Predgovor

Postoje dve vrste kriptografije na ovom svetu: kriptografija koja će sprečiti vašu mlađu sestru da čita vaše datoteke i kriptografija koja će sprečiti vlade velikih zemalja da čitaju vaše datoteke. Ovo je knjiga o onoj drugoj kriptografiji.

Ako uzmem pismo, zaključam ga u sef, sakrijem taj sef negde u Njujorku, a zatim vam kažem da pročitate pismo, to nije sigurnost. To je nejasan zadatak. S druge strane, ako uzmem pismo i zaključam ga u sef, a zatim vam dam taj sef, njegovu projektnu dokumentaciju i sto identičnih sefova s njihovim kombinacijama, tako da najbolji svetski obijači sefova mogu da prouče mehanizam za zaključavanje, a vi i dalje ne možete da otvorite sef i pročitate pismo – to jeste sigurnost.

Tokom dugog niza godina, ova vrsta kriptografije bila je u isključivoj nadležnosti vojske. Nacionalna agencija za bezbednost SAD i odgovarajuće institucije u bivšem Sovjetskom Savezu, Engleskoj, Francuskoj, Izraelu i na drugim mestima, potrošile su milijarde dolara u veoma ozbiljnoj igri obezbeđivanja sopstvenih komunikacija i pokušaja provaljivanja u sve ostale. Pojedinci, s mnogo manje znanja i sredstava, nisu imali moć da zaštite sopstvenu privatnost od tih vlada.

Tokom poslednjih 20 godina, naglo se razvilo javno akademsko istraživanje kriptografije. Dok su obični građani dugo koristili klasičnu kriptografiju, računarska kriptografija je, od Drugog svetskog rata, bila isključivo u vojnoj nadležnosti raznih država. Danas se moderna računarska kriptografija primenjuje izvan zaštitnih zidina vojnih agencija. Sada je laik u stanju da primeni sigurnosne mere koje mogu da ga zaštite od najmoćnijih neprijatelja, a to u predstojećim godinama znači sigurnost od vojnih službi.

Da li je prosečnim ljudima zaista potrebna ova vrsta sigurnosti? Da. Mogu da planiraju političku kampanju, raspravljaju o porezima ili se upuštaju u nedozvoljene aktivnosti. Oni mogu da prave neki nov proizvod, razmatraju tržišnu strategiju ili planiraju preotimanje posla. Ili, možda žive u državama koje ne poštuju prava na privatnost svojih građana. Možda se oni bave nečim za šta osećaju da ne bi trebalo da bude nezakonito, ali jeste. Koji god da je razlog, podaci i komunikacije su lični, privatni i ne tiču se drugih.

Ova knjiga se objavljuje u burnim vremenima. Klintonova administracija je 1994. usvojila Escrowed Encryption Standard (uključujući čip Clipper i karticu Fortezza) i uvrstila u zakon dokument o digitalnoj telefoniji. Oba ova programa predstavljaju pokušaj da se vladi osigura mogućnost sprovođenja elektronske kontrole.

Ovde su na delu neke opasne orvelovske pretpostavke: vlada ima pravo da prisluškuje privatne komunikacije i nešto nije u redu ako građanin pokušava da sačuva neku tajnu od vlade. Primenom zakona, uvek je bilo moguće sprovesti nadzor koji će sud odobriti, ako je to ostvarivo, ali su sada prvi put ljudi primorani da preduzimaju aktivne mere da bi *sebe učinili dostupnim* za nadzor. Ove inicijative nisu obični predlozi vlade u nekoj nejasnoj oblasti, već su to prvi i jednostrani pokušaji da se osvoje prava koja su nekada pripadala građanima.

Clipper i digitalna telefonija ne štite privatnost, nego primoravaju pojedince da bezuslovno veruju kako će vlada poštovati njihovu privatnost. Iste institucije za sprovođenje zakona, koje su bespravno prisluškivale telefone Martina Lutera Kinga Mlađeg, lako mogu da prisluškuju telefon koji je zaštićen čipom Clipper. U nedavnoj prošlosti, lokalne policijske vlasti su krivično ili civilno tužene za bespravno prisluškivanje telefona, u brojnim procesima (Merilend, Konektikat, Vermont, Džordžija, Misuri i Nevada). Loša je ideja da se instalira tehnologija koja bi jednoga dana mogla da olakša uvođenje policijske države.

Odavde se može naučiti da nije dovoljno zaštititi se zakonima, nego se valja štititi matematikom. Šifrovanje je previše značajno da bi bilo prepušteno isključivo državnoj upravi.

Ova knjiga vam daje oruđa kojima ćete zaštititi svoju privatnost: kriptografski proizvodi se mogu proglasiti nezakonitim, ali ne i informacije.

KAKO TREBA ČITATI OVU KNJIGU

Napisao sam *Primenjenu kriptografiju* tako da bude i živopisan uvod u oblast kriptografije i sveobuhvatan pregled. Pokušao sam da očuvam čitljivost teksta bez umanjivanja preciznosti. Nije predviđeno da ova knjiga bude matematički tekst. Iako nisam namerno dao nikakve pogrešne informacije, kroz teoriju prolazim brzo i nemarno. U akademskoj literaturi postoje brojne reference za one koji su zainteresovani za formalizam.

