

**Zastita tajnosti, integriteta i autenticnosti poslovnih i privatnih  
informacija koje se u elektronskom obliku prenose putem  
Interneta**

**AUTOR**

*Sladjan Nikolic*

## SADRZAJ

### Sifrovanje e-maila

Zastita tajnosti informacija.....	4
Simetricni i asimetricni sifarski sistemi.....	4
Zastita integriteta i autenticnosti - digitalni potpis i sertifikat.....	6
<b>PGP (Pretty Good Privacy) – standard za postupanje na Internetu</b>	
Zastita tajnosti.....	7
Zastita integriteta i autenticnosti.....	8
Odakle skinuti PGP i osnovni koraci u radu s ovim alatom.....	8

### Program za sifrovanje telefonskih razgovora– PGPfone

Kako funkcioniše PGPfone.....	9
Sematski prikaz.....	10
Podesavanje.....	10
Telefoniranje upotrebom standardne telefonske linije.....	10
Internet-telefoniranje.....	10

### Sifrovanje online razgovora u tekstualnom rezimu

Secure Communicator i PSST Version 0.2.....	10
---	----

### Steganografija – nauka i umetnost

Uvod.....	11
Steganografija.....	11

<b>Masker 5.0.....</b>	<b>12</b>
<b>Resenja problema prenosa i razlicitosti tajnog kljuc.....</b>	<b>12</b>
<b>SSL (Secure Socket Layer) protokol - metod za obavljanje sigurnih transakcija na Internetu.....</b>	<b>13</b>

### **Sifrovanje e-maila**

Internet je otvorena javna mreza dostupna svima i uvek postoji mogucnost da neko neovlascono prati vasu komunikaciju i to kasnije zloupotrebi! Zato je zastita prenosnih podataka od neovlasćenog citanja, povrede njihovog integriteta i potvrda autenticnosti posiljioca od ogromnog znacaja, posto priroda razmene informacija u elektronskom obliku omogucava njihovo relativno jednostavno presretanje, bez velikog ucesca ljudskog rada, cineci time pracenje tudje komunikacije “dostupnim” vecem broju neovlasćenih osoba Kad se poruka presretne ona se moze pročitati, izmeniti i na adresu primaoca poslati sasvim druga poruka, osim toga moguće je lazno predstavljanje tj. da vam upotrebom specijalizovanih programa neko uputi poruku sa “adrese” vasesg prijatelja ili

poslovnog partnera (E-mail od onih kojima se veruje - <http://www.apisgroup.org/sec.html?id=3> )... Posledice ovakvih akata cesto mogu biti katastrofalne!

Zbog toga je u cilju ozbiljne primene Interneta kako u savremenom elektronskom poslovanju tako i u privatnoj komunikaciji **potrebno koristiti mehanizam koji ce obezbediti : zastitu tajnosti informacija** (sprecanje otkrivanja njihovog sadrzaja), **integritet informacija** ( sprecanje neovlascene izmene informacija) i njihovu **autenticnost** (definisanje i provera identiteta posiljioca).

**Zastita tajnosti i integritet informacija postize se sifrovanjem, a upotrebom digitalnih potpisa i digitalnih sertifikata obezbedjuje se njihova autenticnost tj. definisanje i provera identiteta posiljioca.**

### **Zastita tajnosti informacija**

Tajnost informacija je svojstvo da se informacije mogu citati samo od autorizovanih korisnika ili primaoca. Zastita tajnosti informacija postize se na taj nacin sto se poruka (tekst, govor, slika i sl.) odredjenom operacijom (**sifarskim sistemom**) transformise u novi oblik informacije-**sifrat**. Pod pojmom **sifrovanje** se podrazumeva proces prevodjenja informacija iz njihovog originalnog oblika u novi nerazumljivi oblik-**sifrat**. Tehnike sifrovanja imaju veliki, strateski, i pravni znacaj posto imaju glavnu ulogu u zastiti od informatickih prevara, povrede sigurnosti podataka, zastititi pouzdanosti korespodencije, zastiti profesionalne tajne i elektronskoj trgovini.

