Sadržaj

Uvodna reč Vitfilda Difija xv
Predgovor xix
KAKO TREBA ČITATI OVU KNJIGU *xx*
O autoru xxiii

1 OSNOVE 1

1.1 TERMINOLOGIJA *1*
1.2 STEGANOGRAFIJA *9*
1.3 SUPSTITUCIONE ŠIFRE I TRANSPOZICIONE ŠIFRE *10*
1.4 OBIČAN XOR ALGORITAM *13*
1.5 JEDNOKRATNA BELEŽNICA *15*
1.6 RAČUNARSKI ALGORITMI *17*
1.7 VELIKI BROJEVI *17*

DEO I KRIPTOGRAFSKI PROTOKOLI

2 GRADIVNI ELEMENTI PROTOKOLA *21*

2.1 UVOD U PROTOKOLE *21*
2.2 KOMUNIKACIJA POMOĆU SIMETRIČNE KRIPTOGRAFIJE *27*
2.3 JEDNOSMERNE FUNKCIJE *29*
2.4 JEDNOSMERNE HEŠ FUNKCIJE *29*
2.5 KOMUNIKACIJA UZ PRIMENU KRIPTOGRAFIJE S JAVNIM KLJUČEM *31*
2.6 DIGITALNI POTPISI *34*
2.7 DIGITALNI POTPISI SA ŠIFROVANJEM *40*
2.8 GENERISANJE SLUČAJNIH I PSEUDOSLUČAJNIH SEKVENCI *43*

3 OSNOVNI PROTOKOLI *47*
3.1 Razmena ključeva *47*
3.2 Provera identiteta *52*
3.3 Provera identiteta i razmena ključeva *56*
3.4 Formalna analiza protokola za proveru identiteta i razmenu ključeva *65*
3.5 Više ključeva u kriptografiji s javnim ključem *68*
3.6 Tajno rastavljanje poruke *70*
3.7 Deljenje tajne *71*
3.8 Kriptografska zaštita baza podataka *73*

4 PROTOKOLI SREDNJE SLOŽENOSTI *75*
4.1 Usluge vremenskog označavanja *75*
4.2 Skriveni kanal *79*
4.3 Neporecivi digitalni potpisi *81*
4.4 Potpisi sa izabranim overiocem *82*
4.5 Posrednički potpisi *83*
4.6 Grupni potpisi *84*
4.7 Digitalni potpisi otporni na prevaru *85*
4.8 Računanje sa šifrovanim podacima *86*
4.9 Predavanje bita *86*
4.10 Pošteno bacanje novčića *89*
4.11 Misaoni poker *92*
4.12 Jednosmerni akumulatori *95*
4.13 Otkrivanje tajni „sve ili ništa“ *96*
4.14 Deponovanje ključa *97*

5 NAPREDNI PROTOKOLI *101*
5.1 Dokazi bez otkrivanja dodatnih informacija *101*
5.2 Dokazivanje identiteta bez otkrivanja dodatnih informacija *109*
5.3 Slepi potpisi *112*
5.4 Kriptografija s javnim ključem zasnovana na identitetu *115*
5.5 Nesvesni prenos *115*
5.6 Nesvesni potpisi *117*
5.7 Istovremeno potpisivanje ugovora *117*
5.8 Digitalna sertifikovana pošta *122*
5.9 Istovremena razmena tajni *123*

6 EZOTERIČNI PROTOKOLI *125*
6.1 Bezbedno glasanje *125*
6.2 Bezbedno izračunavanje s više učesnika *134*
6.3 Anonimno objavljivanje poruke *137*
6.4 Digitalni novac *139*

DEO II KRIPTOGRAFSKE TEHNIKE

7 DUŽINA KLJUČA *151*
7.1 Dužina simetričnog ključa *151*
7.2 Dužina ključeva za algoritme s javnim ključem *158*
7.3 Upoređivanje dužina ključeva simetričnih algoritama i algoritama s javnim ključem *165*
7.4 Rođendanski napadi na jednosmerne heš funkcije *165*
7.5 Koliko dugačak treba da bude ključ? *166*
7.6 Važno upozorenje *167*

