**Chapter 1 Computer and Network Security Concepts 19**

1.1 Computer Security Concepts 21

1.2 The OSI Security Architecture 26

1.3 Security Attacks 27

1.4 Security Services 29

1.5 Security Mechanisms 32

1.6 Fundamental Security Design Principles 34

1.7 Attack Surfaces and Attack Trees 37

1.8 A Model for Network Security 41

1.9 Standards 43

1.10 Key Terms, Review Questions, and Problems 44

**Chapter 2 Introduction to Number Theory 46**

2.1 Divisibility and the Division Algorithm 47

2.2 The Euclidean Algorithm 49

2.3 Modular Arithmetic 53

2.4 Prime Numbers 61

2.5 Fermat’s and Euler’s Theorems 64

2.6 Testing for Primality 68

2.7 The Chinese Remainder Theorem 71

2.8 Discrete Logarithms 73

2.9 Key Terms, Review Questions, and Problems 78

**Chapter 3 Classical Encryption Techniques 85**

3.1 Symmetric Cipher Model 86

3.2 Substitution Techniques 92

3.3 Transposition Techniques 107

3.4 Rotor Machines 108

3.5 Steganography 110

3.6 Key Terms, Review Questions, and Problems 112

**Chapter 4 Block Ciphers and the Data Encryption Standard 118**

4.1 Traditional Block Cipher Structure 119

4.2 The Data Encryption Standard 129

4.3 A DES Example 131

4.4 The Strength of DES 134

4.5 Block Cipher Design Principles 135