**Tajnost poruke** se zasniva iskljucivo na **tajnosti kljuc̃a**; nijedan ozbiljan algoritam za sifrovanje ne zasniva tajnost poruke na tajnosti ili nedostupnosti algoritma. Stavise, svi algoritmi za kriptografiju koji se danas upotrebljavaju su javni i lako dostupni. Kljuc je pocetna vrednost algoritma kojim se vrsi sifrovanjea tajnost se sastoji u tome, sto tu pocetnu vrednost znate samo vi.

Evo nekoliko pravila kojih bi trebalo da se pridržavamo prilikom smišljanja tajnog kljuc̃a:

*- Najidealnije je da se za lozinku uzme niz slućajnih slova i brojeva. Pri tom bi trebalo da se koristi vise od jednog niza slućajnih slova i brojeva. Ukupan broj charaktera svih nizova treba da bude najmanje 13.*

Ovakve tajne kljuceve mnogi izbegavaju jer ih smatraju teskim za pamcenje i upotrebljavaju reci iz svakodnevnog govora. U tom slucaju potrebno je pridrzavati se sledecih pravila:

*- Ne koristiti reći koje se lako mogu pogoditi: na primer, godinu rodenja, devojaćko ime, ime deteta, suprućnika, psa/maćke/kanarinca itd.*

*- Trebalo bi koristiti više od jedne reći. Izbegavajte upotrebu reći iz rećnika u neizmenjenom obliku. Korisno je upotrebiti barem kombinaciju jedne reći sa nekim brojem.*

*- Budite inventivni. Najbolja lozinka moće biti deo citata iz neke knjige ili neka besmislena rećenica.*

Mehanizam sifrovanja informacija treba da poseduje tri osnovna svojstva: **zastita tajnosti** (sprecanje otkrivanja njihove tajnosti), **integritet** (sprecanje neovlascene izmene informacija) i **autentićnost** (definisanje i provera identiteta posiljioca).

## Simetricni i asimetrični sifarski sistemi

U ovom tekstu zadržaćemo se na asimetričnim i simetričnim sifarskim sistemima kako bi smo čitaocu koji se prvi put susreće sa ovim pojmovima na najjednostavniji način omogućili da shvati šta su to sifarski sistemi, koja su to osnovna svojstva koja treba da poseduje jedan sifarski sistem, koje su prednosti i mane sifarskih sistema, zašto su asimetrični sifarski sistemi u prednosti, kako se šifrira informacija pomoću njih, kao osnovu za shvatanje danas u svetu najsigurnijeg alata za šifrovanje privatnih e-maila i poslovne komunikacije, PGP-a, i olakšali njegovu upotrebu.

**Simetricni sifarski sistem (sistem šifrovanja tajnim ključem), koristi isti ključ i za šifrovanje i za dešifrovanje informacije.** To je najprostiji vid šifrovanja informacija i odlikuje ga velika propusna moć algoritma, tj., složenost tih algoritama je mala. Kod šifrovanja poruke simetričnim šifrovanjem tajnost i autentičnost poruke zasnivaju se na autentičnosti ključa a sistem je bezbedniji ukoliko se ključ generise što slučajnije.

**Problem** sa simetričnim sifarskim sistemom javlja se u distribuciji samog ključa od pošiljaoca do samog primaoca jer oni mogu biti na veoma udaljenim mestima. Naime postavlja se pitanje kako preneti tajni ključ? Jer ako se presretno tajni ključ, poruka se može pročitati. Postoji još jedan problem, ako pošiljalac želi da komunicira sa više poslovnih partnera mora da obezbedi različite ključeve za svakog primaoca, kako bi se izbegla mogućnost da bilo koji primalac čita poruke koje mu nisu namenjene. **Rešenje ovih problema je pronadeno u vidu sistema šifrovanja javnim ključem (asimetrični sifarski sistem).**

**Asimetrični sifarski sistem (sistem šifrovanja javnim ključem), je takav da u njemu svaki učesnik u komunikaciji koristi dva ključeva, tajni i javni ključ.** Na osnovu **tajnog ključa** koji zadajemo, generiše se **javni ključ**. Javni ključ se može slobodno distribuirati, dok je drugi tajni i dostupan je samo njegovom vlasniku. Iako su različiti, ključevi su međusobno povezani određenim transformacijama. Poznavanje jednog ključa i algoritma transformacije ne omogućava dobijanje drugog ključa. Najbitnije je da se tajni ključ u celom postupku komunikacije nigde ne šalje jer ne postoji potreba da bilo ko sem njegovog vlasnika bude upoznat s njim. To znači da se može bilo kome poslati šifrovana poruka ako se zna javni ključ osobe kojoj se šalje, a samo primalac svojim tajnim ključem može da dešifruje poruku.

