Sigurnost elektroničke pošte i PGP

priredio: Dinko Korunić

inačica 2.1
veljača 2002.

Ciljevi tečaja

- namijenjen naprednim korisnicima
- upoznavanje problematike sigurnosti elektroničke pošte
- uvod u šifriranje i dešifriranje upotrebom tehnike javnih i tajnih ključeva
- zaštita elektroničke pošte pomoću PGP
- korištenje PGP i MS Outlook Express

Predznanje

- **nužno**:
  - osnovna kompjuterska pismenost
  - osnove rada s MS Windows sustavom (W100)
  - osnove elektroničke pošte (A300, odnosno A320)
  - osnove Interneta (A100)
- opcionalno:
  - razumijevanje rada elektroničke pošte

Sadržaj

- Cjelina I – osnovni uvod u problematiku
  - Uvod
  - Potreba zaštite podataka
  - O šifriranju i ključevima
- Cjelina II – koncepti PGP i korištenje
  - PGP – program
  - PGP - koncept ključeva i prstenova
  - PGP - stvaranje vlastitog ključa
  - PGP - izlaganje javnog ključa ostalim korisnicima
  - PGP - pronalaženje potrebnih javnih ključeva
  - PGP - lokalno spremanje javnih ključeva
- Cjelina III – korištenje PGP sa Outlook Express
  - PGP i MS Outlook Express - osnove rada
  - PGP i MS Outlook Express - šifriranje/dešifriranje poruke
  - PGP i MS Outlook Express - potpisivanje/provjera potpisa

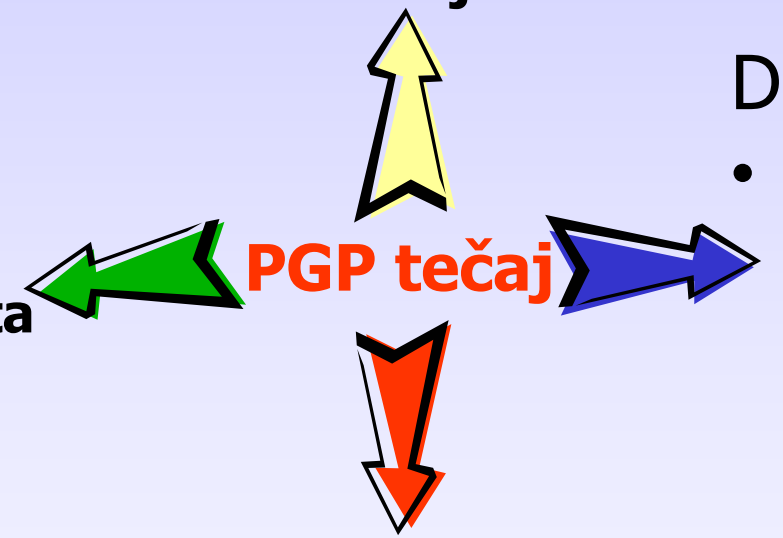
Ostali tečajevi

Stari tečajevi:

- **nekadašnji B100**

Predtečajevi:

- **Windows**
- **Osnove interneta**
- **Elektronička pošta**



Daljnji tečajevi:

- **Pronalaženje informacija na Internetu**

Unix alternativa:

- **Javni servisi (treći dan)**

Tijekom predavanja..

- **Vaša pitanja su poželjna i potrebna** – **kratke** diskusije su **produktivne**
- Ako je štogod prebrzo – zatražite da vam se **ponovi**
- Ako je presporo – **ubrzat** ćemo!
- Radne zadatke **nije nužno dovršiti** ali je **poželjno**
- Anketu je **potrebno ispuniti**

