HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Opis PGP i GnuPG alata

CCERT-PUBDOC-2003-12-51

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.
Rezultat toga rada ovaj je dokument koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

***LS&S*, www.lss.hr**- laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

U doba kada je mrežna razmjena važnih dokumenata u digitalnom formatu općeprihvaćen način privatne i poslovne komunikacije, sve veći problem postaje zaštita takvih dokumenata od krivotvorenja i špijunaže.

Za prijenos poruka elektroničke pošte koristi se SMTP protokol kojim je definiran prijenos poruka u čistom tekstualnom formatu, a jedini podatak o pošiljatelju je njegova adresa, koja je opet u tekstualnom formatu dodana poruci. Na taj način svatko tko presretne nečiju poruku može pročitati njen sadržaj, a isto tako može i krivotvoriti podatak o pošiljatelju poruke. Taj protokol je nastao početkom 80-ih godina prošlog stoljeća, u vrijeme kada je bilo premalo Internet korisnika da bi itko razmišljao o sigurnosti i mogućim zloupotrebama Internet komunikacije. Danas je situacija potpuno drukčija jer se Internet koristi za razmjenu raznih privatnih i poslovnih podataka, a postoje brojni pojedinci ili organizacije sa različitim motivima i sredstvima za presretanje takve komunikacije.

Kako bi se riješio problem sigurne mrežne komunikacije bilo je potrebno stvoriti protokol za enkripciju i potpisivanje poruka koji bi bio dovoljno siguran i raširen da postane novi službeni standard.

Prvi pokušaj stvaranja takvog standarda je bio PEM (*Privacy Enhancment for Internet Electronic Mail*) standard za enkripciju tekstualnih poruka i njegov dodatak MOSS (*MIME Object Security Services*) za binarne datoteke. Standard je razvijan između 1985. i 1993. godine, no danas je uglavnom napušten i koristi se samo u zatvorenim krugovima.

Danas je najprisutniji način enkripcije podataka *OpenPGP* standard, a njegove najpoznatije implementacije su PGP (Pretty Good Privacy) i GnuPG (GNU Privacy Guard) programi. U nastavku ovog dokumenta dan je kratak opis osnovnih karakteristika dvaju spomenutih programa.

2. Povijest

Prvu verziju PGP programa je napisao Phil Zimmermann 1991. godine. Program je nastao kao odgovor na tada aktualnu raspravu u američkom kongresu oko uvođenja zakona o privatnosti. Taj zakon je trebao prisiliti sve telekomunikacijske kompanije u SAD-u da na zahtjev organa vlasti daju uvid u sadržaj komunikacija svojih korisnika.

PGP program koristi kombinaciju simetričnog i asimetričnog algoritma za enkripciju te algoritma za stvaranje *hash* otiska poruke. Princip rada ostao je isti kroz sve verzije programa koje su u međuvremenu nastale, samo su se mijenjali korišteni algoritmi.

Prva verzija programa je koristila tzv. Bass-o-Matic algoritam za simetričnu enkripciju i RSA algoritam za asimetričnu enkripciju. Bass-o-Matic algoritam je razvio sam Zimmermann i ubrzo se pokazalo da je algoritam slab i da ga je lako probiti jednostavnim tehnikama kripto-analize. RSA (Rivest Shamir Adleman) algoritam za asimetričnu enkripciju je u SAD-u bio zaštićen patentom u vlasništvu PKP (Public Key Partners) kompanije, što je uvelike sprječavalo širenje PGP softvera.

U drugoj verziji programa je algoritam Bass-o-Matic zamijenjen IDEA (International Data Encryption Algorithm) algoritmom koji je razvijen u Švicarskoj. Taj algoritam je također komercijalan i zaštićen patentom u Europi, SAD-u i Japanu. Za razliku od RSA patenta koji je u međuvremenu istekao i danas se slobodno koristi u svim inačicama PGP softvera, patent za IDEA algoritam stiče tek 2010. godine u SAD-u i 2011. u Europi, odnosno Japanu pa je implementiran samo u komercijalnim verzijama PGP softvera. Licence za korištenje IDEA algoritma izdaje švicarska firma MediaCrypt AG, a ako se IDEA algoritam koristi u privatne i neprofitabilne svrhe licencu nije potrebno platiti.