Princip korišćenja asimetričnog sifarskog sistema je sledeći: na osnovu tajnog ključa koji zadajemo, generiše se javni ključ. Javni ključ dajemo osobama koje nam šalju šifrovane e-maile. Pomoću njega, ta osoba šifrira e-mail koji želi da nam pošalje i takvog nam ga šalje. Kada nam šifrovani e-mail stigne, mi ga dešifrujemo pomoću našeg tajnog ključa. Znači, tajni ključ imate samo vi, a javni ključ može imati bilo ko, pošto se on koristi samo za šifrovanje, a ne i dešifrovanje.

**RSA** je najpoznatiji primer asimetričnog sifarskog sistema. Ime je dobio po svojim pronalazacima (Rivest, Shamir i Adleman), a objavljen je 1978. godine. Sigurnost RSA zasniva se na složenosti faktorizacije velikih brojeva. Smatra se da je određivanje originalne poruke na osnovu sifrata i ključa za šifrovanje ekvivalentno faktorizaciji proizvoda dva velika prosta broja. Sledeću moćnu klasu praktičnih, asimetričnih algoritama formulisao je **ElGamal** 1985. god., što je ustvari varijanta **Diffie-Hellman** sistema za distribuciju tajnih ključeva javnim kanalima. Tehnički je slična sa RSA, ali je

sifrat dvostruko duzi. Matematička osnova algoritma je u praktičnoj nemogućnosti nalazenja *diskretnog logaritma*.

U poredjenju sa simetričnim algoritmima, asimetrični algoritmi su značajno sporiji, dakle propusna moc im nije velika, pa se uglavnom koriste za sifrovanje manjih poruka, dok im je **glavna praktična primena** u generisanju efikasnih potpisa i upravljanju ključevima. Takodje, može se uočiti da je dužina ključa kod asimetričnog algoritma znatno veća nego kod simetričnog algoritma, ali je prednost u tome **sto se samo privatni ključ mora držati u tajnosti** i sto se kod asimetričnog algoritma **može duže koristiti bez promene**. Vazna je činjenica da se asimetrični algoritam može koristiti za **distribuciju** ključeva za simetrični algoritam, u cilju omogućavanja brze i obimne komunikacije. Na ovaj način od oba algoritma uzimamo najbolje: "dugovećnu" prirodu para  $((e,n),d)$  od asimetričnog algoritma i odlične performanse (brzina i propusna moc) od simetričnog algoritma. Posto je sifrovanje podataka vremenski najzahtevnija operacija u procesu sifrovanja, to samo uspostavljanje ključa u citavom procesu komunikacije odnosi neznatno malo vremena.

#### **Nekoliko saveta u vezi sa tajnim ključem**

- *Najidealnije je da za tajni ključ uzmete niz slučajnih slova i brojeva. Pri tom bi trebalo da se koristite više od jednog niza slučajnih slova i brojeva.* Upotrebljavajte **kombinacije** slova-brojke-**slučajni izbor** ne praveci u nizovima nikakav sistem, kao sto je recimo slovo pa brojka i tako u svakom nizu. Vas tajni ključ nikad nigde ne zapisujte, nek bude samo u vasoj glavi. **Menjajte vas tajni ključ u nekom odredjenom vremenskom periodu-opet slučajni izbor**. Naravno to znaci da ce se i vas javni ključ promeniti, pa je potrebno poslati novi onima sa kojima kontaktirate.

### **Zastita integriteta i autenticnosti - digitalni potpis i sertifikat**

**Digitalni potpis** je skup podataka u elektronskom obliku koji su dodati ili logički pridruženi elektronskim porukama ili dokumentima i služe kao metod za identifikaciju potpisnika. Svrha *digitalnog potpisa* je da potvrdi **autenticnost** sadržaja poruke (dokaz da poruka nije promenjena na putu od posiljaoca do primaoca), kao i da obezbedi garantovanje **identiteta** posiljaoca poruke. Prvi standard digitalnog potpisa usvojen je 1991. god. i bazirao se na RSA asimetričnom algoritmu. 1994 je vlada SAD usvojila Digital Signature Standard (DSS) , koji se bazira na ElGamal šemi asimetričnog algoritma.

