Sadržaj

Predgovor **v**

Sadržaj **vii**

1 Klasična kriptografija **1**
1.1 Osnovni pojmovi 1
1.2 Supstitucijske šifre 5
1.3 Vigenèreova šifra 15
1.4 Playfairova šifra 24
1.5 Hillova šifra 29
1.6 Jednokratna bilježnica 32
1.7 Transpozicijske šifre 34
1.8 Naprave za šifriranje 40
1.8.1 Jeffersonov kotač za šifriranje 40
1.8.2 Hebernov električni stroj za kodiranje 41
1.8.3 ENIGMA 42
1.8.4 Hagelinov stroj M-209 46
1.9 Zadatci 51

2 Moderni simetrični blokovni kriptosustavi **56**
2.1 Data Encryption Standard (DES) 56
2.1.1 Opis algoritma DES-a 57
2.1.2 Svojstva DES-a 64
2.2 Načini djelovanja blokovnih šifri 69
2.3 Kriptoanaliza DES-a 73
2.3.1 Diferencijalna kriptoanaliza 73
2.3.2 Linearna kriptoanaliza 78
2.4 Neke zamjene za DES 81
2.4.1 Trostruki DES 81
2.4.2 IDEA 82
2.4.3 CAST-128 83

2.4.4 RC5 . . . 85
2.5 Advanced Encryption Standard . . . 87
2.6 Zadatci . . . 96

3 Kriptografija javnog ključa 98
3.1 Ideja javnog ključa . . . 98
3.2 Kriptosustavi zasnovani na problemu faktorizacije . . . 102
3.2.1 RSA kriptosustav . . . 102
3.2.2 Kriptoanaliza RSA kriptosustava . . . 105
3.2.3 Rabinov kriptosustav . . . 113
3.3 Kriptosustavi zasnovani na problemu diskretnog logaritma . . . 116
3.3.1 Diffie-Hellmanov protokol za razmjenu ključeva . . . 116
3.3.2 ElGamalov kriptosustav . . . 117
3.3.3 Index calculus metoda . . . 119
3.3.4 Primjena eliptičkih krivulja u kriptografiji . . . 120
3.3.5 Hipereliptičke krivulje . . . 129
3.4 Ostali kriptosustavi s javnim ključem . . . 131
3.4.1 Problem ruksaka . . . 131
3.4.2 McElieceov kriptosustav . . . 133
3.4.3 NTRU kriptosustav . . . 136
3.5 Zadatci . . . 140

4 Kriptografija u praksi 143
4.1 Kriptografske hash funkcije . . . 143
4.1.1 Secure Hash Algorithm . . . 146
4.1.2 MAC kodovi . . . 147
4.2 Generatori slučajnih brojeva . . . 149
4.2.1 Izvori slučajnih bitova . . . 149
4.2.2 Generatori pseudoslučajnih brojeva . . . 150
4.2.3 Analiza sigurnosti generatora . . . 153
4.3 Digitalni potpis . . . 155
4.3.1 Digital Signature Algorithm . . . 156
4.3.2 Elliptic Curve Digital Signature Algorithm . . . 157
4.3.3 Napad zasnovan na paradoksu rođendana . . . 158
4.4 Problem identiteta . . . 160
4.5 Primjer hibridnog kriptosustava: PGP . . . 162
4.6 Zadatci . . . 165

5 Algoritamska teorija brojeva **167**
5.1 Osnovni algoritmi iz teorije brojeva 167
5.1.1 Složenost algoritama 167
5.1.2 Množenje prirodnih brojeva 171
5.1.3 Modularno množenje i potenciranje 174
5.1.4 Euklidov algoritam 179
5.1.5 Kineski teorem o ostatcima 182
5.1.6 Verižni razlomci 184
5.1.7 Kvadratne kongruencije 190
5.1.8 Kvadrati i kvadratni korijeni 195
5.2 Eliptičke krivulje 198
5.2.1 Grupovni zakon 198
5.2.2 Eliptičke krivulje nad $\mathbb{Q}$ 200
5.2.3 Eliptičke krivulje nad konačnim poljima 202
5.2.4 Određivanje reda grupe $E(\mathbb{F}_q)$ 207
5.3 Testiranje i dokazivanje prostosti 211
5.3.1 Distribucija prostih brojeva 211
5.3.2 Pseudoprosti brojevi 213
5.3.3 Dokazivanje prostosti pomoću eliptičkih krivulja 220
5.3.4 Polinomijalni AKS algoritam za dokazivanje prostosti . . 224
5.4 Metode faktorizacije 228
5.4.1 Pollardova ρ metoda 228
5.4.2 Pollardova $p-1$ metoda 230
5.4.3 Faktorizacija pomoću eliptičkih krivulja 231
5.4.4 Metoda verižnog razlomka 233
5.4.5 Metoda kvadratnog sita 236
5.5 Zadatci 240

Bibliografija **244**

Indeks **254**