Verzija 2.5 je umjesto RSA algoritma koristila besplatnu RSAREF biblioteku funkcija koju je objavila tvrtka PKP. To je prva verzija koju je bilo legalno distribuirati unutar SAD-a.

Širenje softvera izvan SAD-a je i dalje bilo ilegalno zbog izvoznog zakona ITAR (International Traffic in Arms Regulations), koji zabranjuje izvoz izvan SAD-a svake tehnologije koja se može upotrijebiti za proizvodnju oružja, a tu spadaju i algoritmi za enkripciju podataka. Naravno, takav zakon je u praksi bilo nemoguće provesti i PGP softver se vrlo brzo proširio preko Interneta. Zbog toga je vlada SAD-a Philu Zimmermannu prijetila sudskom tužbom koja je na kraju odbačena. Iz koda koji je ilegalno izvezen iz SAD-a je nastala nova verzija programa nazvana PGPi (PGP International), koja se dalje samostalno razvijala u Europi.

Phil Zimmermann je osnovao kompaniju PGP Inc. koja je preuzela razvoj PGP softvera i 1997. godine izlazi PGP verzija 5.0 sa podrškom za brojne enkripcijske algoritme. Za simetrični dio enkripcije je podržavala algoritme: IDEA, Triple-DES i CAST, a za asimetrični dio: RSA, Hellman (El Gamal) i DSS/DSA algoritme. Kao *hash* algoritmi mogli su se iskoristiti MD5 ili SHA-1 algoritmi. 1998. godine pojavila se nova inačica 6.0 koja je prva imala podršku za integraciju s uredskim programima kao što su MS Outlook ili MS Outlook Express.
Prva verzija GnuPG (GNU Privacy Guard) programa je razvijena 1999. godine. GnuPG program je nastao unutar *open source* zajednice kao odgovor na brojne patentne i druge zakonske probleme koji su se javljali kod distribucije PGP programa.

3. Princip rada

Programi PGP i GnuPG omogućavaju šifriranje i digitalni potpis dokumenata. Princip rada oba programa je sličan i bazira se na kombinaciji raznih enkripcijskih algoritama kako bi se postigla što veća razina sigurnosti. Za opis rada programa prvo je potrebno dati kratak opis enkripcijskih algoritama koje programi koriste.

3.1. *Hash* algoritam

Hash algoritam je poseban skup matematičkih operacija kojima se iz dokumenta generira jedinstven sažetak koji se još zove i *hash* kod ili otisak poruke (engl. *message digest*). Korisna karakteristika takvog otiska je činjenica da je gotovo nemoguće proizvesti dva različita dokumenta za koje će algoritam proizvesti jednak otisak i gotovo je nemoguće iz poznatog otiska ponovo kreirati izvorni dokument. Na taj način je moguće dva puta generirati otisak nekog dokumenta i ako su otisci jednaki, to je dokaz da su generirani iz istog dokumenta. U okviru kriptografskih sustava *hash* algoritmi najčešće se koriste za zaštitu dokumenata od neovlaštenih promjena tijekom prijenosa.

3.2. Simetrična enkripcija

Simetrična enkripcija je postupak u kojem se za šifriranje i dešifriranje dokumenta koristi isti kriptografski ključ. Prednost ovakvih algoritama je velika brzina šifriranja i dešifriranja te velika sigurnost. Mana je uvjet da obje strane u komunikaciji moraju znati tajni ključ, a njega nije lako razmijeniti na siguran način.

3.3. Asimetrična enkripcija

Asimetrična enkripcija umjesto jednog ključa za enkripciju koristi par ključeva. Potpuno je svejedno koji se od ta dva ključa koristi za šifriranje poruke, ali se za dešifriranje mora koristiti odgovarajući ključ iz istog para. Jedan ključ se javno objavi (javni ključ), dok drugi ostaje u tajnosti (privatni ili tajni ključ). Na taj način je moguće slati poruke bez prethodne razmjene ključeva jer svatko može šifrirati poruku s javnim ključem, ali je samo osoba kojoj je namijenjena može dešifrirati svojim tajnim ključem. Takav algoritam omogućava i digitalno potpisivanje dokumenata jer ako netko šifrira dokument sa svojim tajnim ključem onda ga svatko može dešifrirati s javnim ključem i biti siguran da dokument stvarno potječe od te osobe.