Uvod

Potreba zaštite podataka

O šifriranju i ključevima

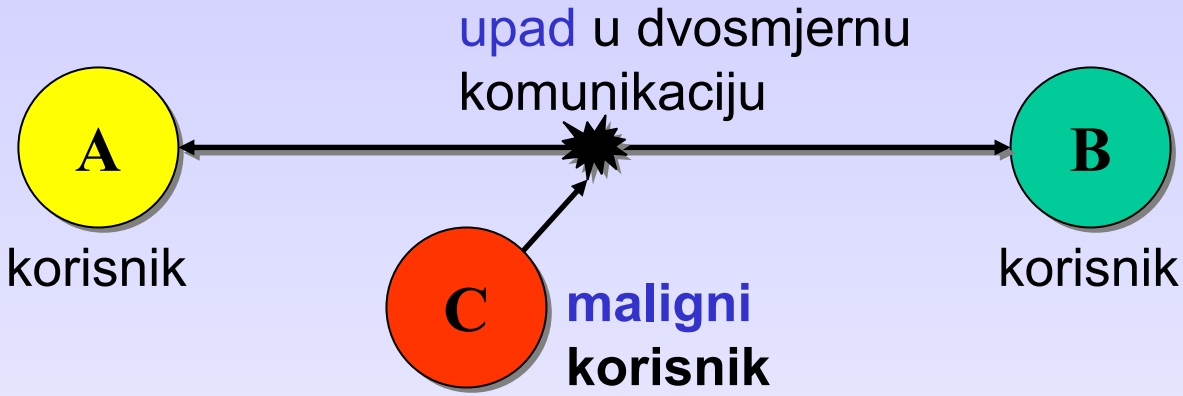
(kratki osvrt na kriptografiju)

Uvod (1)

- e-mail – rasprostranjena svakodnevna moderna komunikacija: posao, razbibriga, itd.
- e-mail – pošta čiji se sadržaj treća osoba može vidjeti u svakom trenutku
- e-mail se može krivotvoriti = treća osoba lažno šalje drugoj osobi tako da izgleda da je od prve osobe

- **napredak** tehnologije + educiranost **malignih korisnika** = mogućnost **zloupotrebe**

Uvod (2)



- komunikacija u vidu čistog teksta (ASCII) ⇒ prisluškivanjem dolazimo do **potpunog** sadržaja tuđih poruka
- potreba za **efikasnom** i **jednostavnom** **zaštitom** dostupnom svima

Potreba zaštite podataka (1)

- e-mail problematika:
  - upitan sadržaj - protokol čistog teksta = treća osoba može pročitati i izmijeniti
  - upitno izvorište – zaglavlje se može dobro krivotvoriti, pa čak i poslati sa lažnog poslužitelja
  - upitna odredište – može se preuzeti tuđi e-mail

- moguća rješenja:
  - moderna kriptografija: tuneli, šifriranje, ...

Potreba zaštite podataka (2)

- P: Čemu podatke uopće zaštićivati?
- O: U poslovne, znanstvene, privatne svrhe. Koja je svrha komunikacije u kojoj nemate privatnosti, u kojoj niste sigurni s kime pričate, da li će druga strana uopće dobiti vaše poslane podatke ili nečije tuđe i slično? Čitanje tuđe pošte predstavlja kršenje osnovnih prava pojedinca, pa čemu to nekome dozvoliti!