Osnovu digitalnog potpisa čini sadržaj same poruke. Posiljalac primenom kriptografskih algoritama prvo od svoje poruke koja je proizvoljne dužine stvara zapis fiksne dužine (pr. 512 ili 1024 bita) koji u potpunosti odslikava sadržaj poruke. To praktično znaci da svaka promena u sadržaju poruke dovodi do promene potpisa. Dakle, posiljalac kreira digitalni potpis na osnovu poruke koju želi da pošalje. Sifruje ga svojim tajnim ključem i šalje zajedno sa porukom. Primalac po prijemu poruke deifruje potpis posiljaoca njegovim javnim ključem. Zatim kreira potpis na osnovu poruke koju je primio i upoređuje ga sa primljenim potpisom. Ako su potpisi identični, može biti siguran da je poruku zaista poslao pravi posiljalac (jer je njegovim javnim ključem uspesno deifrovao potpis) i da je ona stigla nepromenjena (jer je utvrđeno da su potpisi identični). I pored velike sigurnosti koju pruža ovaj metod zaštite, i dalje postoji mogućnost prevare. Neko je

mogao poslati svoj javni ključ tvrdeći da je od pravog posiljaoca, a zatim slati poruke za koje bi primaoc mislio da ih šalje pravi posiljaoc. Resenje ovog problema pruza upotreba **digitalnih sertifikata**.

Ako nam neko šalje svoj javni ključ, kako mozemo biti sigurni da je taj ključ zaista njegov? Resenje ovog problema postize se upotrebom *digitalnih sertifikata*. Mozemo ih nazvati i digitalnom licnom kartom. **Digitalni sertifikat je uverenje kojim se potvrđuje veza izmedju podataka za verifikaciju elektronskog potpisa i identiteta potpisnika, koji je izdat od strane akreditovanog certifikacionog tela.** Na internetu postoje kompanije CA (Certificate Authority) cija je uloga da provere i utvrde neciji identitet i nakon toga mu izdaju digitalni sertifikat. Posto prosledimo svoj javni ključ u CA, oni kreiraju digitalni potpis i izdaju sertifikat koji potvrđuje da taj javni ključ zaista pripada nama. Ako dalje zelimo da komuniciramo sa nekim, pri prvom kontaktu mu saljemo digitalni sertifikat i svoj javni ključ. Primalac onda lako utvrđuje validnost naseg sertifikata. Ako imamo server i zelimo digitalni sertifikat, tada digitalni sertifikat naseg servera izdat od strane CA mora da sadrzi sledece:

- Naziv nase organizacije
- Dodatne podatke za identifikaciju,
- Nas javni ključ
- Datum do koga vazi nas javni ključ
- Ime CA koji je izdao digitalni sertifikat i
- Jedinstveni serijski broj.

Svi ovi podaci formiraju sertifikat koji se na kraju šifruje koristeći tajni ključ CA. Ako korisnik ima poverenja u CA i ima CA javni ključ, može biti siguran u ispravnost sertifikata. Velika je verovatnoća da Web browser koji korisnik poseduje već sadrži javni ključ CA jer su Netscape i Microsoft procenili kojim se CA može najviše verovati, pa su njihove javne ključeve uključili u svoje browsere. Najčešće korišćeni standard za digitalne sertifikate je X.509.

### **PGP (Pretty Good Privacy) – standard za postupanje na Internetu**

PGP obezbedjuje sigurnu korespodenciju koristeći hibridni sistem sifrovanja, i ispunjava zahteve u vezi sa zastitom tajnosti, integriteta i autenticnosti. Zastita tajnosti, integriteta i autenticnosti su upravo sto je potrebno kad je rec o elektronskom poslovanju pod kojim se podrazumeva svaka finansijska transakcija koja koristi informaciju razmenjenu elektronskim putem. Kako se se elektronsko poslovanje u vecini slucajeva obavlja preko Interneta, javne mreze koja je dostupna svima, uvek postoji mogucnost neovlascenog pracenja elektronskog poslovanja iz zloupotrebe saznanja iz tog pracenja. PGP danas predstavlja standard postupanja na Internetu kad je rec o elektronskom poslovanju a nista manje koristi se i u privatne svrhe.