8 UPRAVLJANJE KLJUČEVIMA *169*
8.1 Generisanje ključeva *170*
8.2 Nelinearni prostori ključeva *175*
8.3 Prenos ključeva *176*
8.4 Provera ključeva *178*
8.5 Korišćenje ključeva *179*
8.6 Ažuriranje ključeva *180*
8.7 Skladištenje ključeva *181*
8.8 Rezervne kopije ključeva *181*
8.9 Kompromitovani ključevi *182*
8.10 Rok važenja ključeva *183*
8.11 Uništavanje ključeva *185*
8.12 Upravljanje ključevima u kriptografiji s javnim ključem *185*

9 TIPOVI I REŽIMI ALGORITAMA *189*
9.1 Režim ECB *190*
9.2 Ponavljanje bloka *191*
9.3 Režim CBC *193*
9.4 Šifre toka *197*
9.5 Samosinhronizujuće šifre toka *199*
9.6 Režim CFB *200*
9.7 Sinhrone šifre toka *202*
9.8 Režim OFB *203*
9.9 Brojački režim *205*
9.10 Ostali režimi blokovskih šifara *206*
9.11 Izbor šifarskog režima *208*
9.12 Preplitanje *210*
9.13 Upoređivanje blokovskih šifara i šifara toka *210*

10 PRIMENA ALGORITAMA *213*
10.1 Izbor algoritma *214*
10.2 Poređenje kriptografije s javnim ključem i simetrične kriptografije *216*

10.3 Šifrovanje komunikacionih kanala *217*
10.4 Šifrovanje podataka za skladištenje *220*
10.5 Poređenje hardverskog i softverskog šifrovanja *223*
10.6 Kompresija, kodiranje i šifrovanje *225*
10.7 Otkrivanje šifrovanja *226*
10.8 Skrivanje šifrata u šifratu *226*
10.9 Uništavanje informacija *228*

DEO III KRIPTOGRAFSKI ALGORITMI

11 MATEMATIČKE OSNOVE *231*
11.1 Teorija informacija *231*
11.2 Teorija složenosti *235*
11.3 Teorija brojeva *240*
11.4 Faktorisanje *253*
11.5 Generisanje prostih brojeva *256*
11.6 Diskretni logaritmi u konačnom polju *259*

12 DATA ENCRYPTIONSTANDARD (DES) *263*
12.1 Osnove *263*
12.2 Opis standarda DES *268*
12.3 Sigurnost algoritma DES *276*
12.4 Diferencijalna i linearna kriptoanaliza *283*
12.5 Stvarni kriterijumi projektovanja *291*
12.6 Varijante algoritma DES *292*
12.7 Koliko je DES danas siguran? *296*

13 OSTALE BLOKOVSKE ŠIFRE *299*
13.1 Lucifer *299*
13.2 Madryga *300*
13.3 NewDES *302*
13.4 FEAL *304*
13.5 REDOC *307*
13.6 LOKI *310*
13.7 Khufu i Khafre (tj. Keops i Kefren) *312*
13.8 RC2 *314*
13.9 IDEA *315*
13.10 MMB *321*
13.11 CA-1.1 *323*
13.12 Skipjack *324*

14 JOŠ NEKE BLOKOVSKE ŠIFRE *327*
14.1 GOST *327*
14.2 CAST *330*

14.3 Blowfish *332*
14.4 SAFER *335*
14.5 3-Way *338*
14.6 Crab *338*
14.7 SXAL8/MBAL *340*
14.8 RC5 *340*
14.9 Ostali blokovski algoritmi *342*
14.10 Teorija projektovanja blokovskih šifara *342*
14.11 Primena jednosmernih heš funkcija *347*
14.12 Izbor blokovskog algoritma *350*

