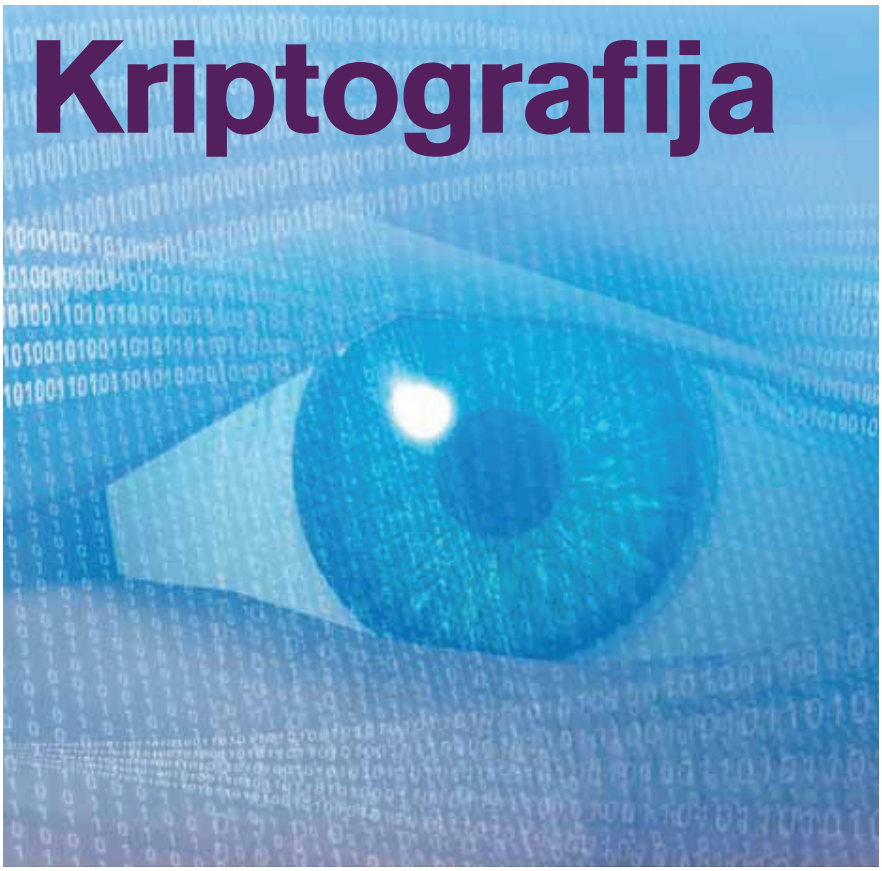
Bože Tokić, dipl. ing.

Kriptografija

Kriptografija je već jako dugo vremena interesno područje obavještajnih agencija, policija i vojski diljem svijeta. Zbog činjenice da zadire u privatnost pojedinca usprkos njegovoj zabrani, kriptografija je tako postala i predmetom interesa udruga koje podupiru ljudska prava. Tijekom povijesti postoji cijeli niz kontroverznih legislativnih problema koji okružuju kriptografiju tijekom njezinog razvoja, posebice danas, kad je pojava jeftinih računala omogućila široku uporabu vrlo visokog stupnja zaštite podataka – kriptografiranja.



Kriptografija (ili **kriptologija**; izvedenica iz grčkih riječi *kryptós* "skriveno," i glagola *gráfo* "pisati") je znanost o skrivanju poruka. Danas je kriptografija postala ogranak informacijske teorije, kao matematičke znanosti o informaciji i posebno načinu njenog prijenosa od mjesta do mjesta. Poznati **kriptograf Ron Rivest** je primijetio da je "*u kriptografiji riječ o raznolikoj komunikaciji u sadašnjosti*". On je doprineso na razvoju kriptografije na nekoliko polja: informacijskoj sigurnosti i problemima koji se odnose na nju, posebno o autentifikaciji i upravljanju pristupom informacijama. Osnovna svrha kriptografije je skrivanje značenja poruke. Kriptografija je doprinijela računalnoj znanosti, posebno pri tehnologijama zaštite informacija na samom računalu i mrežnoj sigurnosti pri upravljanju pristupom i povjerljivosti informacija. Kriptografija se također na veliko **koristi i u svakodnevnom životu**: sigurnost kartice bankomata, računalne lozinke su nekriptirane na vašim osobnim računalima, cjelokupno elektroničko trgovanje ovisi o kriptografiji.