### **Zastita tajnosti**

PGP koristi hibridni sistem za šifrovanje, jer kombinuje i simetrični i asimetrični šifarski sistem, i ElGamel varijantu Diffie-Hellman sistema za distribuciju tajnih ključeva javnim kanalima. Tehnički je slična sa RSA, ali je šifrat dvostruko duži. Matematička osnova algoritma je u praktičnoj nemogućnosti nalaženja diskretnog logaritma.

Simetrični šifarski sistem je oko hiljadu puta brži od asimetričnog, ali kod njega postoji problem prenosa ključa (ako se presretne ključ, podaci se mogu dešifrovati). Kada se ukombinuju ova dva načina šifrovanja, dobija se željeni efekat: brza šifrovanje sa sigurnim prenosom ključa. Ključ se, dakle, prenosi, ali šifrovan tako da ga samo osoba koja ima tajni ključ može dešifrovati. Podaci se pre šifrovanja pakuju, ako je moguće. Ovo je korisno iz dva razloga. Prvi je manja količina podataka za prenos. Drugi je dodatna sigurnost, jer se pakovanjem eliminiše pojavljivanje sličnih delova u izvornoj datoteci. Mnoge tehnike kriptanalize iskorišćavaju baš te slične delove da bi probile zaštitu. Naravno, fajlovi koji su ili prekratki za pakovanje ili se ne mogu spakovati dovoljno, ostavljaju se u izvornom obliku. Posle pakovanja, PGP pravi privremeni ključ, odnosno slučajan broj koji se generiše korisnikovim pokretima miša i pritiskanjem tastera, jer su i oni takođe slučajni. Ovaj ključ ima jednokratnu upotrebu, jer se koristi da bi se podaci šifrovali simetričnom enkripcijom. PGP zatim šifrjuje samo privremeni ključ asimetričnom enkripcijom i pridružuje šifrovanim podacima. Dešifrovanje se vrši suprotnim procesom. Prvo PGP pomoću tajnog ključa dešifrjuje privremeni ključ, a njim se onda dalje dešifruju podaci.

### **Zastita integriteta i autenticnosti**

PGP ima mogućnost **digitalnog potpisivanja** dokumenata (**zastita integriteta i autenticnosti**), uz jednu razliku. Umesto da se ceo dokument šifrjuje tajnim ključem i od njega generiše potpis, to se radi samo na kontrolnom kodu dokumenta (veoma slično CRC-u). Bilo kakva promena na dokumentu rezultuje promenom u kontrolnom kodu, samim tim potpis više nije važeći, a vi znate da je u pitanju falsifikat. Time se izbegava dupliranje dužine dokumenta, jer se potpis ne generiše od celog dokumenta.

### **Odakle skinuti PGP i osnovni koraci u radu s ovim alatom**

PGP mozete naci na sledecoj web adresi: <http://cws.internet.com/encrypt-pgp.html>. Uz PGP dobijate i tri dokumenta edukativnog karaktera u PDF formatu, i uz pomoc njih i naseg teksta mozete nauciti kako da koristite ovaj alat i kako da vasa korespodencija i transakcije elektronskog poslovanja na Interenetu imaju svojstva tajnosti, integriteta i autenticnosti.

#### **Prvi korak-Generisanje kljuca**

*pgp -kg*

Upisite duzinu kljuca kojeg zelite koristiti (768 ili 1024 bita). Upisite svoje podatke u obliku: Ime Prezime . Izaberite lozinku . Zatim upisujete slucajno izabrane znakove na tastaturi dok vam PGP ne kaze da ste upisali dovoljnu kolicinu.

#### **Drugi korak- Izdvajanje javnog kljuca**

Prvo izdvojite javni kljuc

*pgp -kxa korisnik javni.asc*

koji postavite na vidljivo mjesto, posaljete ga u javnost.