3.4. Opis rada PGP/GnuPG programa

Za digitalno potpisivanje dokumenata prvo je potrebno kreirati njegov otisak primjenom nekog od podržanih *hash* algoritama. Taj otisak se šifrira privatnim ključem pošiljatelja i dodaje na početak poruke. Primatelj može dešifrirati otisak pomoću javnog ključa pošiljatelja i usporediti otisak s otiskom koji je sam generirao iz dokumenta koji je primio. Ako su otisci jednaki, onda može biti siguran da je poruka stvarno došla od osobe koja je deklarirana kao pošiljatelj i da dokument u međuvremenu nije bio promijenjen. Ako se program koristi samo za digitalni potpis bez enkripcije, onda se dokument šalje nešifriran i primatelj može jednostavno zanemariti potpis, ukoliko ga ne zanima autentičnost poruke.
Kod šifriranja se dokument najprije komprimira ZIP algoritmom, a nakon toga šifrira odgovarajućim simetričnim algoritmom. Ako je dokument potpisan onda se komprimira i šifrira sa već dodanim

potpisom. Dokument se komprimira da se ukloni redundantna informacija iz dokumenta prije šifriranja jer se na taj način postiže puno bolja zaštita (i naravno, manji dokument). Kako je ZIP nedeterministički algoritam, onda se *hash* otisak mora generirati prije kompresije.
Ključ za simetrični algoritam enkripcije se generira automatski kao slučajna vrijednost i svaki puta je drukčiji. Taj ključ se šifrira asimetričnim algoritmom pomoću javnog ključa primatelja poruke i dodaje na početak poruke.
Prije korištenja programa potrebno je generirati barem jedan par ključeva za asimetričnu enkripciju. Program na slučajan način generira takav par ključeva. S obzirom da je generirani ključ predugačak da ga korisnik pamti i upisuje svaki put kada želi šifrirati dokument, privatni se ključ šifrira pomoću posebne kratke šifre (tzv. *passphrase*) i pohranjuje na lokalni disk. Tu šifru je potrebno upisati svaki puta kada se dokument šifrira pomoću privatnog ključa. Isto tako, prije svake komunikacije osobe moraju izmijeniti javne ključeve, što je najlakše napraviti objavljivanjem ključa na za to specijaliziranim poslužiteljima (engl. *keyservers*).

3.5. Sigurnost programa

GnuPG/PGP programi su otporni na sve trenutno poznate tehnike kripto-analize osim na napad primjenom sile (engl. *brute force*), ali za maksimalnu sigurnost potrebno je strogo pridržavanje određenih pravila.
Kao što je već opisano u prethodnom poglavlju, privatni ključ je pohranjen na lokalnom disku i šifriran pomoću posebne šifre. Osoba koja može pročitati datoteku u kojoj je zapisan ključ teoretski može dešifrirati ključ. To je pogotovo opasno ako se koriste "slabe" zaporke koje se baziraju na pojmovima iz svakodnevnog života. Ovakve zaporke vrlo je lako kompromitirati primjenom tzv. *dictionary attack* napada, koji koristi bazu riječi iz različitih rječnika kao izvor za pogađanje zaporki. Na UNIX operacijskom sustavu moguće je zbog praktičnosti tajnu zaporku zapisati u posebnu varijablu okoline sustava, no to jako narušava sigurnost programa jer zaporku tada može pročitati svatko tko ima pristup ljusci sustava (u nekim verzijama sustava za to čak nisu ni potrebne administratorske ovlasti).
Svi ključevi se generiraju unutar programa na slučajan način. Za sigurnost ključeva potrebno je da oni zaista budu slučajno izabrani, tj. potreban je kvalitetan generator slučajnih brojeva. Mnogi operacijski sustavi imaju ugrađen generator slučajnih brojeva, ali njihovo ponašanje se često može predvidjeti određenim matematičkim postupcima. Mnoge verzije GnuPG/PGP programa imaju ugrađene svoje generatore slučajnih brojeva, koji svoj rad baziraju na praćenju kretanja miša, pritiskanju tipki na tastaturi i nekih drugih procesa u sustavu koji se događaju u slučajnim intervalima. Postoje i razni komercijalni alati za generiranje slučajnih vrijednosti.
Nužan preduvjet za komunikaciju je da osobe razmijene svoje javne ključeve. Na Internetu postoje specijalizirani poslužitelji na kojima svatko može objaviti svoj javni ključ ili više njih te skinuti javne ključeve osoba s kojima želi komunicirati. Problem je što svatko može postaviti svoj javni ključ na poslužitelj i deklarirati ga kao da pripada nekoj drugoj osobi te na taj način dešifrirati sve poruke koje su namijenjene toj drugoj osobi.
Osobe koje žele komunicirati moraju pronaći treću osobu kojoj obje vjeruju, koja će svojim tajnim ključem potpisati javne ključeve koje treba razmijeniti. U sustavu sa mnogo javnih ključeva svaka osoba može digitalno potpisati ključeve drugih osoba kojima vjeruje i na taj način se stvara mreža isprepletenih garancija koja se zove mreža povjerenja (engl. *web of trust*).
Danas postoje posebne organizacije koje rade uslugu potpisivanja javnih ključeva i oni tada garantiraju autentičnost objavljenog javnog ključa. Takva garancija se naziva digitalni certifikat, a sustavi koji ih izdaju i održavaju se nazivaju PKI (engl. *Public Key Infrastructure*).

