Sadržaj:

1 2
1
1 Uvod
“Why I Wrote PGP” by Philip Zimmermann, Part of the Original 1991 PGP User's Guide (updated in 1999)
Ovim se riječima Philip Zimmermann, tvorac PGP-a, obratio svijetu. Vjerovao je da je zaštita privatnosti ljudsko pravo. U doba kada nas svjetske sile i korporacije mogu locirati bilo gdje na zemlji, kada svaki telefonski poziv može biti prisluškivan, kada se mailovi korisnika provlače kroz računala u potrazi za ključnim riječima, zaštita podataka i privatnosti nam omogućuje zaštitu slobode govora. U doba kada je kra a identiteta i ideja suparničkih tvrtki sve popularnija kriptografija postaje zaštitom sloboda.
2
2 Kriptografija
2.1 Uvod u kriptografiju
Kriptografiju možemo definirati kao znanost korištenja matematike za šifriranje i dešifriranje podataka. Ona omogućuje sigurno spremanje tajnih podataka ili sigurno slanje tih istih podataka preko nezaštićenog komunikacijskog kanala, pritom osiguravajući da nitko nema pristup tim podacima osim onog kome su namijenjeni.
Kriptografija svoje početke bilježi još u vremenu prije Krista. Naznake korištenja nekih kriptografskih metoda se javljaju već oko 4000. godine pr.n.e., naravno u njihovom najprimitivnijem obliku jer u to vrijeme kriptografija nije korištena toliko za očuvanje tajnosti podataka koliko za misteriozniji prikaz istih. Iz tog razloga nije bilo ni potrebe za razvijanjem kompliciranijih metoda kriptiranja, pa je veći razvoj kriptografije počeo tek u srednjem vijeku. Kao primjer jedne od jednostavnijih metoda kriptiranja možemo navesti način na koji je Cezar kriptirao poruke za svoje generale da ih ne bi razumjeli glasnici: jednostavno je koristio metodu zamjene slova iz abecede drugim slovima po principu rotacije za tri mjesta. Tako je svako slovo A zamijenjeno slovom D, svako slovo B slovom E itd. Na tom principu su se zasnivale sve primitivne metode kriptiranja.
Kao što je već spomenuto kriptografija se počela značajnije razvijati u srednjem vijeku, ali „zlatno doba“ razvoja kriptografske znanosti je 20.stoljeće kada je nagli napredak u tehnologiji značajno potpomogao razvoj kompliciranijih kripto-metoda time što je omogućio izvo enje najkompliciranijih matematičkih operacija u vrlo kratkom vremenu istovremeno donoseći i veću potrebu za tajnošću i zaštitom podataka.