Sadržaj

SADRŽAJ V

1 LAGANI UVOD U KRIPTOGRAFIJU 13

1.1 OSNOVNI KRIPTOGRAFSKI POJMOVI 13

1.1.1 Osnovni termini *14*

Algoritam (cipher) 15

Osnovni termini 16

Klasifikacija dvosmjernih kriptografskih algoritma 16

Jednosmjerna kriptografska Heš funkcija (Heš algoritam) 19

2 FORMALNI KRIPTOGRAFSKI POJMOVI 21

2.1 GENERATORI SLUČAJNIH I PSEUDOSLUČAJNIH BROJEVA 23

2.2 SIMETRIČNI KLJUČEVI I SIMETRIČNI ALGORITMI 24

2.2.1 Različite vrste simetričnih algoritama *25*

Blokovski algoritmi 25

Protočni algoritmi 26

2.3 BLOKOVSKI SIMETRIČNI KRIPTOGRAFSKI ALGORITMI 27

XOR operacija 27

Supstituciona kutija (S-BOX , Substitution box) 28

Permutaciona kutija (P-BOX, Permutation BOX) 30

2.3.1 Feistelova mreža i SP mreža *32*

2.3.2 Najčešće korišćeni blokovski simetrični algoritmi *36*

2.4 DETALJNA SPECIFIKACIJA ALGORITMA AES 38

2.4.1 Specifikacija i formalna reprezentacija *39*

Standardom definisani AES algoritam i njegove transformacije 39

Ulazi i izlazi 41

Osnovna jedinica ulaza - Bajt 42

Niz bajta 42

Niz Stanje (State) ... 43
Nizovi 32-bitnih riječi u sastavu kolona i kao dijelovi ključa ... 44
Matematičke pretpostavke ... 45
Sabiranje ... 46
Množenje ... 46
Množenje sa x ili množenje ponovljenom operacijom šift ... 47
Množenje konačnih polja pomoću tabela ... 48
Polinomi čiji su koeficijenti u GF(2^8) ... 51
Dijeljenje ... 54
Multiplikativni inverzni elementi ... 54
Transformacije algoritma AES ... 55
Šifrovanje (Transformacija Cipher) ... 56
Transformacija SubBytes() ... 57
Transformacija ShiftRows() ... 60
Transformacija MixColumns() ... 61
Transformacija AddRoundKey() ... 63
Ekspanzija ključeva ... 64
Dešifrovanje (transformacija InvCipher) ... 65
Transformacija InvShiftRows() ... 66
Transformacija InvSubBytes() ... 67
Transformacija InvMixColumns() ... 67
Inverzna transformacija AddRoundKey () ... 69
Dopuna (Padding) ... 69
Osnovne pretpostavke za softversko poboljšanje performansi algoritma AES ... 70
Elementarno ubrzavanje algoritma množenja ... 70
Poboljšavanje performansi AES algoritma pomoću T-tabela ... 72
Bertonijeve ideje za poboljšanje performansi pomoću transponovanja matrice Stanje ... 74
2.5 PROTOČNI SIMETRIČNI KRIPTOGRAFSKI ALGORITMI ... 77
2.5.1 Algoritam RC4 ... 77
Inicijalizacija stanja S ... 78
2.5.2 Algoritam Salsa20 ... 79
Gradivne funkcije algoritma Salsa20 ... 81

Osnovne transformacije algoritma Salsa20 84
2.5.3 Algoritam ChaCha *85*
2.6 KRIPTOGRAFSKI ALGORITMI SA ASIMETRIČNIM KLJUČEVIMA 86
2.6.1 Detaljna specifikacija Algoritma RSA *87*
Matematičke pretpostavke 88
Prosti brojevi 88
Problem rastavljanja na faktore (factoring problem) 88
Kongruencija 88
Šta je Grupa 89
Ojlerova Fi funkcija (Ojlerov *totient*) 90
Fermatov mali teorem 92
Ojlerov teorem 92
Opis algoritma RSA 93
2.6.2 Algoritmi ElGamel i DSA *100*
2.6.3 Algoritam Rabin *100*
2.6.4 Diffie-Hellman (& Merkle) *100*
Prosti brojevi 100
Generatori 101
DH protokol 101