4. Dostupan softver

Danas postoje tri razvojne linije softvera baziranog na *OpenPGP* standardu. To su:

- PGP verzije 2.x
- PGP verzije 5.x ili više
- GnuPG

PGP programi verzija 2.x se razvijaju zasebno i kod svake nove verzije raste druga znamenka (prva znamenka je uvijek 2). Najnovija verzija koja postoji je 2.6. Taj softver je besplatan, razvija se unutar

open source zajednice i dostupan je na mnogim Internet stranicama. Glavni distributer ovih verzija programa u SAD-u je MIT. Program je moguće koristiti samo iz naredbenog retka i ne postoji grafičko sučelje. Iako je program besplatan i slobodan za korištenje u SAD-u, još uvijek ga je ilegalno izvoziti izvan SAD-a.
PGP program verzija 5.x i većih je komercijalni softver koji razvija i prodaje PGP korporacija koju je 1996. godine osnovao Phil Zimmermann. Zadnja verzija koja postoji na tržištu je PGP 8.0.3 i postoje verzije za Windows i Mac OS operacijske sustave.
Program ima intuitivno grafičko sučelje. Kod instalacije se integrira s aplikacijama za rad s elektroničkom poštom, kao što su MS Outlook i MS Outlook Express, a omogućava i zaštitu dokumenata pohranjenih na lokalnom disku. Postoje verzije programa za zaštitu jednog računala, ali i verzije za zaštitu cijele mreže.
GPG (GNU Privacy Guard) je program koji je nastao kao *open source* alternativa PGP alatu. GPG ne koristi algoritme koji podliježu bilo kakvim softverskim patentima. Program podliježe GPL licenci pa ga je moguće slobodno koristiti, kopirati, modificirati i distribuirati.
GPG je kompatibilan sa *OpenPGP* standardom, a na Internetu je moguće pronaći i neslužbene dodatne module koji dodaju podršku za IDEA algoritam. Program postoji u verzijama za Linux, Windows, Unix i Mac OS operativne sustave.
Instalacijski paket se može skinuti sa adrese http://www.gnupg.org, a osim toga postoji u sastavu mnogih Linux distribucija i raznih drugih paketa kao što je Cygwin. Osnovna verzija programa se pokreće iz naredbenog retka, ali postoje i grafička sučelja koja olakšavaju upotrebu programa. Najpoznatije grafičko korisničko sučelje za Windows operacijski sustav je WinPT (Windows Privacy Tools), program koji također podliježe GPL licenci i dostupan je na spomenutoj Web adresi.
Za integraciju GPG alata u druge programe postoje posebne biblioteke funkcija napisane za programski jezik C++.

5. Rad s GnuPG/PGP alatima

U ovom poglavlju će biti ukratko opisan princip rada s GnuPG programom na Linux operacijskom sustavu i PGP 8.0.3 programom na Windows operacijskom sustavu.