### **Treci korak- Igranje s javnim kljucevima**

Kad uzmete neciji kljuc pridruzite ga u prsten javnih kljuceva i provjerite je li to uopste njegov javni kljuc.

*pgp -ka tudji.asc*

*pgp -kvc ime*

Provera ponekad nije potrebna.

Ukljanjanje necijeg kljuca je isto tako jednostavno:

*pgp -kr ime*

### **Cetvrti korak- Sifrovanje i desifrovanje poruka**

*pgp -eat jasnopis.txt ime*

(ime - ime pod kojim je spremljen tudji kljuc), a desifrovanje pristigle poruke

*pgp primljena-poruka*

## **PROGRAM ZA SIFROVANJE TELEFONSKIH RAZGOVORA – PGPfone**

Upotreba programa PGPfone u nekomercialne svrhe je besplatna i ne zahteva neku posebnu opremu koja se razlikuje od one koju koristimo da bi smo krstarali Internetom i koristili racunar u svrhe komunikacije. Potrebna oprema:

- modem brzi od 9600b bps
- zvučna kartica
- mikrofonski i slusalice
- OS Windows 95, 98, ...
- program PGPfone

### **Kako funkcioniše PGPfone**

PGPfone preko modema, putem telefonske linije ili Interneta uspostavlja vezu sa racunarnom osobom sa kojom zelimo da komuniciramo. Kad se veza uspostavi program zapocinje razmenu digitalnih podataka – naseg govora. Program pomocu zvučne kartice digitalizuje nas govor, sifira ga i preko modema prenosi do naseg sagovornika. Sagovornik nas govor slusa uz pomoc zvučne kartice i slusalica ili zvučnika. Govor koji se digitalizovan prenosi putem telefonske linije ili Internete sifruje se RSA algoritmom. Ako neko prisluškuje nas razgovor, cuce nerazgovetne sumove jer je prisluškivanje prakticno nemoguće.

Program [pgpfone10b2.zip](#) moraju da upotrebljavaju oba sagovornika i moze se koristiti za Internet-telefoniranje ili telefoniranje koriscenjem standardne telefonske linije.

### **Sematski prikaz**

**osoba A** -> mikroskop -> zvučna kartica -> računar -> modem -> prenos kodiranih podataka putem telefonske linije -> modem -> računar-> zvučna kartica -> zvučnici ili slusalice -> **osoba B**

### **Podesavanje**

U meniju **Edit, Preferences**, kartica **Phone**, polje **Identity**, upišite ime po kome će vas sagovornik prepoznati kad ga budete pozvali. U kartici **Modem**, postavite odgovarajući port vašeg modema i njegovu brzinu. U kartici **Encryption** izaberite način šifrovanja.

### **Telefoniranje upotrebom standardne telefonske linije**

Upišite broj telefona koji zovete i kliknite na Dial.

### **Internet-telefoniranje**

Upišemo IP sagovornika i kliknemo na Connect. IP adresu vašeg sagovornika najlakše možete saznati ako pre Internet-telefonskog razgovora, obostrano upotrebite ICQ, ili odete na neki od IRC servera, tu možete videti IP adresu, koju zatim upišete i kliknete na Connect.

I to je sve. Ako vam posle čitanja ovog teksta nešto ne bude jasno uz PGPfone dobijate i uputstvo u PDF-u gde je detaljno razradjeno korišćenje ovog programa.

## **Šifrovanje online razgovora u tekstualnom režimu**

**Secure Communicator** je program koji vam omogućava šifrovanje online razgovora i fajlova koje u online režimu razmenjujete sa svojim sagovornikom. Za uspostavljanje šifrovane komunikacije potrebno je znati IP sagovornika. Šifrovana komunikacija upotrebom ovog programa se takođe može uspostaviti i korišćenjem posebnih servisa kao što su MS NetMeeting, Netscape Cooltalk, iPhone...Program se može naći na sledećoj WEB lokaciji: <http://www.idirect.com/secure/>

**PSST Version 0.2** je takođe jedan od programa koji možete koristiti da šifrujete vašu Internet-telefonsku, MSN, IRC ili ICQ komunikaciju. Za uspostavljanje šifrovane komunikacije potrebno je znati IP sagovornika. Kliknite na Connect, upišite IP sagovornika, a zatim na OK. Kad se komunikacija uspostavi, rečenice koje pišete se automatski šifruju i tako šifrovane prenose do vašeg sagovornika, dešifrovanje se vrši tek u njegovom računaru. Ovaj program možete skinuti sa adrese <http://netforth.sourceforge.net/psst/links.html>

Oba programa su izuzetno laka za korišćenje, a uz njih dobijate i sva potrebna uputstva.

