Michele Elia

An introduction to Classic Cryptography

With an exposition of the mathematics of private and public key ciphers

Contents

13 *Preface*

15 Chapter I
Cryptography from Art to Science

1.1. Introduction, 15 – 1.2. Information Protection, 16 – 1.2.1. *The goals of Information Protection*, 16 – 1.2.2. *Aims*, 18 – 1.2.3. *Summary*, 18 – 1.3. Historical glimpses, 19 – 1.3.1. *Cryptography from diplomacy to commerce*, 19 – 1.3.2. *From art to science*, 23.

25 Chapter II
The Shannon theory of secrecy systems

2.1. Introduction, 25 – 2.2. Uncertainty: Entropy and Mutual Information, 27 – 2.3. Uncertainty and Secrecy, 29 – 2.3.1. *Binary message encryption*, 33 – 2.4. Cryptology, 33 – 2.5. The science of cryptography, 34 – 2.6. Steganography, 37.

39 Chapter III
Random Sequences and Statistics

3.1. Introduction, 39 – 3.1.1. *Sample Spaces*, 41 – 3.2. Statistical Tests for Binary Sequences, 44 – 3.2.1. *Linear Complexity Profile*, 53.

59 Chapter IV
Secret-key cryptography

4.1. Introduction, 59 – 4.2. The role of the secret-key, 59 – 4.3. Historical Encryption Systems, 61 – 4.3.1. *Substitution encryption*, 61 – 4.3.2. *Transposition encryption*, 62 – 4.3.3. *Polybius method*, 62 – 4.3.4. *Alberti's disk*, 62 – 4.3.5. *Bellaso cipher*, 63 – 4.3.6. *Vigenère cipher*, 66 – 4.3.7. *Hill Cipher*, 67 – 4.3.8. *The Francis Bacon Cipher*, 68 – 4.3.9. *One-time pad*, 68 – 4.3.10. *Enigma*, 69 – 4.4. Block ciphers, 70 – 4.4.1. *Common structure of block ciphers*, 71 – 4.4.2. *Modes*, 72 – 4.5. DES, 75 – 4.5.1. *DES transformations*, 77 – 4.5.2. *Local key generation*, 80 – 4.6. AES, 82 – 4.6.1. *Round Transformations*, 85 – 4.6.2. *Local Key generation*, 86.

87 Chapter V
Secret-Key Cryptography Stream ciphers

5.1. Introduction, 87 – 5.1.1. *The structure*, 87 – 5.1.2. *Finite State Machines*, 88 – 5.2. Output functions - Boolean functions, 89 – 5.3. Periodic generators and LFSRs, 92 – 5.3.1. *The mathematics of LFSRs*, 94 – 5.4. Linear Codes and Binary

Sequences, 97 – 5.4.1. *BCH codes*, 98 – 5.4.2. *Goppa codes*, 99 – 5.5. Nonlinear Feedback Shift Registers, 100 – 5.5.1. *Clock-controlled LFSR*, 101 – 5.5.2. *Self-clock-controlled LFSR*, 102 – 5.5.3. *Clock-controlling and puncturing*, 103 – 5.5.4. *LCP of clock-controlled LFSR sequences*, 104 – 5.6. Encryption with rate less than 1, 105 – 5.7. Appendix I - Matrix Representation of Finite Fields, 109 – 5.8. Appendix II - Linear recurrent equations in $\mathbb{F}_q$, 111 – 5.8.1. *Generating functions*, 113 – 5.8.2. *Characteristic equation methods*, 118 – 5.9. Appendix III - Tridiagonal matrices and LFSRs, 121 – 5.9.1. *Lanczos' tridiagonalization*, 130.

133 Chapter VI
Public–key Cryptography

6.1. Introduction, 133 – 6.1.1. *One–way functions*, 135 – 6.2. The RSA Scheme, 139 – 6.3. The Rabin Scheme, 143 – 6.4. The El Gamal Scheme, 145 – 6.5. The McEliece Scheme, 147.

149 Chapter VII
Electronic signatures

7.1. Introduction, 149 – 7.1.1. *Electronic signature of an electronic document*, 152 – 7.2. Components of electronically signed documents, 153 – 7.2.1. *The Document*, 154 – 7.2.2. *Standard hash function SHA-1*, 156 – 7.3. Signature based on RSA, 157 – 7.4. Signature based on the Rabin scheme, 158 – 7.5. Signature based on El Gamal, 162 – 7.6. Blind signature, 164 – 7.7. Secret Sharing – Shamir, 165.

167 Chapter VIII
Complexity

8.1. Introduction, 167 – 8.1.1. *A heuristic view of computational complexity*, 169 – 8.2. Complexity: the Heart of Cryptography, 171 – 8.2.1. *One–way functions*, 173 – 8.3. Arithmetic complexity, 174 – 8.3.1. *Complexity of product and exponentiation*, 174 – 8.3.2. *Finite field arithmetics*, 176 – 8.4. Factorization complexity, 177 – 8.4.1. *Factorization in* $\mathbb{Z}$, 178 – 8.5. Discrete logarithm, 178 – 8.5.1. *Discrete logarithm as one–way function*, 180 – 8.5.2. *Discrete Logarithm Complexity*, 181 – 8.5.3. *Shanks' Bound*, 184 – 8.6. Searching Unsorted Data (SUD), 185.

189 Chapter IX
ECC

9.1. Introduction, 189 – 9.2. Elliptic Curves and Group Law, 191 – 9.2.1. *Group Law*, 193 – 9.3. EC over Finite Fields, 196 – 9.4. EC Public–key Schemes, 200 – 9.5. Arithmetics and complexity in ECC, 201 – 9.6. Historical Notes, 204 – 9.6.1. *The origins*, 205.

207 Chapter X
Cryptanalysis

10.1. Introduction, 207 – 10.2. Axioms, 208 – 10.3. Cryptanalysis of secret-key systems, 209 – 10.3.1. *Cryptanalysis of classic schemes*, 210 – 10.4. Enigma and its Cryptanalysis, 224 – 10.5. DES Cryptanalysis, 231 – 10.6. Cryptanalysis of Public

Key Systems, 235 – 10.6.1. *Factorization*, 236 – 10.6.2. *Factorization procedure with EC*, 237 – 10.6.3. *Discrete logarithms*, 238.

241 Chapter XI
Cryptography in Mobile Systems

11.1. Evolution of cellular systems, 242 – 11.2. GSM, 244 – 11.2.1. *Origins*, 244 – 11.2.2. *Communications aspects*, 246 – 11.2.3. *Security and Protections*, 247 – 11.3. Conclusions, 250.

253 Chapter XII
Steganography

12.1. Introduction, 253 – 12.2. Some historical notes, 254 – 12.3. Steganographic channel models, 256 – 12.4. Concealment issues, 259 – 12.4.1. *Examples, Simulation, and Results*, 259 – 12.5. Conclusions, 264.

267 *References*

273 *Acknowledgments*