5.1. Rad s GnuPG programom

Prije početka rada s programom potrebno je generirati par ključeva koji će se koristiti u asimetričnoj enkripciji. U GPG alatu to se radi pomoću naredbe:
 # gpg --gen-key
Nakon pokretanja naredbe pojavljuje se tekstualni izbornik u kojem treba izabrati razne parametre za generiranje ključa. Osim upisivanja imena i adrese elektroničke pošte, treba izabrati algoritam koji će se koristiti za asimetričnu enkripciju, duljinu ključa i vremensko razdoblje nakon kojeg ključ više neće vrijediti.
Ključ se generira uz pomoć slučajnih vrijednosti koje program skuplja iz ugrađenog generatora slučajnih brojeva. Kod Linux operacijskog sustava tom generatoru se pristupa preko datoteke */dev/random*. Sigurnost ključa može se povećati unošenjem slučajnih znakova preko tastature.
Generirani ključ se može ispisati naredbom:
 # gpg --armor --export
Opcija *--armor* određuje hoće li ključ biti zapisan u tekstualnom ili binarnom obliku. Ključ se može pohraniti i u datoteku preusmjeravanjem standardnog izlaza.
Ključevi se mogu učitati u program iz datoteke naredbom:
 # gpg --import [ime_datoteke]
Naredba:
 # gpg --fingerprint
ispisuje otisak pohranjenih ključeva. To je jedan od načina kako se može provjeriti autentičnost primljenog ključa.
Datoteka se šifrira naredbom:
 # gpg --recipient [primatelj] --encrypt [ime_datoteke]
Primatelj je osoba kojoj je poruka namijenjena i biti će šifrirana njenim javnim ključem. GPG program mora imati javni ključ te osobe u svojoj bazi. Ako primatelj nije naveden program će tražiti da se

navede. Rezultat ove naredbe će biti nova datoteka s imenom: *ime_datoteke.gpg*. To je binarna datoteka koja nije pogodna za slanje putem elektroničke pošte. Program može generirati i tekstualnu datoteku s imenom *ime_datoteke.asc* i to se postiže naredbom:
 # gpg --recipient [primatelj] --armor --encrypt [ime_datoteke]
Primjer jedne šifrirane datoteke je dan u nastavku:

