

Contents

| | |
|--|----|
| Introduction | 1 |
| 1 Classical Polyalphabetic Substitution Ciphers | 9 |
| 1.1 The Vigenère Cipher | 9 |
| 1.2 The One Time Pad, Perfect Secrecy, and Cascade Ciphers ... | 12 |
| 2 RSA and Probabilistic Prime Number Tests | 17 |
| 2.1 General Considerations and the RSA System | 17 |
| 2.2 The Solovay-Strassen Test | 19 |
| 2.3 Rabin's Test | 22 |
| 2.4 *Bit Security of RSA | 25 |
| 2.5 The Timing Attack on RSA | 33 |
| 2.6 *Zero-Knowledge Proof for the RSA Secret Key | 34 |
| 3 Factorization with Quantum Computers: Shor's Algorithm . | 37 |
| 3.1 Classical Factorization Algorithms | 37 |
| 3.2 Quantum Computing | 38 |
| 3.3 Continued Fractions | 40 |
| 3.4 The Algorithm | 43 |
| 4 Physical Random-Number Generators | 47 |
| 4.1 Generalities | 47 |
| 4.2 Construction of Uniformly Distributed Random Numbers from a Poisson Process | 48 |
| 4.3 *The Extraction Rate for Biased Random Bits | 52 |
| 5 Pseudo-random Number Generators | 57 |
| 5.1 Linear Feedback Shift Registers | 57 |
| 5.2 The Shrinking and Self-shrinking Generators | 62 |
| 5.3 Perfect Pseudo-randomness | 65 |
| 5.4 Local Statistics and de Bruijn Shift Registers | 68 |
| 5.5 Correlation Immunity | 69 |
| 5.6 The Quadratic Congruential Generator | 72 |

| | | |
|-----------|---|-----|
| 6 | An Information Theory Primer | 77 |
| 6.1 | Entropy and Coding | 77 |
| 6.2 | Relative Entropy, Mutual Information, and Impersonation Attack | 80 |
| 6.3 | *Marginal Guesswork | 86 |
| 7 | Tests for (Pseudo-)Random Number Generators | 89 |
| 7.1 | The Frequency Test and Generalized Serial Test | 89 |
| 7.2 | Maximum Absolute Value of Random Walk Test | 91 |
| 7.3 | Number of Visits of Random Walk Test | 92 |
| 7.4 | Run Tests | 93 |
| 7.5 | Tests on Frequencies of Patterns | 95 |
| 7.6 | Tests Based on Missing Words | 95 |
| 7.7 | Approximate Entropy Test | 97 |
| 7.8 | The Ziv-Lempel Complexity Test | 98 |
| 7.9 | Maurer's "Universal Test" | 99 |
| 7.10 | Rank of Random Matrices Test | 100 |
| 7.11 | Linear Complexity Test | 101 |
| 8 | Diffie-Hellman Key Exchange | 107 |
| 8.1 | The Diffie-Hellman System | 107 |
| 8.2 | Distribution of Diffie-Hellman Keys | 107 |
| 8.3 | Strong Primes | 112 |
| 9 | Differential Cryptanalysis | 115 |
| 9.1 | The Principle | 115 |
| 9.2 | The Distribution of Characteristics | 119 |
| 10 | Semantic Security | 125 |
| 11 | *Algorithmic Complexity | 135 |
| 12 | Birthday Paradox and Meet-in-the-Middle Attack | 139 |
| 12.1 | The Classical Birthday Attack | 139 |
| 12.2 | The Generalized Birthday Problem and Its Limit Distribution | 140 |
| 12.3 | The Meet-in-the-Middle Attack | 143 |
| 13 | Quantum Cryptography | 145 |
| | Bibliographical Remarks | 147 |
| | References | 151 |
| | Index | 157 |