U nekim zemljama je zabranjena, tj. ograničena uporaba kriptografije. Tako je bila značajno ograničena u Francuskoj do 1999. godine. U Kini, još uvijek trebate imati licencu da biste smjeli koristiti kriptografiju. Zemlje koje imaju restriktivne zakone po pitanju kriptografije su: Bjelorusija, Kazahstan, Mongolija, Pakistan, Rusija, Tunis, Venezuela i Vijetnam.

Problemi kriptografije u SAD-u

U SAD-u, kriptografija je legalna za kućnu uporabu, ali postoji mnogo sukoba oko **legalnih problema** vezanih za kriptografiju. Jedan posebno važan problem je izvoz kriptografskog softvera i hardvera. Zbog važnosti kriptoanalize tijekom drugog svjetskog rata i očekivanja da će se kriptografija nastaviti razvijati do tog nivoa da bi bila važna za nacionalnu sigurnost, mnoge zapadne vlade imaju, do neke točke, strogo reguliran izvoz kriptografskih materijala.

Iza drugog svjetskog rata, bilo je ilegalno prodavati ili distribuirati u SAD-u tehnologiju za enkripciju preko mora. Zapravo, enkripcija je bila klasificirana kao oružje, npr. tenkovi ili nuklearne rakete. Sve do pojave osobnih računala i Interneta, ova restrikcija nije predstavljala neki posebno velik problem. **Većina kriptografskih tehnika**, koje su bile dobre bile su spore, pa je korisnik vrlo lako mogao razlikovati dobru kriptografsku tehnologiju od loše. Obje, i dobra i loša, bile su podložne greškama. Ipak, kako se Internet razvijao i računala postaju sve dostupnija širokom krugu korisnika, visoko kvalitetne enkripcijske tehnike su postale vrlo dobro poznate diljem svijeta. Kao rezultat svega toga, **kontrola izvoza** se pokazala nemoćnom na području trgovine i istraživanja.

Svrha kriptografije

Kriptografija je znanost pisanja tajnog koda, ali i antička je umjetnost. Prva dokumentirana uporaba kriptografije pri pisanju datira oko 1900. prije Krista, kad je jedan Egipćanin iskoristio nestandardne hijeroglife pri pisanju. Neki eksperti se svađaju oko toga dali se kriptografija spontano pojavila u neko vrijeme nakon što je otkrivena tehnika pisanja, s primjenama počevši od diplomatskih nota do ratnih planova. Nije iznenađenje, da su novi oblici kriptografije došli vrlo brzo nakon što je široko rasprostranjena računalna komunikacija. Pri podatkovnoj komunikaciji i u telekomunikacijama, kriptografija je neophodna kad se vrši prijenos putem neprovjerenog medija, koji uključuje bilo koju mrežu, posebice Internet.

U kontekstu komunikacije među aplikacijama, potrebno je **zadovoljiti neke posebne sigurnosne zahtjeve**, uključujući:

RECIMO DA JE TU NEGDJE VRHUNAC VAŠEG POSLOVNOG USPJEHA

VI STE TU, U POTRAZI ZA IZAZOVIMA I PITATE SE S KIM I KOJIM PUTEM KRENUTI

A TU SMO MI, POMAŽEMO VAM STIĆI DO CILJA

Ubrzani razvoj informacijskih tehnologija, multimedije i komunikacija odredio je naš put prema sistemskoj integraciji. /**150 stručnjaka u Ericssonu Nikoli Tesli radi na poslovima sistemske integracije**/ Taj put podrazumijeva multidisciplinarni ICT pristup istraživačkim i razvojnim aktivnostima na raznim projektima, koji se vrlo često izvode kroz međunarodnu suradnju. /**U Hrvatskoj djeluje jedan od globalno najuspješnijih Ericssonovih R&D centara, s poslovnim aktivnostima diljem svijeta**/ Kao vodeći sistem integrator u Hrvatskoj imamo znanja i iskustva na različitim područjima i tehnologijama te kontinuirano ulažemo u razvoj novih kompetencija.

www.ericsson.hr

ERICSSON

TAKING YOU FORWARD

Ericsson Nikola Tesla d.d.