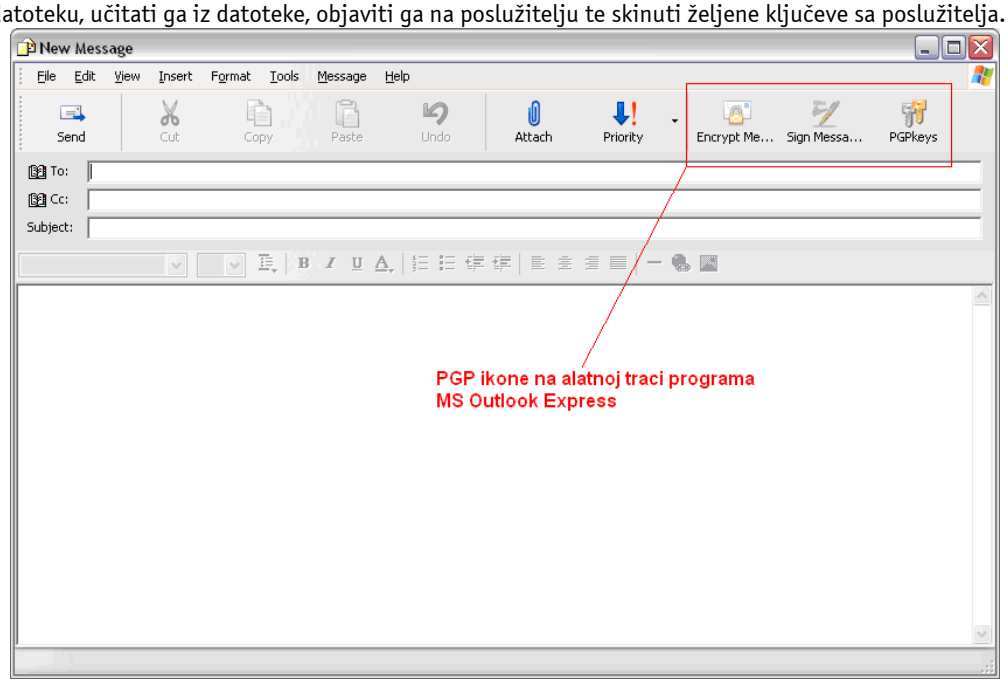
```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.2.3 (GNU/Linux)

hQINA3Pf4rrcJwg4EAf4sWGzynNQmpYXb2CAs8aO48ZOjFP7PlOWpqOkofaRiuV+
IdzU6j8xb2zWqpgMtyQhSg3AXO7wMv5Ei+6dXEg+C6VISduifKDG6leM0wTSQ+Ts
KbNRYATgNWif0knvMxgpBDzlHi0TNxPCaDdsX6fECcv6clv786bsBJnJMqX6p0ad
ppGwP0/kGRgKcU7ud80HPQPp0OU14a4WxswjUU3rWfbB6MeCGhXkwW3tZFqWPO3N
XPbY/6rvu3J8Fs96Llq6Jzixg/NkyRSKA/v1xoLxUFn9fbDrpGLjtaB9JpaUZ8XU
bfNrxVaFFppey7bBDMwSSII4rkl0e0m/DnsGawTbB/4qy9MQmJGa3ddCoE7phhKN
rxRobRYpn8EGi9quje0Pt0ggSxG7ekUBZ9h+IZiN/UZJkBkVZahh9+ZIgpt6oQpN
YRrZ80KR5I+YRSSX2kzS43wQn4YuDvDTvvzL32+d4qGIB9YfC9dptd3gI+6QTaqH
+wp/sxujDtzmB9sLy+DxKGRTbF8trLdIGhuas+DcsmuVxg+lZtTCsX+lKDEarH+K
joNSTMZBUppz5QDwUzGQOzvQqaebi3zD2q3ODGHHMuE4Cu7SZE7xEEkOQSr4oJwz
eynSOyujtCaMqm+S9N2TVLT7Hv6/PZVhXnwsXUaBCYyRE7FGqWXIQOZpXcNrZrun
0ncB/oPlmZYAHCfzCy+xVR3hFiLU3bF0CTzcYuomGHI78rDyT6ebLL15WzNUWnE4
oiZiVxBTRchsiSCQ+/iUIYwmvf1cPk5CtViGUSnhEJOevHXF9dye080k0iHcadbY
S0npfVkHZ1OjNZooFIjCslaVmvZOEMwGIQ==
=EpqN
-----END PGP MESSAGE-----
```

Datoteka se dešifrira pomoću naredbe:
gpg --decrypt [ime_datoteke]
Program će nakon toga tražiti zaporku kojom je šifriran tajni ključ kojim treba dešifrirati poruku. Dešifrirana datoteka će biti ispisana na standardni izlaz odnosno na ekran. Izlaz se i ovdje može pohraniti u datoteku preusmjeravanjem standardnog izlaza.
Potpisivanje datoteka može se napraviti na dva načina. Prvi način je potpisivanje datoteke i spremanje dokumenta i potpisa zajedno u novu datoteku s ekstenzijom *.gpg*. To se može napraviti s naredbom:
gpg --sign [ime_datoteke]
Kao i kod šifriranja dokumenta, umjesto binarne datoteke moguće je kreirati tekstualnu datoteku pomoću opcije *--armor*. Drugi način je spremanje potpisa u posebnu datoteku s ekstenzijom *.sig*. Za to služi naredba:
gpg --sign-detach [ime_datoteke]
Ova posljednja opcija je korisna kada se šalje dokument koji nije šifriran.
Autentičnost digitalnog potpisa se provjerava naredbom:
gpg --verify [ime datoteke]
ako je potpis integriran s dokumentom u istoj datoteci, a ako je u posebnoj datoteci onda se koristi naredba:
gpg --verify [potpis] [ime_datoteke]
Digitalno potpisivanje i šifriranje datoteke se može napraviti istovremeno naredbom:
gpg --encrypt --sign [ime_datoteke]

