Contents

Contemporary Cryptology: A Foreword vii
G. J. Simmons

Contemporary Cryptology: An Introduction 1
James L. Massey

Preliminaries . . . Secret key cryptography . . . Public key cryptography . . . Cryptographic protocols . . . References

SECTION 1 CRYPTOGRAPHY 41

Chapter 1 The Data Encryption Standard: Past and Future 43
Miles E. Smid and Dennis K. Branstad

The birth of the DES . . . The DES controversy . . . Acceptance by government and commercial sectors . . . Applications . . . New algorithms . . . DES: The next decade . . . Conclusions . . . References

Chapter 2 Stream Ciphers 65
Rainer A. Rueppel

Introduction . . . Information-theoretic approach . . . System-theoretic approach

. . . Complexity-theoretic approach . . . Randomized stream ciphers . . . References

Chapter 3 The First Ten Years of Public Key Cryptology 135
Whitfield Diffie

Initial discoveries . . . Exponential key exchange . . . Trapdoor knapsacks . . . The Rivest-Shamir-Adleman system . . . The McEliece coding scheme . . . The fall of the knapsacks . . . Early responses to public key cryptosystems . . . Application and implementation . . . Multiplying, factoring, and finding primes . . . Directions in public key cryptography research . . . Where is public key cryptography going? . . . References

Chapter 4 Public Key Cryptography 177
James Nechvatal

Introduction . . . Cryptosystems and cryptanalysis . . . Key management . . . Digital signatures and hash functions . . . Examples of public key systems and hash functions . . . Implementations of public key cryptography . . . A sample proposal for a LAN implementation . . . Mathematical and computational aspects . . . An introduction to zero-knowledge . . . Alternatives to the Diffie-Hellman model . . . Appendices . . . References

Chapter 5 A Comparison of Practical Public Key Cryptosystems Based on Integer Factorization and Discrete Logarithms 289
Paul C. van Oorschot

Introduction . . . Discrete logarithms in fields of characteristic 2 . . . Integer factorization . . . Comparing El Gamal in GF (2^n) versus RSA . . . Recent work regarding elliptic curve cryptosystems . . . Concluding remarks . . . References

SECTION 2 AUTHENTICATION 323

Chapter 6 Digital Signatures 325
C. J. Mitchell, F. Piper, and P. Wild

Introduction . . . Fundamental concepts . . . Techniques for digital signatures . . . Techniques for hashing . . . Applications for digital signatures . . . References

Chapter 7 A Survey of Information Authentication 379
G. J. Simmons

Introduction . . . The threat(s) . . . A natural classification of authentication schemes . . . How insecure can unconditionally secure authentication be? . . . The practice of authentication . . . Conclusions . . . References

SECTION 3 PROTOCOLS 421

Chapter 8 Overview of Interactive Proof Systems and Zero-Knowledge 423
J. Feigenbaum

Introduction . . . Definitions . . . Examples . . . Known results . . . Related notions . . . Open problems . . . References . . . Appendix

Chapter 9 An Introduction to Shared Secret and/or Shared Control Schemes and Their Application 441
G. J. Simmons

Introduction . . . The general model(s) . . . Constructing concurrence schemes . . . The geometry of shared secret schemes . . . Setting up shared secret schemes . . . Key distribution via shared secret schemes . . . Conclusions . . . References . . . Bibliography

SECTION 4 CRYPTANALYSIS 499

Chapter 10 Cryptanalysis: A Survey of Recent Results 501
E. F. Brickell and A. M. Odlyzko

Introduction . . . Knapsack cryptosystems . . . Generalized knapsack cryptosystems. . . The Ong–Schnorr–Shamir (OSS) signature scheme . . . The Okamoto–Shiraishi signature scheme . . . Additional broken two-key systems . . . The RSA cryptosystem . . . Discrete exponentiation . . . The McEliece cryptosystem . . . Congruential generators . . . DES . . . Fast data encipherment algorithm . . . Additional comments . . . References

Chapter 11 Protocol Failures in Cryptosystems 541
J. H. Moore

Introduction . . . The notary protocol . . . The common modulus protocol . . . The small exponent protocol failure . . . The low entropy protocol failure . . . A single key protocol failure . . . Summary and analysis . . . References

SECTION 5 APPLICATIONS 559

Chapter 12 The Smart Card: A Standardized Security Device Dedicated to Public Cryptology 561
Louis Claude Guillou, Michel Ugon, and Jean-Jacques Quisquater

Introduction . . . Comprehensive approach . . . Standardization . . . Technology . . . Security . . . Evolution of card authentication . . . Conclusions . . . Appendix . . . Glossary . . . References

Chapter 13 How to Insure That Data Acquired to Verify Treaty Compliance Are Trustworthy **615**
G. J. Simmons

Introduction . . . Verification of a comprehensive test ban treaty . . . Verification without secrecy . . . Verification with arbitration . . . Verification in the presence of deceit . . . Concluding remarks

Index **631**

Editor's Biography **640**