3 KRIPTOGRAFSKI NAČINI RADA (MODES OF OPERATION) 103

3.1 ECB (ELECTRONIC CODEBOOK) MOD 105
3.2 CBC (CIPHER BLOCK CHAINING) MOD 107
3.3 CTR (COUNTER) ILI SIC (SEGMENTED INTEGER COUNTER) NAČIN RADA 110
3.4 OFB (OUTPUT FEEDBACK) NAČIN RADA 112
3.5 CFB (CIPHER FEEDBACK) NAČIN RADA 114
3.6 XEX, XE KONSTRUKCIJE I XTS-AES NAČIN RADA 116

4 RAZMATRANJA MOGUĆNOSTI PARALELIZACIJE KRIPTOGRAFSKOG ALGORITMA AES 119

4.1 PARALELIZACIJA - OSNOVNI KONCEPT 120

4.2 PARALELNO OFB ŠIFROVANJE SA ODLOŽENOM SINHRONIZACIJOM NITI U KOM SE KORISTE XEX I XE KONSTRUKCIJE- FORMALNA REPREZENTACIJA 121

5 KRIPTOGRAFSKE HEŠ FUNKCIJE (HASH) 130

5.1 PRIMJENA KRIPTOGRAFSKIH HEŠ FUNKCIJA 132

5.2 KONSTRUKCIJA MERKLE-DAMGARDA 137

5.3 MD4 HEŠ FUNKCIJA 139

5.4 MD5 HEŠ FUNKCIJA 141

5.5 SHA FAMILIJA HEŠ FUNKCIJA 143

5.5.1 SHA i SHA-1 heš funkcije 143

5.5.2 SHA2 familija heš funkcija 146

5.5.3 SHA3 heš funkcija i spužva (sponge) konstrukcija 146

6 OVJERAVANJE AUTENTIČNOSTI PORUKA (MESSAGE AUTHENTICATION) 149

6.1 MESSAGE AUTHENTICATION CODE (MAC) U FUNKCIJI VERIFIKACIJE AUTENTIČNOSTI PORUKE 151

6.1.1 Heš funkcija ojačana pomoću ključa (konstrukcija sa tajnim prefiksom) 151

6.1.2 Heš funkcija ojačana pomoću ključa (konstrukcija sa tajnim sufiksom) 152

6.1.3 Message authentication code (MAC) funkcija zasnovana na heš funkciji i ključu - HMAC 152

6.1.4 Message authentication code (MAC) funkcije bazirane na blokovskim algoritmima – DAA i CMAC 155

CBC-MAC i Data Authentication Algorithm (DAA) 155

Cipher-Based Message Authentication Code (CMAC) algoritam 157

Poly1305 158

Univerzalna heš funkcija (*universal hash function*) 159

Vegman-Karter konstrukcija (Wegman–Carter construction) 159

Poly1305-AES 160

6.2 AUTENTIFIKOVANA ENKRIPCIJA (AUTHENTICATED ENCRYPTION ILI AE) – CCM I GCM 161
6.2.1 CCM mod (CTR/CBC-MAC) odnosno Counter with Cipher Block Chaining-Message Authentication Code 163
6.2.2 Galois/Counter Mode ili GCM način rada 164
7 DIGITALNI POTPIS 167
7.1 ALGORITAM DSA - DIGITAL SIGNATURE ALGORITHM 169
7.2 ALGORITAM ECDSA – ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM 169
8 KRIPTOGRAFIJA ELIPTIČNE KRIVE 170
8.1 „NJEŽNI" UVOD U KRIPTOGRAFIJU ELIPTIČNE KRIVE 170
8.2 KRIPTOGRAFIJA ELIPTIČNE KRIVE 176
8.2.1 Kriva Curve25519 182
9 VJEŽBE 185
9.1 VJEŽBA: JAVA I POTREBNE KRIPTOGRAFSKE BIBLIOTEKE I TEHNOLOGIJE 185
9.1.1 Noseće (engine) klase i algoritmi 187
Transparentne i neprozirne (opaque) specifikacije ključeva 188
9.1.2 Osnovne (core) klase i algoritmi 189
9.2 VJEŽBA: KRIPTOGRAFSKA BIBLIOTEKA BOUNCY CASTLE 189
9.2.1 Vježba: Priprema za instalaciju kriptografskih paketa 190
Instalacija Java JDK 8 190
Instalacija Java SE Development Kit 12 i OpenJDK 12 192
9.2.2 Vježba: Instalacija kriptografske biblioteke Bouncy Castle .. 193
9.2.3 Vježba: Program CSPLista 197
9.3 VJEŽBA: INSTALACIJA JAVA UNLIMITED STRENGTH JURISDICTION POLICY FILES 198
9.3.1 Vježba: Program TestUnlimited 199
9.4 PROGRAM SVIALGORITMI 200