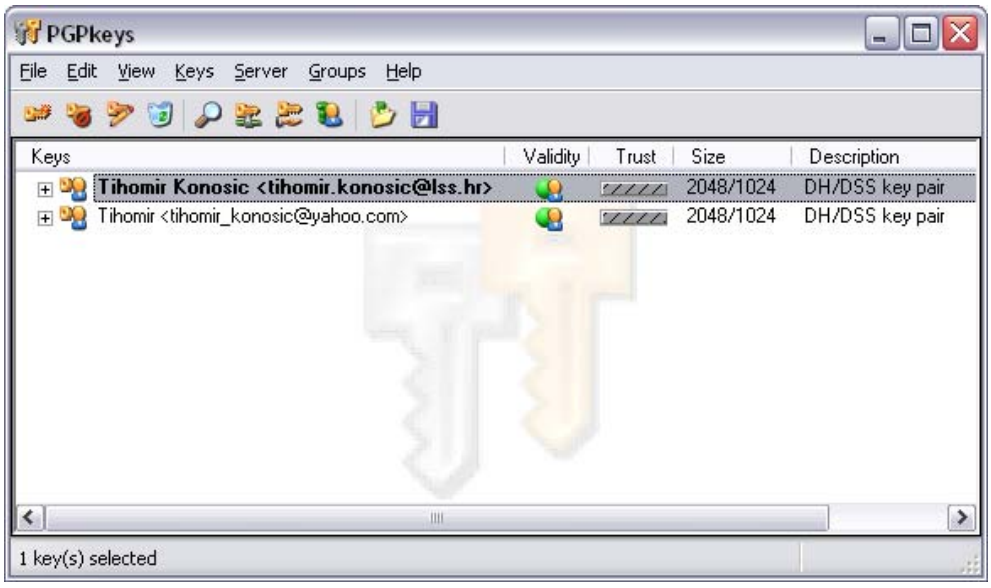
5.2. Rad s PGP programom

Program PGP 8.0.3 ima grafičko sučelje koje olakšava rad s programom. Program je komercijalan, ali postoji verzija za osobnu, nekomercijalnu, upotrebu koja se može besplatno skinuti s adrese http://www.pgp.com. Ovaj opis se odnosi na tu verziju.
Program ima podršku za integraciju s programima MS Outlook, MS Outlook Express, Qualcomm Eudora, GroupWise i ICQ.
Za generiranje ključeva postoji poseban prozor koji se može pokrenuti klikom na ikonu u alatnoj traci programa MS Outlook Express, kao što je vidljivo na Slika 1, ili iz Windows Start izbornika. Prozor za

generiranje ključeva je prikazan na Slika 2. Osim generiranja ključeva, program može snimiti ključ u datoteku, učitati ga iz datoteke, objaviti ga na poslužitelju te skinuti željene ključeve sa poslužitelja.



Slika 1: *MS Outlook Express sa integriranim PGP programom*



Slika 2: *Prozor za rad s ključevima*

Šifriranje i digitalno potpisivanje poruka elektroničke pošte u programu MS Outlook Express se postiže klikom miša na odgovarajuće ikone na alatnoj traci.

6. Zaključak

Oba programa koriste slične algoritme enkripcije i sigurnost im je podjednaka. Program GnuPG nema podrške za algoritme koji su komercijalni ili zaštićeni patentima poput IDEA-e, ali sigurnost tih algoritama u usporedbi sa sličnim besplatnim algoritmima ne pravi razliku.

PGP program nema podrške za UNIX i Linux operacijske sustave pa je GnuPG program tu jedini izbor. GnuPG program je razvijen za Linux platformu, ali postoje verzije i za Windows i Mac OS sustave.
Program GnuPG je razvijen kao alat iz naredbenog retka, ali su danas razvijena mnoga grafička sučelja koja olakšavaju rad s programom, kao WinPT za Windows te GnomePGP i KGPG za Linux operacijski sustav.
Prednost programa PGP je u boljoj integraciji s postojećim uredskim aplikacijama, a mana je njegova cijena. GnuPG program je besplatan i potpuno slobodan za korištenje, mijenjanje i distribuciju.

7. Reference

PGP FAQ, http://www.uk.pgp.net/pgpnet/pgp-faq/pgp-faq.html
Cryptography, http://axion.physics.ubc.ca/crypt.html
GPG manual stranice
Using PGP/GnuPG and S/MIME with Email, Tilman Linneweh