Contents

1 Introduction **3**
1.1 Fundamental Knowledge for Cryptographers 3

2 Classical Cryptography **5**
2.1 The Scytale ($\sigma\kappa\upsilon\tau\acute{\alpha}\lambda\eta$) 5
2.2 Substitution Cipher 5
2.2.1 Caesar Cipher 5
2.4 Vigenère Cipher 5
2.6 Formal Definition of a Cryptosystem and Types of Attacks 5
2.6.1 Cryptanalysis 5

3 Cryptanalysis of Classical Systems **7**
3.1 Frequency Analysis 7
3.2 The Friedmann Test 7
3.3 Estimating the Keylength of a Vigenère Cipher 7
3.4 Attacks Against Vigenère Cipher with Running Key 7

4 Entropy and Perfect Secrecy **9**
4.1 Foundations of Information Theory 9
4.1.1 Entropy 9
4.2 Perfect Secrecy 9
4.2.1 Perfect Secrecy of the Vernam Cipher 9

5 Fast Block Ciphers **11**
5.2 The Advanced Encryption Standard (AES) 11
5.2.1 Encryption Procedure 11
5.2.2 Key Expansion 11
5.2.3 Decryption 11
5.2.4 Design Considerations and Security 11
5.3 Other Block Ciphers 11
5.4 Modes of Operation 11
5.4.1 Electronic Codebook Mode (ECB) 11
5.4.2 Cipher-Block Chaining Mode (CBC) 11
5.4.3 Output Feedback Mode (OFB) 11
5.4.4 Cipher Feedback Mode (CFB) 11
5.4.5 Counter Mode (CTR) 11

6 Number-Theoretic Reference Problems 13
6.1 Primality Testing 13
6.1.1 Fermat Primality Test (FPT) 13
6.1.2 Miller-Rabin Primality Test (MRPT) 13
6.1.3 Deterministic Primality Testing 13
6.1.4 Finding Large Prime Numbers 13
6.2 The Integer Factorization Problem 13
6.3 The Extended Euclidean Algorithm 13
6.4 The Chinese Remainder Theorem 13

7 The Discrete Logarithm 15
7.1 Diffie-Hellman Key Distribution and Key Agreement 15
7.1.1 Intruder-in-the-Middle Attack on the DH-System 15
7.2 Shamir's No-Key Protocol 15

8 Public-Key Cryptography 17
8.1 The RSA-Cryptosystem 17
8.1.1 Security of RSA 17
8.1.2 Implementation of RSA 17
8.2 The ElGamal Cryptosystem 17
8.4 Public Key Infrastructure 17
8.4.1 The PGP Hierarchy 17

9 Public Key Cryptography (ctd.) 19
9.2 The Rabin Cryptosystem 19

10 Cryptographic Hash Functions 21
10.1 Security of Hash Functions 21
10.2 Construction of Hash Functions 21

11 Signature Schemes 23
11.1 The ElGamal Signature Scheme 23
11.1.1 Security of the ElGamal Signature Scheme 23

13 Elliptic Curves 25
13.1 Foundations and Definitions 25
13.2 The Group Law 25
13.3 The DLP on Elliptic Curves 25
13.3.1 Algorithms for Solving DLP/ECDLP 25
13.3.2 Cryptographically Secure Elliptic Curves 25
13.3.3 Comparison DLP vs. ECDLP 25