Ono što je bitno jeste da sa svojim sagovornikom dogovorite **šifru, kao znak raspoznavanja**, koju ćete upotrebiti svaki put kad započnete komunikaciju kako se ne bi desilo da šifrovanoj komunikaciji uspostavite sa nekim drugim.

## Steganografija – nauka i umetnost

### Uvod

Kako preneti osetljiv materijal u elektronskom obliku koji nije za svačije oči, a da ne bude presretnut i njegova tajnost zauvek izgubljena? Naravno, nekim od do sada poznatih načina podatke možete da šifrujete svoje e-maile, ali takav e-mail ako se presretne prosto mami da bude dešifrovan. Da li ce biti desifrovan zavisi od umeca onih koji su vas prisluskivali i tajnosti ključa koji koristite. Rešenje za ovaj problem ponudili su još stari Grci, u vidu Trojanskog konja – u unutrašnjosti nekog bezazlenog fajla (recimo, skenirane fotografije nekog pejzaza), mogu se sakriti podaci koje ne zelite da vide neke druge ocim osim onih kojima su nemanjeni.

### Steganografija

Termin steganografija – vestina tajnog pisanja, potice od starih Grka - “setagnos”- cutljiv, pokriven i “graphia” - pisanje, a prvi dokumenti u kojima se ova vestina opisuje mogu se naci u delima cuvenog istoricara Herodota. Kroz istoriju tehnike steganografije stalno su razvijane a najsiru primenu dozivele su u drugom svetskom ratu. Nasiroko je bila koriscena tehnika mikrofilmovanja dokumenata i njihovog prenosjenju do odredista sakrivenih u neke bezazlene predmete. Takodje, u upotrebi je bila i tehnika pisanja pisama nevidljivim mastilom.

Sa razvojem kompjutera i tehnike steganografije dozivljavaju pravi procvat jer su oni koji razmenju informacije preko racunara uvek zeleli da te informacije zastite od nezelnih pogleda.. Jedna od najsire koriscenih tehnika steganografije danas jeste, sakrivanje poruke u unutrašnjost nekog multimedijalnog fajla (zvucni, video ili sliku). Glavna prednost ovakvog načina sifrovanja podataka je to što sem primaoca poruke niko drugi ne može da zna da li je sifrovana poruka uopšte poslata. Takođe, moguće je sifrovanje više poruka (ili izvršnih fajlova) u jedan fajl. Korisnik koji prima ovakvu poruku (ili poruke), dobiće sliku ili zvučni fajl koje svi mogu da vide, ali će samo onaj koji ima ključ moći da desifruje poruku koja se nalazi u takvom fajlu.

### *Masker 5.0*

Jedan od programa koji koristi tehnike steganografije je Masker 5.0. Kod ovog programa fajl nosilac može da bude slika (BMP, GIF, JPG, TIF), zvučni fajl (WAV, MID, SND, MP3), programski fajl (EXE, DLL, OCX) ili video fajl (AVI, MOV, MPG, ASF), a u

njemu može da se sakrije bilo koji drugi fajl (ili više njih). Skriveni fajlovi se unutar nosioca mogu sifrovati CAST-256, BLOWFISH-256, RIJNDAEL-256, TWOFISH-256 algoritmima (simetrični). Nasa preporuka je da za sifrovanje koristite belgijski algoritam RIJNDAEL-256, autora Joan Daemena i Vincent Rijmena, koji je početkom 2000., na konkursu u SAD za AES (Advanced Encryption Standard) izabran kao najbolji. Dosadasnji pokusaji kriptanalitičkih napada na ovaj algoritam su bili bezuspesni. Korišćenje programa izuzetno je jednostavno. Prvo je potrebno izabrati fajl nosilac, zatim se biraju fajlovi koje je potrebno sakriti i šifra kojom se dodatno zaštićuju skriveni fajlovi. Moguće je izabrati da izvorni fajlovi koje sakrivete automatski budu obrisani posle skrivanja, tako da ne mogu da se povrate. Za svaki od fajlova koje sakrivete moguće je uneti komentar. Sa jednim „paketom” skrivenih fajlova radi sa kao sa standardnom arhivom: mogu da se dodaju novi fajlovi, brišu postojeći, promene komentari ili da se izvuče jedan ili više fajlova iz nosioca.

