1 Basics and History **1**
1.1 What It Is About: The Scenario 1
1.2 Alphabets and Digitisation. 3
1.3 Caesar Cipher. 6
1.4 Secret Writing of the Illuminati 8
1.5 Vigenère Cipher 10
1.6 Kasiski and Friedman Attack 12
1.7 Enigma Machine 15

2 Symmetric Ciphers **19**
2.1 Keys and Attack Strategies. 19
2.2 Vernam Cipher and Pseudo-Randomness 22
2.3 GSM Mobile Communications 24
2.4 Feistel Cipher. 26
2.5 Data Encryption Standard DES 29
2.6 Operating Modes of Block Ciphers 38
2.7 UMTS/LTE Mobile Communications and Digital Television 41
2.8 Advanced Encryption Standard AES 43
2.9 Hard Disk and ZIP Archive 49

3 Public-Key Ciphers **53**
3.1 Factorization and RSA Cipher 53
3.2 Internet and WLAN 59
3.3 Monte Carlo Prime Numbers 61
3.4 Attack by Factorization 65
3.5 Discrete Logarithm and Diffie-Hellman 69
3.6 Attack with Baby and Giant Steps 74
3.7 Bluetooth and ECDH 78
3.8 ElGamal Cipher 83
3.9 Knapsack and Merkle-Hellman Cipher 85

Bibliografische Informationen
https://d-nb.info/126291471X

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

4 Digital Signature **87**
4.1 Man-in-the-Middle Attack and Authentication 87
4.2 RSA and ElGamal Signature 90
4.3 Hash Value and Secure Hash Algorithm SHA 94
4.4 Email with PGP and WhatsApp 99
4.5 DSA and ECDSA Signature 102
4.6 Online Banking 107
4.7 Blind Signature and Cryptocurrencies 110
4.8 Password Security and Challenge Response 114
4.9 Mobile Phone, Credit Card and Passport 118

Bibliography **125**

Index **131**