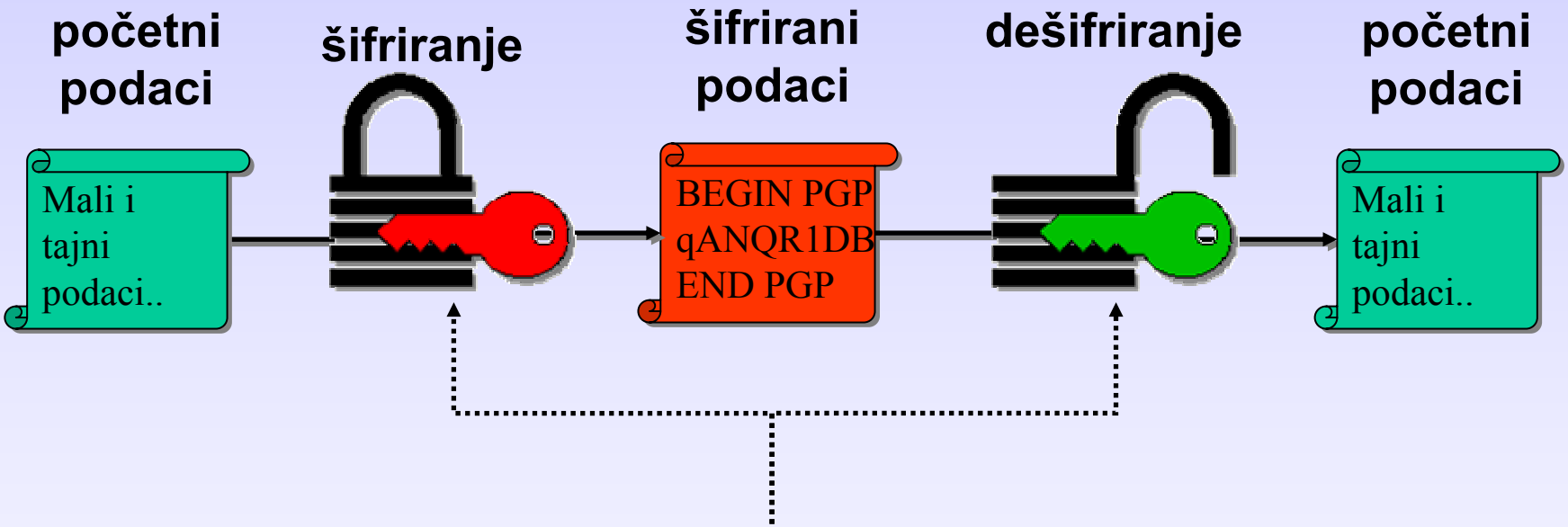
O (de)šifriranju (1)

- V. Anić "Rječnik hrvatskog jezika": **kripto-** kao prvi dio rečenice znači tajni, potajan, skriven [*~grafija* tajno pismo]
- **kriptografija** (šifriranje) = moderna znanost bazirana na primijenjenoj matematici:
  - nekad korištena u ratu zbog tajnosti
  - danas sve veća primjena u informatici: MD5sum, passwd, SSH, S/Key, PGP, OpenBSD, ...
  - postoji hardver koji obavlja kripto-funkcije

O (de)šifriranju (2)

- šifriranje = skrivanje podataka i transformiranje u obično neprepoznatljiv sadržaj
- dešifriranje = konverzija iz neprepoznatljivog šifriranog oblika u "čitljiv" oblik
- ključ – podatak koji omogućava šifriranje ili dešifriranje
- "caesar" šifriranje: Julije Cezar je radi zaštite tajnosti slao generalima poruke u kojima je A postajalo D, B je bilo E, itd.; svako slovo je bilo pomaknuto za 3
- ROT13 – sreće se često na Usenetu, rotiranje za 13

O (de)šifriranju (3)



Ključevi (1)

- ključ – podatak (jedan ili više) koji uz poznati algoritam vodi do početnih podataka i obrnuto

- nekada davno:
  - samo jedan ključ za šifriranje i dešifriranje - u WW2 je to bila crna kutija koja "nešto" radi
  - inicijalno je potrebno “sigurno” prenijeti ključ
  - sigurnost šifriranih podataka = sigurnost inicijalnog ključa!
  - stručan naziv: "standardni kriptosistemi"
  - velika brzina rada naspram “jakog” šifriranja
- “jako šifriranje” – nešto što se teško može provaliti u “normalnom” vremenu sa “normalnom” opremom

Ključevi (2)

- prva mogućnost:
  - ključ za šifriranje isti kao i za dešifriranje = **jedinstveni ključ** ⇒ simetrično šifriranje
  - jednostavnije, brže, no ako se ključ ukrade - sve pada u vodu
- druga mogućnost:
  - **dva odvojena ključa** - jedan za šifriranje, jedan za dešifriranje ⇒ asimetrično šifriranje
  - ključ za šifriranje ne mora biti tajan!
  - vrlo sigurno, kvalitetno, sporo, ali tajno

Ključevi (3)

- treća mogućnost:
  - na poseban način dobije se nekakva suma iz početnog sadržaja
  - takva suma služi **samo** za provjeru autentičnosti i nepromijenjenosti sadržaja
  - jednosmjerno šifriranje ⇔ nema reverzibilnosti, iz odredišne sume se ne može dobiti početni sadržaj!

- danas se koriste kombinacije simetričnog i asimetričnog šifriranja u svakodnevnom radu: Windowsi, Unix, GSM, banke, itd.

