Johannes A. Buchmann

INTRODUCTION TO CRYPTOGRAPHY

RSA-155

=

109417386415705274218097073220403576120
037329454492059909138421314763499842889
347847179972578912673324976257528997818
33797076537244027146743531593354333897

=

102639592829741105772054196573991675900
716567808038066803341933521790711307779

×

106603488380168454820927220360012878679
207958575989291522270608237193062808643

Springer

Contents

Preface v

1 Integers 1

1.1 Basics 1

1.2 Divisibility 2

1.3 Representation of Integers 4

1.4 O- and Ω-Notation 6

1.5 Cost of Addition, Multiplication, and Division with Remainder 7

1.6 Polynomial Time 9

1.7 Greatest Common Divisor 9

1.8 Euclidean Algorithm 12

1.9 Extended Euclidean Algorithm 16

1.10 Analysis of the Extended Euclidean Algorithm 18

1.11 Factoring into Primes 21

1.12 Exercises 24

2 Congruences and Residue Class Rings 29

2.1 Congruences 29

2.2 Semigroups 32

2.3 Groups 34

2.4 Residue Class Rings 35
2.5 Fields 36
2.6 Division in the Residue Class Ring 36
2.7 Analysis of Operations in the Residue Class Ring . . . 38
2.8 Multiplicative Group of Residues 39
2.9 Order of Group Elements 41
2.10 Subgroups 42
2.11 Fermat's Little Theorem 44
2.12 Fast Exponentiation 45
2.13 Fast Evaluation of Power Products 48
2.14 Computation of Element Orders 49
2.15 The Chinese Remainder Theorem 51
2.16 Decomposition of the Residue Class Ring 54
2.17 A Formula for the Euler φ-Function 55
2.18 Polynomials 57
2.19 Polynomials over Fields 59
2.20 Structure of the Unit Group of Finite Fields 62
2.21 Structure of the Multiplicative Group of Residues mod a Prime Number 63
2.22 Exercises 64

3 Encryption **69**
3.1 Encryption Schemes 69
3.2 Symmetric and Asymmetric Cryptosystems 71
3.3 Cryptanalysis 71
3.4 Alphabets and Words 73
3.5 Permutations 75
3.6 Block Ciphers 77
3.7 Multiple Encryption 78
3.8 Use of Block Ciphers 79
3.9 Stream Ciphers 8
3.10 Affine Cipher 8
3.11 Matrices and Linear Maps 9
3.12 Affine Linear Block Ciphers 9
3.13 Vigenère, Hill, and Permutation Ciphers 9
3.14 Cryptanalysis of Affine Linear Block Ciphers 9
3.15 Exercises 9

4 Probability and Perfect Secrecy 103
4.1 Probability 103
4.2 Conditional Probability 105
4.3 Birthday Paradox 106
4.4 Perfect Secrecy 107
4.5 Vernam One-Time Pad 110
4.6 Random Numbers 111
4.7 Pseudorandom Numbers 112
4.8 Exercises 112

5 DES 115
5.1 Feistel Ciphers 115
5.2 DES Algorithm 116
5.3 An Example 123
5.4 Security of DES 124
5.5 Exercises 125

6 Prime Number Generation 127
6.1 Trial Division 127
6.2 Fermat Test 129
6.3 Carmichael Numbers 130
6.4 Miller-Rabin Test 132
6.5 Random Primes 135
6.6 Exercises 136

7 Public-Key Encryption 139
7.1 Idea 139
7.2 RSA Cryptosystem 141
7.3 Rabin Encryption 153
7.4 Diffie-Hellman Key Exchange 158
7.5 ElGamal Encryption 162
7.6 Exercises 167

8 Factoring 171
8.1 Trial Division 171
8.2 $p-1$ Method 172
8.3 Quadratic Sieve 173
8.4 Analysis of the Quadratic Sieve 178

8.5 Efficiency of Other Factoring Algorithms
8.6 Exercises

9 Discrete Logarithms

9.1 DL Problem
9.2 Enumeration
9.3 Shanks Baby-Step Giant-Step Algorithm
9.4 Pollard ρ-Algorithm
9.5 Pohlig-Hellman Algorithm
9.6 Index Calculus
9.7 Other Algorithms
9.8 Generalization of the Index Calculus Algorithm
9.9 Exercises

10 Cryptographic Hash Functions

10.1 Hash Functions and Compression Functions
10.2 Birthday Attack
10.3 Compression Functions from Encryption Functions
10.4 Hash Functions from Compression Functions
10.5 Efficient Hash Functions
10.6 An Arithmetic Compression Function
10.7 Message Authentication Codes
10.8 Exercises

11 Digital Signatures

11.1 Idea
11.2 RSA Signatures
11.3 Signatures from Public-Key Systems
11.4 ElGamal Signature
11.5 Digital Signature Algorithm (DSA)
11.6 Exercises

12 Other Groups

12.1 Finite Fields
12.2 Elliptic Curves
12.3 Quadratic Forms
12.4 Exercises

13 Identification 241
13.1 Passwords 242
13.2 One-Time Passwords 243
13.3 Challenge-Response Identification 243
13.4 Exercises 247

14 Public-Key Infrastructures 249
14.1 Personal Security Environments 249
14.2 Certification Authorities 251
14.3 Certificate Chains 256

References 257

Solutions to the Exercises 261

Index 277