TABLE OF CONTENTS

CHAPTER 1: MATHEMATICAL FOUNDATIONS OF CRYPTOGRAPHY AND CYBERSECURITY **01-52**

1.1 Role of Mathematics in Cybersecurity
1.2 Security Objectives, Threat Models and Adversarial Capabilities
1.3 Cryptographic Primitives, Protocols and Security Parameters
1.4 Computational Security and the Notion of Hardness

CHAPTER 2: ELEMENTARY NUMBER THEORY **53-91**

2.1 Divisibility, Prime Numbers and Fundamental Theorem of Arithmetic
2.2 Greatest Common Divisor and Euclidean Algorithm
2.3 Extended Euclidean Algorithm and Bézout's Identity
2.4 Congruences, Residue Classes and Modular Inverses

CHAPTER 3: MODULAR ARITHMETIC AND NUMBER-THEORETIC THEOREMS **92-127**

3.1 Arithmetic in the Integers Modulon
3.2 Modular Exponentiation and Repeated Squaring
3.3 Euler's Totient Function and Multiplicative Order
3.4 Fermat's Little Theorem and Euler's Theorem
3.5 Chinese Remainder Theorem and Cryptographic Applications

CHAPTER 4: ABSTRACT ALGEBRA AND FINITE FIELDS **128-149**

4.1 Groups, Subgroups and Cyclic Groups
4.2 Generators, Rings, Integral Domains and Fields
4.3 Finite Fields GF(p) and Binary Extension Fields GF(2^n)
4.4 Polynomial Arithmetic and Irreducible Polynomials
4.5 Finite-Field Operations in Cryptographic Algorithms

CHAPTER 5: PROBABILITY, INFORMATION THEORY AND RANDOMNESS **150-174**

5.1 Probability Rules, Conditional Probability and Independence
5.2 Random Variables, Expected Value and Variance
5.3 Entropy, Information Content and Uncertainty
5.4 Perfect Secrecy and the One-Time Pad
5.5 Birthday Bound, Collision Probability and Secure Randomness

CHAPTER 6: CLASSICAL CRYPTOSYSTEMS AND CRYPTANALYSIS **175-203**

6.1 Substitution and Transposition Ciphers
6.2 Caesar, Affine, Vigenère and Hill Ciphers
6.3 Frequency Analysis and Classical Cryptanalytic Techniques
6.4 Brute-Force Search, Key Space and Work-Factor Estimation
6.5 Lessons from Classical Ciphers for Modern Security

CHAPTER 7: SYMMETRIC-KEY CRYPTOGRAPHY **204-234**
7.1 Symmetric Encryption Models and Design Principles
7.2 Confusion, Diffusion and Feistel Networks
7.3 Stream Ciphers, Keystreams and Nonce Requirements
7.4 Block Ciphers and the Advanced Encryption Standard (AES)
7.5 Modes of Operation, Initialization Vectors and Common Misuse

CHAPTER 8: PRIME GENERATION, PRIMALITY TESTING AND FACTORISATION **235-264**
8.1 Prime Generation and Probabilistic Primality Testing
8.2 Fermat and Miller–Rabin Primality Tests
8.3 Integer Factorisation and Computational Complexity
8.4 Introductory Factorisation Methods
8.5 Impact of Number-Theoretic Algorithms on Cryptographic Security

CHAPTER 9: RSA PUBLIC-KEY CRYPTOGRAPHY **265-292**
9.1 Public-Key Cryptography and RSA Key Generation
9.2 Public and Private Exponents Using Modular Inverses
9.3 RSA Encryption and Decryption: Worked Examples
9.4 Correctness of RSA and the Chinese Remainder Theorem
9.5 Padding, Implementation Risks and Security Considerations

CHAPTER 10: DISCRETE LOGARITHMS AND KEY-EXCHANGE PROTOCOLS **293-326**
10.1 Discrete Logarithm Problem in Finite Groups
10.2 Primitive Roots, Generators and Cyclic Subgroups
10.3 Diffie–Hellman Key Exchange
10.4 ElGamal Encryption and Digital Signature Concepts
10.5 Authentication, Man-in-the-Middle Attacks and Protocol Protection

CHAPTER 11: ELLIPTIC-CURVE CRYPTOGRAPHY **327-362**
11.1 Elliptic Curves over Real Numbers and Finite Fields
11.2 Point Addition, Point Doubling and Scalar Multiplication
11.3 Elliptic-Curve Discrete Logarithm Problem
11.4 Elliptic-Curve Diffie–Hellman and Digital Signatures
11.5 Security Parameters and Implementation Considerations