Javni i tajni ključ

- PGP = kriptosistemi bazirani na dva odvojena ključa:
  - **javni ključ** (public key): isključivo služi za šifriranje poruke **osobi čiji je taj ključ**; slobodno se prenose različitim medijima: HTTP, LDAP, finger, mail
  - **tajni ključ** (secret key, private key): **služi za dešifriranje** te iste poruke, bez njega je to nemoguće!; lokalno spremljen i najčešće zaštićen tajnom rečenicom (> od jedne riječi!)

Potpis (1)

- javni i tajni ključ - služe samo za sigurno komuniciranje
- što ako nam **ne treba tajnost**, ali nam treba **potvrda** da je sadržaj od **neke određene** osobe i još k tome **nepromijenjen**?
- odgovor: jednosmjerno šifriranje (MD5 sume, CRC16 i CRC32 cikličke sume, itd.):
  - danas se mnogo koristi za kvalitetu sadržaja
  - harddiskovi, CDROMovi, kartice, računala, ECC

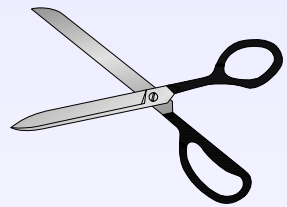
Potpis (2)

- možemo i potpisati tuđi javni ključ:
  - time garantiramo za drugu osobu
  - njegov javni ključ i naš potpis zajedno tvore certifikat

- potpis nam omogućava:
  - provjeru od koga je poruka/sadržaj = izvornost
  - provjeru nepromijenjenosti sadržaja = cjelovitost
  - provjeru tuđeg ključa = neporecivost

Sažetak (1)

- e-mail = protokol "čistog teksta"
- ključevi: tajni + javni
- jaka kriptografija (javni/tajni ključevi):
  - javni ključ + originalni podaci = šifrirana poruka
  - tajni ključ + šifrirana poruka = originalni podaci
  - reverzibilnost, tajnost
- potpis:
  - autentičnost, izvornost



PGP

PGP kao program

Koncept ključeva i prstenova

stvaranje vlastitog ključa

Izlaganje javnog ključa ostalim korisnicima

Pronalaženje potrebnih javnih ključeva

Lokalno spremanje javnih ključeva

PGP – program (1)

- PGP = Pretty Good Privacy
- autor Phil Zimmerman – nedavno otišao iz PGP kompanije (odnosno Network Associatesa)
- najraširenija program za zaštitu e-mailova i podataka općenito:
  - PGP2, PGP5, PGP6
  - posljednja verzija (u razvoju) je PGP7
- adresa:
  - http://www.pgpi.com/
  - http://www.pgp.com/
- alternative: GnuPG – pridržava se OpenPGP standarda, PGP2 kompatibilan

PGP – program (2)

- nudi mogućnost zaštite lokalnih podataka, e-mailova:
  - šifriranje - zaštita tajnosti sadržaja
  - potpisivanje – garancija autentičnosti, neporecivosti i nepromijenjenosti sadržaja
  - izuzetno kvalitetna zaštita: pojam "**military grade**" jakosti zaštite – takve da vojska uz pomoć superračunala ne može u razumnom vremenskom roku provaliti šifrirane poruke
- integracija u postojeća sučelja i OS-ove:
  - Unix: Pine, mutt, elm+me, (X)Emacs
  - Windows: MS Outlook, Eudora, Netscape Mail
- komandno-linijski ali i GUI program

PGP – sigurnost sigurnosti (1)

- da li je sam PGP siguran?

- **nekad**:
  - PGP koristio RSA algoritam - u to vrijeme smatrao se vrlo sigurnim
  - RSA se služi stvaranjem velikih slučajih primitivnih brojeva - da bi se poruka provalila treba takav broj rastaviti u jednostavne faktore (faktorizirati)
  - jučerašnja superbrza računala su danas spora ⇒ brz razvoj industrije

PGP – sigurnost sigurnosti (2)

- vrijeme faktoriziranja pomoću Number Field Sieve algoritma (najbrži postojeći algoritam za brojeve veće od 110):
  - 768 bit : 200,000,000 MIPS-godina
  - 1024 bit : 300,000,000,000 MIPS-godina
  - **2048 bit : 300,000,000,000,000,000,000** ...
- **danas**:
  - RSA se smatra **nesigurnim**
  - koriste se bolje, jače, sporije metode: Diffie-Helman, Digital Signature Standard, itd.