U poglavlju 1 uvodi se kriptografija, definišu se mnogi termini i ukratko se razmatra stanje u oblasti kriptografije pre početka korišćenja računara.

U poglavljima od 2 do 6 (I deo) opisuju se kriptografski protokoli: šta ljudi mogu da urade pomoću kriptografije. Opisani protokoli su u opsegu od jednostavnih (jedna osoba šalje šifrovane poruke drugoj), preko složenih (bacanje novčića preko telefona), do ezoteričnih (sigurna i anonimna razmena digitalnog novca). Neki od navedenih protokola su očigledni, a drugi su skoro začuđujući. Kriptografija može da reši mnoge probleme za koje većina ljudi nikada nije verovala da će biti rešeni.

U poglavljima od 7 do 10 (II deo) razmatraju se kriptografske tehnike. Sva četiri poglavlja ovog dela značajna su čak i za osnovne primene kriptografije. Poglavlja 7 i 8 su o ključevima: koliko ključ treba da bude dugačak da bi bio siguran, kako generisati ključeve, kako ih čuvati, kako se osloboditi ključeva i tako dalje. Upravljanje ključevima je najteži deo kriptografije i često je to Ahilova peta sistema koji je inače siguran. U poglavlju 9 razmatraju se različiti načini korišćenja kriptografskih algoritama, a poglavlje 10 bavi se preostalim temama: kako izabrati, realizovati i koristiti algoritme.

U poglavljima od 11 do 23 (III deo) nabrojani su algoritmi. Poglavlje 11 daje matematičke osnove. Ovo poglavlje pročitajte samo ako ste zainteresovani za algoritme s javnim ključem. Ukoliko vas zanima samo primena algoritma DES (ili nekog sličnog), preskočite ovo poglavlje. U poglavlju 12 opisan je algoritam DES: njegova istorija, njegova sigurnost i neke varijante. U poglavljima 13, 14 i 15 opisani su drugi blokovski algoritmi: ako hoćete nešto što je sigurnije od algoritma DES, pređite na odeljak o algoritmima IDEA i trostrukom DES-u. Ukoliko hoćete da čitate o grupi algoritama, od kojih neki mogu da budu sigurniji nego što je DES, pročitajte celo poglavlje.

Poglavlja 16 i 17 opisuju algoritme toka. Poglavlje 18 opisuje jednosmerne heš funkcije: najčešće se koriste MD5 i SHA, mada se bavim i mnogim drugim. U poglavlju 19 opisani su algoritmi za šifrovanje s javnim ključem, u poglavlju 20 – algoritmi za digitalno potpisivanje s javnim ključem. Poglavlje 21 razmatra algoritme za identifikaciju s javnim ključem, a poglavlje 22 – algoritme za razmenu ključeva s javnim ključem. Značajni algoritmi su: RSA, DSA, Fiat–Shamirov i Diffie–Hellmanov. Poglavlje 23 obuhvata neobičnije algoritme i protokole s javnim ključem, a matematička osnova ovog poglavlja prilično je komplikovana, pa vežite pojaseve.

Poglavlja 24 i 25 (IV deo) okreću se stvarnom svetu kriptografije. U poglavlju 24 opisan je izvestan broj trenutnih realizacija ovih algoritama i protokola, dok poglavlje 25 dotiče neka politička pitanja koja okružuju kriptografiju. Nije predviđeno da ova poglavlja budu iscrpna u bilo kom pogledu.

U knjizi su dati i listinzi – izvorni kôd 10 algoritama opisanih u III delu. S obzirom na prostorna ograničenja, nisam mogao da navedem sav izvorni kôd koji sam hteo, a kriptografski izvorni kôd ne može se – u vreme pisanja ove knjige – izvesti na drugi način. (Čudi me kako je Ministarstvo unutrašnjih poslova dozvolilo izvoz prvog izdanja ove knjige sa izvornim kodom, ali je zabranilo izvoz diska s potpuno istim kodom. Pokušajte da izvedete zaključak.) Pridruženi skup diskova sa izvornim kodom sadrži mnogo više koda nego što je moglo da stane u knjigu i to je verovatno najveća kolekcija kriptografskog izvornog koda izvan neke vojne institucije. Diskove sa izvornim kodom mogu da šaljem samo američkim i kanadskim građanima koji žive u Sjedinjenim Državama i Kanadi, ali se nadam da će se to jednoga dana promeniti. (Na Web lokaciji ove knjige piše da više nema restrikcija za slanje ovog diska van SAD i Kanade. Prim. red.) Ako hoćete da koristite kriptografske algoritme iz ove knjige ili da se s njima igrate, nabavite disk. Više detalja potražite na kraju knjige.

