential Cryptanalysis....387
Differential Cryptanalysis....388
Linear Cryptanalysis....396
Performing Linear Cryptanalysis....396
S-Boxes....397
Linear Approximation of S-Box....399
Concatenation of Linear Approximations....399
Assembling Two Variables....399
Conclusion....408
References....408

Chapter 20: Integral Cryptanalysis....411
Basic Notions....411
Practical Approach....413
Conclusion....422
References....422

Chapter 21: Brute Force and Buffer Overflow Attacks 423

Brute Force Attack 424

Buffer Overflow Attack 432

Conclusion 434

References 434

Chapter 22: Text Characterization 435

The Chi-Squared Statistic 435

Cryptanalysis Using Monogram, Bigram, and Trigram Frequency Counts 439

Counting Monograms 439

Counting Bigrams 440

Counting Trigrams 443

Conclusion 446

References 446

Chapter 23: Implementation and Practical Approach of Cryptanalysis Methods 447

Ciphertext-Only Attack 450

Known-Plaintext Attack 450

Chosen-Plaintext Attack 451

Chosen-Ciphertext Attack 459

Conclusion 460

References 461

Correction to: Pro Cryptography and Cryptanalysis with C++20 .... C1

Index 463