PGP – sigurnost sigurnosti (3)

- do danas nije pronađen način kako provaliti PGP poruku u razumnoj količini vremena
- mogući načini su:
  - ukrasti lozinku
  - nadgledati proces šifriranja uz pomoć najviših ovlasti
  - brute force napad
  - trojan napadi: lažni ključevi, lažni programi, itd.
  - prisluškivanje kompjuter - Van Eck zračenje
- pouka:
  - čuvajte svoje ključeve, generirajte što **veći** ključ (o tome kasnije)

PGP - koncept ključeva i prstenova (1)

- ključevi:
  - podaci koji služe za šifriranje, dešifriranje i potpisivanje
  - "slučajno" (pseudoslučajno) generirani i zaštićeni lozinkama
- dva tipa:
  - javni: svima dostupni, najčešće u ASCII obliku
  - tajni: zaštićeni lozinkom za slučaj da budu ukradeni, lokalno (na disku) spremljeni, u binarnom obliku

PGP - koncept ključeva i prstenova (2)

- jedna ovojnica, tzv. certifikat ključeva (key certificate) sadržavaja jedan ili više **tematski** vezanih ključeva sa svim njihovim dijelovima:
  - user ID (ime+prezime osobe ili login ili e-mail adresa)
  - vremenska oznaka kada je ključ stvoren = timestamp
  - sam materijal ključa

- tajni ključ ovdje služi i za "potpisivanje" poruka (digital signature) – primatelj pomoću javnog ključa osobe može provjeriti točnost izvora i sadržaja!

PGP - koncept ključeva i prstenova (3)

- stari način čuvanja sadržaja pisama - ostavljao se voštani pečat sa vlastitim žigom na koverti pisma

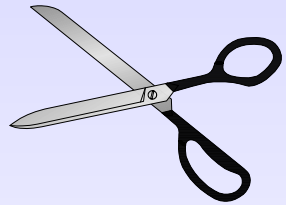
- digitalni potpis danas pomoću PGP:
  - sadržaj pisma šifriran tajnim ključem
  - sadržava samo kriptografsku sumu
  - nemoguće reproducirati
  - garantira autentičnost potpisanih podataka

PGP - koncept ključeva i prstenova (4)

- skup više ključeva je tzv. prsten ključeva, odnosno key ring – dijelimo na:
  - **tajne** = kolekcije vlastitih tajnih ključeva
  - **javne** = kolekcije tuđih ključeva
- svaki ključ ima svoju jedinstvenu oznaku:
  - "key ID" (usporedi sa JMBG)
  - 64 bitova najmanje važnosti
  - u radu se prikazuje donjih 32bita
  - služi za prepoznavanje

Sažetak (2)

- upotreba PGP:
  - šifriranje/dešifriranje – zaštita tajnosti sadržaja
  - potpisivanje – zaštita originalnosti (nepromjenjivosti) sadržaja
- ovojnice tajnih i javnih ključeva
- jedinstvena oznaka ključa
- tajni ključevi zaštićeni vlastitom lozinkom (niz riječi!)