Kada prvi put otvorite fajl nosilac program će od vas zahtevati da unesete šifru kojom je taj fajl zaključan. Ako šifru znate, u prozoru će se pojaviti lista skrivenih fajlova, njihova veličina, vreme i datum skrivanja i komentar. Sem „vađenja”, brisanja i dodavanja fajlova, moguće je promeniti šifru celog paketa, a takođe se može izvršiti i fajl nosilac.

Korisna opcija je i pretraživanja diska ili direktorijuma za fajlovima nosiocima. Potrebno je uneti šifru koja je korišćena prilikom stvaranja paketa i program će prikazati sve fajlove nosioce sa tom šifrom. Ukoliko postoje i drugi fajlovi nosioci, a vi ne znate koja je šifra korišćena za njih, nema načina da ih na ovaj način pronađete. Program razlikuje velika i mala slova pri unosu šifre.

Pri kreiranju paketa treba obratiti pažnju na veličinu paketa i ne treba preterivati sa „punjenjem”. Iako fajl nosilac funkcioniše normalno, i ne postoji način da se otkrije da postoje sakriveni fajlovi, složit ćete se da neočekivano velika dužina fajla sama po sebi izgleda sumnjivo. Analizom fajla nosioca ne može se utvrditi da u njemu postoji nešto sakriveno, a sam fajl će i dalje raditi kako treba

*Masker* možete pronaći na adresi (<http://www.softpuls.com/indmain.html>).

## **Resenja problema prenosa i razlicitosti tajnog kljuc**

*Masker* koristi simetricni sifarski sistem, kod koga se koristi isti kljuc i za sifrovanje i za desifrovanje poruka i zato se kod ovih sistema se uvek javljaju dva problema kako preneti tajni kljuc jer ako se on presretne poruka se moze procitati, i ako posiljalac zeli da komunicira sa vise primaoca mora da obezbedi razlicit kljuc za svakog od njih, kako bi se izbegla mogucnost da bilo koji primalac cita poruke koje mu nisu namenjene. Resenje ovog problema je koristite PGP na pocetku vase komunikacije kako bi ste preneli tajni kljuc, a za svakog od primaoca obezbedite razlicit kljuc.

## **SSL (Secure Socket Layer) protokol - metod za obavljanje sigurnih transakcija na Internetu**

SSL (Secure Socket Layer) protokol koji je razvila firma Netscape, je trenutno najčešće korišćen metod za obavljanje sigurnih transakcija na Internetu. Podržava ga većina Web servera kao i klijenata uključujući Microsoft Internet Explorer i Netscape Navigator.

SSL obezbeđuje *privatnost, integritet podataka i autentičnost* pošiljalaca korišćenjem kombinacije šifrovanja javnim ključem, simetričnog šifrovanja i digitalnih sertifikata.

Transakcija korišćenjem SSL protokola uključuje sledeće aktivnosti:

- server šalje svoj digitalni sertifikat klijentu
- klijent proverava da li je sertifikat izdat od strane CA
- klijent i server razmenjuju javne ključeve
- klijent generise tajni ključ koji se koristi samo u započetoj transakciji.
- klijent šifruje generisani tajni ključ, korišćenjem serverovog javnog ključa i šalje ga serveru.

U daljem toku transakcije server i klijent koriste isti tajni ključ metodom simetričnog kriptovanja.

U verziji 2.0 SSL podržava samo proveru autentičnosti servera, dok je u novoj SSL v3.0 uključena i podrška za proveru autentičnosti klijenta.

**Adrese vezane za ovaj tekst:**

[Netscape SSL Version 3.0](#)

[SSL FAQ](#)

[SSL 3.0 specification](#)

[How SSL works](#)