1. **AUTENTIKACIJA:** proces dokazivanja identiteta pojedinca (služi za prepoznavanje među dvama računalima, a prepoznavanje se zasniva na imenima računala ili na adresama – u oba slučaja radi se o smiješno niskoj zaštiti),
2. **PRIVATNOST/POVJERLJIVOST:** osiguravanje da nitko ne može pročitati poruku osim onog kome je namijenjena,
3. **INTEGRITET:** osigurati se da je primatelj primio poruku u originalu kako je i poslana, tj. da nije izmijenjena na bilo koji način u odnosu na original,
4. **NEPORECIVOST:** mehanizam koji dokaziva da je pošiljatelj zaista i poslao poruku koju smo primili.

Kriptografija, ne štiti podatke samo od krađe ili mijenjanja, već može biti i iskorištena za autentikaciju.

Općenito gledajući, postoje **dva tipa kriptografskih shema** koje se tipično koriste da bi se postigli ovi ciljevi:

1. kriptografija tajnim ključem (simetričan) i
2. javnim ključem (nesimetričan).

U svim slučajevima, početni neenkriptirani podatak se označava pod pojmom obični tekst koji se zatim enkriptira u tzv. *cipher* tekst (šifrirani tekst), koji obično biva dekriptiran nakon slanja u upotrebljivi obični tekst.

Tipovi kriptografskih algoritama

Postoji nekoliko načina klasifikacije kriptografskih algoritama. Ovdje ćemo ih kategorizirati prema broju ključeva koji se koriste za ekripciju i dekripciju, i prema njihovom načinu primjene.

Dva tipa algoritama su:

- kriptografiranje tajnim ključem (koristi jedan te isti ključ za enkripciju i dekripciju poruke) i
- kriptografiranje javnim ključem (koristi jedan ključ za enkripciju i drugi za dekripciju).

Kriptografija simetričnim ključem se odnosi na enkripcijske metode u kojima i pošiljatelj i primatelj dijele isti ključ (ili manje često, njihovi ključevi su različiti, ali povezani na način da ih je jednostavno izračunati). Ovo je bio jedini poznati javnosti dostupan način enkripcije do 1976. godine.

Značajan nedostatak simetričnog kriptiranja je distribucija ključeva koja je potrebna da bi ih se sigurno koristilo. Svaki par u komunikaciji mora razmijeniti ključ, koji je različit od ključa koji koristi drugi par u komunikaciji. Broj ključeva na ovaj način raste s kvadratom članova mreže, što vrlo brzo zahtjeva jako komplicirane sheme za distribuciju ključeva da bi svi ostali sigurni i tajni. Poteškoća dijeljenja tajnog ključa između dviju strana koje sudjeluju u komunikaciji, kad sigurni kanal ne postoji između njih prije dijeljenja ključa, također predstavlja problem kokoši i jajeta. Odnosno, ukoliko razmijenite ključeve pomoću kojih enkriptirate poruku, a kanal nije siguran, onda nema koristi od enkripcije (jer i vaš protivnik, koji prisluškuje kanal, dolazi do ključeva i same poruke netom nakon toga).

Kriptoanaliza

Cilj kriptoanalize je pronaći slabosti ili sigurnosne propuste u kriptografskoj shemi, koja dopušta iskorištavanje nedostataka enkripcije ili komunikacijskog kanala, a u svrhu zadobivanja načina enkripcije, enkripcijskog ključa i dijela ili cijele poruke. **Kriptoanalizu provodi** napadač koji se želi "podvući" u sustav – iskoristiti njegove nedostatke ili tvorac samog sustava pri pokušaju procjene zaštićenosti mreže, traženju propusta - u svrhu popravljanja propusta.