9.5 PROGRAM HEXUTILSTEST – NEMOJTE GA PRESKOČITI! 202
9.6 PROGRAM BCHEXDECODE 208
9.7 PROGRAM DATATYPECONVERTOR 210
9.8 PRIMJENA OPERACIJE XOR U KRIPTOGRAFIJI 214
9.8.1 Program XorKarakteri 214
9.8.2 Program XorInteger 216
9.8.3 Program XorBinarno 217
9.8.4 Program SimerticniBlokovskiXor 218
9.9 GRADIVNI ELEMENTI - PRIMJENA SUPSTITUCIJE I PERMUTACIJE U KRIPTOGRAFIJI 220
9.9.1 Program MiniSBox 221
9.9.2 Program MiniSBox2 222
9.9.3 Program AesSbox 224
9.9.4 Program PBox 227
9.9.5 Program AesShiftRows 228
9.9.6 Program AesInvShiftRows 231
9.9.7 Program KeyExpand 233
9.9.8 Program SpMreza 234
9.10 BLOKOVI PODATAKA I UČITAVANJE DATOTEKE U FRAGMENTIMA 238
9.10.1 Program OcitajObradiDatoteku 239

10 RAD SA KLJUČEVIMA 240

10.1 PROGRAM KEYGENERATOR1 240
10.2 PROGRAM KEYGENERATOR2 242
10.3 PROGRAM KEYPAIRGENERATOR1 243
10.4 PROGRAM KEYPAIRGENERATOR2 245
10.5 PROGRAM KEYPAIRGENERATOR3 247
10.6 PROGRAM KEYAGREEMENTDHTEST 250

11 SIMETRIČNI ALGORITMI 253

11.1 PROGRAM AESDATOTEKACIP 253

11.2 PROGRAM AESDATOTEKAINVCIP 257
11.3 PROGRAM AESDATOTEKACIPINVCIPBC 259
11.4 PROGRAM AESDATOTEKACIPINVCIPBC256 261
11.5 PROGRAM DES 263
11.6 PROGRAM DESINV 265
11.7 PROGRAM CHACHABUFF 266
11.8 PROGRAM CHACHADATOTEKA 268
11.9 PROGRAM BLOWFISHDATOTEKA 270
11.10 PROGRAM BLOWFISHINVDATOTEKA 272
11.11 PROGRAM TWOFISH 273
11.12 PROGRAM DESSECRETKEYFACTORY 275
11.13 PRIMJENA RAZLIČITIH KRIPTOGRAFSKIH NAČINA RADA 276
11.13.1 Program AesDatotekaCTR 276
11.13.2 Program AesDatotekaCTRInv 279
11.13.3 Program AesDatotekaCBC 280
11.13.4 Program AesBuffCfb 282

12 ASIMETRIČNI ALGORITMI 285

12.1 PROGRAM RSASTRING 285
12.2 PROGRAM ELGAMALSTRING 286

13 KRIPTOGRAFSKE HEŠ FUNKCIJE I DIGITALNI POTPISI .. 289

13.1 PROGRAM ISPISHESALGORITAMA 289
13.2 PROGRAM SHA256 292
13.3 PROGRAM ISPISDIGPOTPISA 293
13.4 PROGRAM ISPISALIASADIGPOTPISA 295
13.5 PROGRAM DIGITALNIPOTPISI 297

14 ZAKLJUČAK 301

15 BIBLIOGRAFIJA 303