Jedna od primedbi na ovu knjigu jeste da njena enciklopedijska priroda umanjuje čitljivost. To jeste tačno, ali sam hteo da obezbedim referentni priručnik onima koji naiđu na neki algoritam u akademskoj literaturi ili nekom proizvodu. Izvinjavam se onima kojima je potrebnije uputstvo za rad. Mnogo posla je urađeno na polju kriptografije, a ovo je prvi put da se tako veliki deo toga našao između dve korice. Ipak, problemi sa obimom knjige primorali su me da mnoge stvari izostavim. Obradio sam teme koje sam smatrao važnim, primenljivim ili zanimljivim. Ako neku temu nisam mogao detaljno da razradim, ukazao sam na odgovarajuće članke i radove.

Dao sam sve od sebe da pronađem i uklonim sve greške iz ove knjige, ali su me mnogi uverili da je to nemoguć zadatak. U svakom slučaju, drugo izdanje ima mnogo manje grešaka nego prvo. Od mene se može dobiti spisak grešaka, koji periodično šaljem Usenet diskusionoj grupi sci.crypt. Ako neki čitalac uoči grešku, neka me o tome obavesti. Svakoj osobi koja prva pronađe neku grešku u knjizi, poslaću besplatan primerak diska sa izvornim kodom. (Na Web lokaciji ove knjige nalazi se spisak svih do sada uočenih grešaka. Spisak se povremeno ažurira. Prim. red.)

Zahvalnice

Spisak ljudi koji su zaslužni za ovu knjigu deluje kao da je beskonačan, ali su svi oni vredni da budu spomenuti. Moju zahvalnost zaslužuju Don Alvarez, Ross Anderson, Dave Balenson, Karl Barrus, Steve Bellovin, Dan Bernstein, Eli Biham, Joan Boyar, Karen Cooper, Whit Diffie, Joan Feigenbaum, Phil Karn, Neal Koblitz, Xuejia Lai, Tom

Leranth, Mike Markowitz, Ralph Merkle, Bill Patton, Peter Pearson, Charles Pfleeger, Ken Pizzini, Bart Preneel, Mark Riordan, Joachim Schurman i Marc Schwartz, za čitanje i uređivanje celine ili delova prvog izdanja, Marc Vauclair za prevođenje prvog izdanja na francuski, Abe Abraham, Ross Anderson, Dave Banisar, Steve Bellovin, Eli Biham, Matt Bishop, Matt Blaze, Gary Carter, Jan Comenisch, Claude Crépeau, Joan Daemen, Jorge Davila, Ed Dawson, Whit Diffie, Carl Ellison, Joan Feigenbaum, Niels Ferguson, Matt Franklin, Rosario Gennaro, Dieter Gollmann, Mark Goresky, Richard Graveman, Stuart Haber, Jingman He, Bob Hogue, Kenneth Iversen, Markus Jakobsson, Burt Kaliski, Phil Karn, John Kelsey, John Kennedy, Lars Knudsen, Paul Kocher, John Ladwig, Xuejia Lai, Arjen Lenstra, Paul Leyland, Mike Markowitz, Jim Massey, Bruce McNair, William Hugh Murray, Roger Needham, Clif Neuman, Kaisa Nyberg, Luke O'Connor, Peter Pearson, René Peralta, Bart Preneel, Yisrael Radai, Matt Robshaw, Michael Roe, Phil Rogaway, Avi Rubin, Paul Rubin, Selwyn Russell, Kazue Sako, Mahmoud Salmasizadeh, Markus Stadler, Dmitry Titov, Jimmy Upton, Marc Vauclair, Serge Vaudenay, Gideon Yuval, Glen Zorn i nekoliko anonimnih službenika vlade, za čitanje i korigovanje celine ili delova drugog izdanja, pa Lawrie Brown, Leisa Condie, Joan Daemen, Peter Gutmann, Alan Insley, Chris Johnston, John Kelsey, Xuejia Lai, Bill Leininger, Mike Markowitz, Richard Outerbridge, Peter Pearson, Ken Pizzini, Colin Plumb, RSA Data Security, Inc., Michael Roe, Michael Wood i Phil Zimmermann, koji su obezbedili izvorni kôd, Paul MacNerland koji je napravio slike za prvo izdanje, Karen Cooper koja je pripremila za štampu drugo izdanje, Beth Friedman koja je pregledala drugo izdanje, Carol Kennedy koja je napravila indeks za drugo izdanje, čitaoci diskusione grupe sci.crypt i liste slanja *Cypherpunks* koji su davali komentare, odgovarali na pitanja i pronalazili greške u prvom izdanju, Randy Seuss koji je omogućio pristup preko Interneta, Jeff Duntemann i Jon Erickson koji su mi pomogli da započnem posao, Insleyievi koji su mi pružili motivaciju, ohrabrenje, podršku, razgovore, prijateljstvo i večere, kao i kompanija AT&T Bell Labs koja me je otpustila i sve ovo učinila mogućim. Svi ovi ljudi su pomogli da nastane mnogo bolja knjiga od one koju bih napravio sam.

Brus Šnajer
Ouk Park, Illinois
schneier@counterpane.com