

Contents

1	Introduction	5
1.1	Fundamental Knowledge for Cryptographers	5
2	Classical Cryptography	7
2.1	The Scytale (<i>σκυτάλη</i>)	7
2.2	Substitution Cipher	7
2.2.1	Caesar Cipher	7
2.2.2	Affine Cipher in Z_m	7
2.4	Vigenère Cipher	7
2.6	Formal Definition of a Cryptosystem and Types of Attacks	7
2.6.1	Cryptanalysis	7
3	Cryptanalysis of Classical Systems	9
3.1	Frequency Analysis	9
3.2	The Friedmann Test	9
3.3	Estimating the Keylength of a Vigenère Cipher	9
3.4	Attacks Against Vigenère Cipher with Running Key	9
4	Entropy and Perfect Secrecy	11
4.1	Foundations of Information Theory	11
4.1.1	Entropy	11
4.2	Perfect Secrecy	11
4.2.1	Perfect Secrecy of the Vernam Cipher	11
5	Fast Block Ciphers	13
5.2	The Advanced Encryption Standard (AES)	13
5.2.1	Encryption Procedure	13
5.2.2	Key Expansion	13
5.2.3	Decryption	13
5.2.4	Design Considerations and Security	13
5.3	Other Block Ciphers	13
5.4	Modes of Operation	13
5.4.1	Electronic Codebook Mode (ECB)	13
5.4.2	Cipher-Block Chaining Mode (CBC)	13
5.4.3	Output Feedback Mode (OFB)	13
5.4.4	Cipher Feedback Mode (CFB)	13
5.4.5	Counter Mode (CTR)	13

6	Number-Theoretic Reference Problems	15
6.1	Primality Testing	15
6.1.1	Fermat Primality Test (FPT)	15
6.1.2	Miller-Rabin Primality Test (MRPT)	15
6.1.3	Deterministic Primality Testing	15
6.1.4	Finding Large Prime Numbers	15
6.2	The Integer Factorization Problem	15
6.3	The Extended Euclidean Algorithm	15
6.4	The Chinese Remainder Theorem	15
7	The Discrete Logarithm	17
7.1	Diffie-Hellman Key Distribution and Key Agreement	17
7.1.1	Intruder-in-the-Middle Attack on the DH-System	17
7.2	Shamir's No-Key Protocol	17
8	Public-Key Cryptography	19
8.1	The RSA-Cryptosystem	19
8.1.1	Security of RSA	19
8.1.2	Implementation of RSA	19
8.1.3	The RSA Signature Scheme	19
8.2	The ElGamal Cryptosystem	19
8.3	Generalized ElGamal Encryption	19
8.4	Public Key Infrastructure	19
8.4.1	The PGP Hierarchy	19
9	Public Key Cryptography (ctd.)	21
9.2	The Rabin Cryptosystem	21
10	Cryptographic Hash Functions	23
10.1	Security of Hash Functions	23
10.2	Construction of Hash Functions	23
11	Signature Schemes	25
11.1	The ElGamal Signature Scheme	25
11.1.1	Security of the ElGamal Signature Scheme	25
11.2	The Digital Signature Algorithm (DSA)	25
13	Elliptic Curves	27
13.1	Foundations and Definitions	27
13.2	The Group Law	27
13.2.1	Group Order $\#E(\mathbb{F}_q)$	27
13.3	The DLP on Elliptic Curves	27
13.3.1	Algorithms for Solving DLP/ECDLP	27
13.3.2	Cryptographically Secure Elliptic Curves	27
13.3.3	Comparison DLP vs. ECDLP	27

13.4 Cryptographic Applications	27
13.4.1 Diffie-Hellman Key Exchange	27
13.4.2 ElGamal on Elliptic Curves (ECElGamal)	27