15 KOMBINOVANJE BLOKOVSKIH ŠIFARA *353*

15.1 Dvostruko šifrovanje *353*
15.2 Trostruko šifrovanje *355*
15.3 Udvostručavanje dužine bloka *359*
15.4 Druge šeme višestrukog šifrovanja *360*
15.5 Skraćivanje ključeva u CDMF *362*
15.6 Izbeljivanje *363*
15.7 Kaskadiranje više blokovskih algoritama *363*
15.8 Kombinovanje više blokovskih algoritama *364*

16 GENERATORIPSEUDOSLUČAJNIH SEKVENCI I ŠIFRE TOKA *365*

16.1 Linearni kongruentni generatori *365*
16.2 Linearni pomerački registri s povratnom spregom *369*
16.3 Projektovanje i analiza šifara toka *376*
16.4 Šifre toka sa LFS registrima *377*
16.5 A5 *385*
16.6 Hughes XPD/KPD *386*
16.7 Nanoteq *386*
16.8 Rambutan *387*
16.9 Aditivni generatori *387*
16.10 Gifford *389*
16.11 Algoritam M *390*
16.12 PKZIP *390*

17 OSTALE ŠIFRE TOKA I PRAVI GENERATORI SLUČAJNIH SEKVENCI *393*

17.1 RC4 *393*
17.2 SEAL *394*
17.3 WAKE *397*
17.4 Pomerački registri s povratnom spregom i prenosom *398*
17.5 Šifre toka sa FCS registrima *401*
17.6 Nelinearni pomerački registri s povratnom spregom *408*
17.7 Ostale šifre toka *409*

17.8 Pristup projektovanju šifara toka sa stanovišta teorije sistema *411*
17.9 Pristup projektovanju šifara toka sa stanovišta teorije složenosti *412*
17.10 Ostali pristupi projektovanju šifara toka *414*
17.11 Kaskadiranje više šifara toka *416*
17.12 Izbor šifre toka *416*
17.13 Generisanje više tokova jednim generatorom slučajne sekvence *417*
17.14 Pravi generatori slučajnih sekvenci *418*

18 JEDNOSMERNE HEŠ FUNKCIJE *425*

18.1 Osnove *425*
18.2 Snefru *427*
18.3 N-Hash *428*
18.4 MD4 *430*
18.5 MD5 *432*
18.6 MD2 *437*
18.7 Secure Hash Algorithm (SHA) *438*
18.8 RIPE-MD *441*
18.9 HAVAL *441*
18.10 Ostale jednosmerne heš funkcije *442*
18.11 Simetrični blokovski algoritmi kao jednosmerne heš funkcije *442*
18.12 Primena algoritama s javnim ključem *451*
18.13 Izbor jednosmerne heš funkcije *451*
18.14 Kodovi za proveru identiteta poruke *451*

19 ALGORITMI S JAVNIM KLJUČEM *457*

19.1 Osnove *457*
19.2 Algoritmi zasnovani na problemu ranca *458*
19.3 Algoritam RSA *462*
19.4 Algoritam Pohlig–Hellman *470*
19.5 Algoritam Rabin *471*
19.6 Algoritam ElGamal *472*
19.7 Algoritam McEliece *475*
19.8 Kriptosistemi zasnovani na eliptičnim krivama *476*
19.9 Algoritam LUC *477*
19.10 Kriptosistemi s javnim ključem zasnovani na konačnom automatu *478*

20 ALGORITMI ZA DIGITALNO POTPISIVANJE S JAVNIM KLJUČEM *479*

20.1 Algoritam za digitalno potpisivanje (DSA) *479*
20.2 Varijante algoritma DSA *489*
20.3 Algoritam GOST za digitalno potpisivanje *490*
20.4 Šeme digitalnih potpisa zasnovane na diskretnom logaritmu *491*
20.5 Ong–Schnorr–Shamir *494*