Danas, kriptografski algoritmi i protokoli se moraju pažljivo pregledati i testirati da bi ponudili sigurnost u kvaliteti sustava (ili barem sigurnosne propuste sveli na razinu pretpostavke).

Pravni problemi vezani uz kriptografiju isključivo se tiču već ranije spomenute kontrole izvoza tehnologije, umiješanosti nacionalnih sigurnosnih agencija, u prvom redu SAD-ove NSA, te upravljanje digitalnim pravima enkripcijskih sustava. ps

Sigurnost i zaštita podataka u informacijskom sustavu primarne zdravstvene zaštite

Zaštita podataka od zloupotrebe i neovlaštenog korištenja jedan je od najznačajnijih zahtjeva kojeg treba ispuniti bilo koji informacijski sustav. U zdravstvenim informacijskim sustavima taj zahtjev je još izraženiji, jer se u njima razmjenjuju i pohranjuju vrlo osjetljivi podaci. Zloupotreba ili neovlašteno korištenje tih podataka može povrijediti pravo privatnosti pacijenta, a eventualni gubitak podataka prikupljenih tijekom liječenja može uzrokovati pogreške te ugroziti zdravstvenu skrb pojedinca i konzistentnost odgovarajućih statističkih podataka cijele nacije.

To su osnovni razlozi zbog kojih je **Ericsson Nikola Tesla** prilikom izgradnje i definiranja Središnjeg informacijskog sustava primarne zdravstvene zaštite koristio najsuvremenije mehanizme zaštite podataka, temeljene za infrastrukturi javnog ključa i pametnim karticama. Time su svi podaci pohranjeni u središnjem sustavu u potpunosti osigurani, a sigurnost samog sustava postavljena na najvišu moguću razinu.

Budući da se sva komunikacija između liječničkih ordinacija i središnjeg informacijskog sustava primarne zdravstvene zaštite odvija putem Interneta, osnovnu zaštitu sustava od neovlaštenog pristupa obavlja tzv. virtualna privatna mreža (VPN), koja omogućava pristup samo autoriziranim korisnicima. Svi podaci koji se prenose između ordinacija i središnjeg sustava kodiraju se korištenjem privatnog ključa pohranjenog na korisnikovoj pametnoj kartici te su i dodatno zaštićeni od neovlaštenog pristupa.

Nakon priključenja na VPN i liječnik i sestra se prijavljuju u sustav korištenjem pametne kartice i certifikata, čime se potvrđuje njihov identitet i određuje njihova uloga, odnosno ovlasti i razina pristupa podacima i uslugama u sustavu. Potpuni pristup podacima o pacijentu ima njegov odabrani liječnik PZZ-a, ali taj isti liječnik ne može pristupiti podacima o ostalim pacijentima, koji su odabrali nekog drugog liječnika PZZ-a.

Digitalni potpis u informacijskom sustavu PZZ-a zamjenjuje žig i vlastoručni potpis liječnika, a štiti podatke i od neovlaštenog mijenjanja.

Najzanimljiviji sigurnosni mehanizam implementiran u Središnji informacijski sustav primarne zdravstvene zaštite jest njegova specifična arhitektura. Naime, svi su podaci pohranjeni u dvije razdvojene baze podataka. U prvoj, elektroničkom registru pacijenata nalaze se samo osobni podaci o pacijentu kao što su ime i prezime, adresa, polica osiguranja itd. Druga baza podataka, elektronički registar zdravstvenih kartona, sadrži samo medicinske podatke, ali ne i podatke na koje se konkretne pacijente ti podaci odnose. Da bi se dobio potpuni uvid u medicinski karton pacijenta podaci iz ove dvije baze podataka se moraju povezati pomoću specijalnog šifriranog identifikatora, a njime raspolaže samo liječnik koji je od pacijenta dobio dozvolu pristupa. Na ovaj se način privatnost medicinskih podataka pacijenta štiti čak i od administratora sustava, jer bez privatnog ključa odabranog liječnika koji se nalazi isključivo na pametnoj kartici tog liječnika, nije moguće povezati medicinske i administrativne podatke pacijenta.

Krešimir Kerš, manager za složena rješenja sistemske integracije u Ericssonu Nikoli Tesli