20.6 ESIGN *494*
20.7 Ćelijski automati *496*
20.8 Ostali algoritmi s javnim ključem *496*

21 IDENTIFIKACIONE ŠEME *499*
21.1 Feige-Fiat-Shamir *499*
21.2 Guillou–Quisquater *504*
21.3 Schnorr *506*
21.4 Konverzija identifikacionih šema u šeme za potpisivanje *508*

22 ALGORITMI ZA RAZMENU KLJUČEVA *509*
22.1 Diffie–Hellman *509*
22.2 Protokol stanica–stanica *512*
22.3 Šamirov troprolazni protokol *512*
22.4 COMSET *514*
22.5 Razmena šifrovanih ključeva (EKE) *514*
22.6 Zaštićeni pregovori o ključu *518*
22.7 Distribucija konferencijskog ključa i tajno objavljivanje *519*

23 SPECIJALNI ALGORITMI ZA PROTOKOLE *525*
23.1 Više ključeva u kriptografiji s javnim ključem *525*
23.2 Algoritmi za deljenje tajni *526*
23.3 Skriveni kanal *529*
23.4 Neporecivi digitalni potpisi *534*
23.5 Potpisi sa izabranim overiocem *537*
23.6 Računanje sa šifrovanim podacima *538*
23.7 Pošteno bacanje novčića *539*
23.8 Jednosmerni akumulatori *541*
23.9 Otkrivanje tajni „sve ili ništa“ *542*
23.10 Pošteni kriptosistemi i kriptosistemi sigurni u slučaju otkaza *544*
23.11 Dokazi bez otkrivanja dodatnih informacija *546*
23.12 Slepi potpisi *548*
23.13 Nesvesni prenos *548*
23.14 Bezbedno izračunavanje s više učesnika *549*
23.15 Probabilističko šifrovanje *551*
23.16 Kvantna kriptografija *553*

DEO IV STVARNI SVET

24 PRIMERI REALIZACIJA *557*
24.1 Protokol za upravljanje tajnim ključem kompanije IBM *557*
24.2 MITRENET *558*
24.3 ISDN *559*

24.4 STU-III *561*
24.5 Kerberos *562*
24.6 KryptoKnight *567*
24.7 SESAME *568*
24.8 Common Cryptographic Architecture (CCA) kompanije IBM *568*
24.9 Radni okvir za proveru identiteta organizacije ISO *569*
24.10 Privacy-Enhanced Mail (PEM) *573*
24.11 Protokol za sigurnost poruke (MSP) *579*
24.12 Pretty Good Privacy (PGP) *580*
24.13 Pametne kartice *582*
24.14 Standardi kriptografije s javnim ključem (PKCS) *583*
24.15 Univerzalni sistem za elektronsko plaćanje (UEPS) *585*
24.16 Clipper *586*
24.17 Capstone *589*
24.18 Bezbedni telefonski uređaj (TSD) AT&T Model 3600 *590*

25 POLITIKA *591*

25.1 Nacionalna agencija za bezbednost (NSA) *591*
25.2 Nacionalni centar za računarsku sigurnost (NCSC) *593*
25.3 Nacionalni institut za standarde i tehnologiju (NIST) *594*
25.4 RSA Data Security, Inc. *597*
25.5 Public Key Partners *598*
25.6 Međunarodno udruženje za kriptološka istraživanja (IACR) *599*
25.7 RACE ocena integriteta primitiva (RIPE) *599*
25.8 Uslovni pristup za Evropu (CAFE) *600*
25.9 ISO/IEC 9979 *601*
25.10 Profesionalne grupe, grupe za zaštitu ljudskih prava i industrijske grupe *601*
25.11 Sci.crypt *602*
25.12 Cypherpunks *603*
25.13 Patenti *603*
25.14 Zakoni SAD o izvozu *604*
25.15 Stavovi drugih zemalja o uvozu i izvozu kriptografije *610*
25.16 Pravna pitanja *611*

Pogovor Meta Blejza 613

DEO V IZVORNI KÔD

Izvorni kôd 617
Reference 669
Spisak termina korišćenih u knjizi 741
Indeks 749