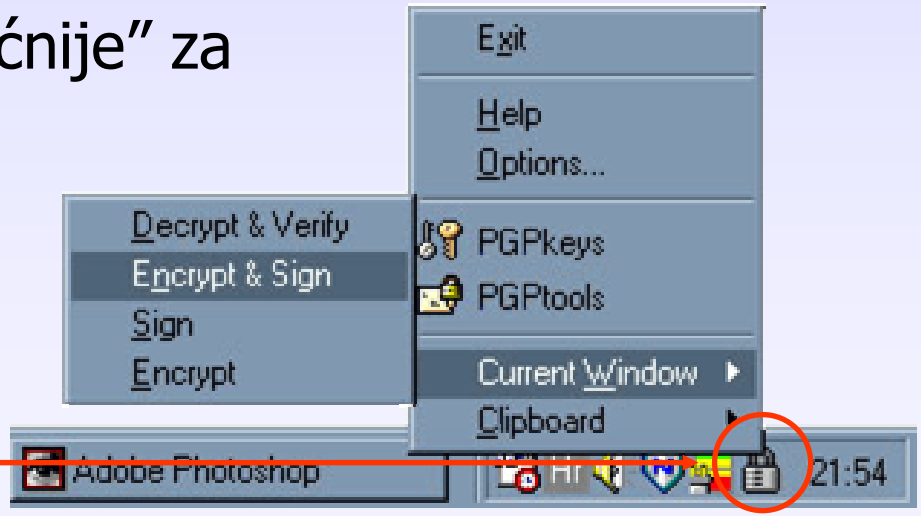


Pauza

10 minuta

PGP – osnovni rad (1)

- komandno-linijsko sučelje (CLI):
  - nužno znati opcije i parametre, za svakodnevni rad kompliciranije od GUI i nespretno
- grafičko sučelje (GUI):
  - jednostavnije i "moćnije" za korištenje
  - online pomoć
  - "prečaci"



PGP – osnovni rad (2)

- komandna linija:
  - pgp je osnovni i jedini program (verzija 5: pgpk, pgpv, pgps, etc.) za sve
- GUI programi:
  - PGPtools – niz alata za šifriranje, dešifriranje, brisanje i potpisivanje
  - PGPtray – prečaci u Windows taskbaru i Outlook/Eudora integracija
  - PGPkeys – baratanje privatnim i javnim ključevima
  - PGPLog – logovi o PGP akcijama/radnjama

PGP - stvaranje vlastitog ključa (1)

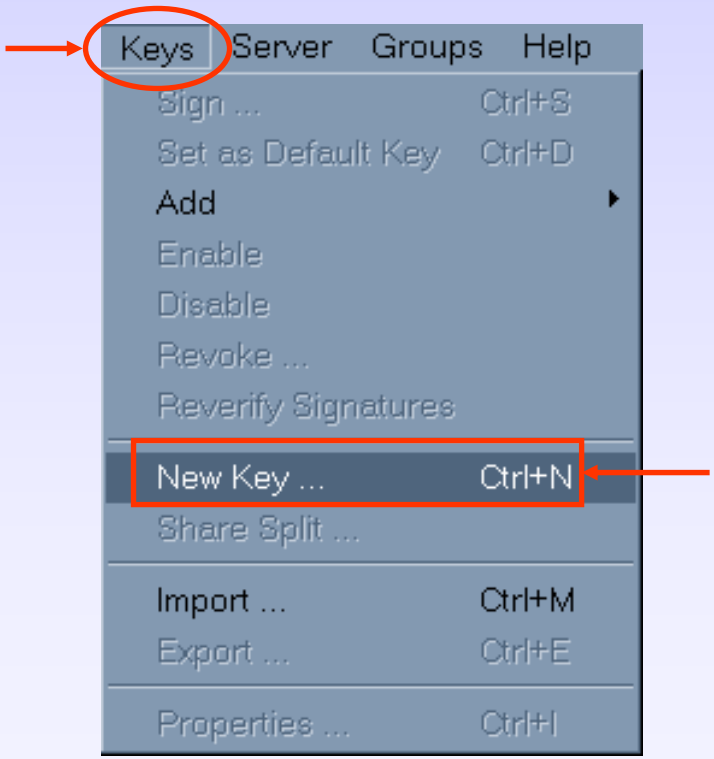
- stvaranje novog **vlastitog** ključa:
  - odabir imena i prezimena te e-mail adrese
  - odabir tipa ključa: RSA (staro!) ili DH/DSS (novo!) (napomena: DH=Diffie-Hellman, DSS=Digital Signature Standard)
  - odabir veličine/kvalitete ključa u bitovima: 1024, 1536, 2048, 3072 (povećavaju se DH bitovi ključa za šifriranje, DSS ostaje 1024 bita)
  - kada ključ ističe
  - zaštitna šifra (lozinka)

PGP - stvaranje vlastitog ključa (2)

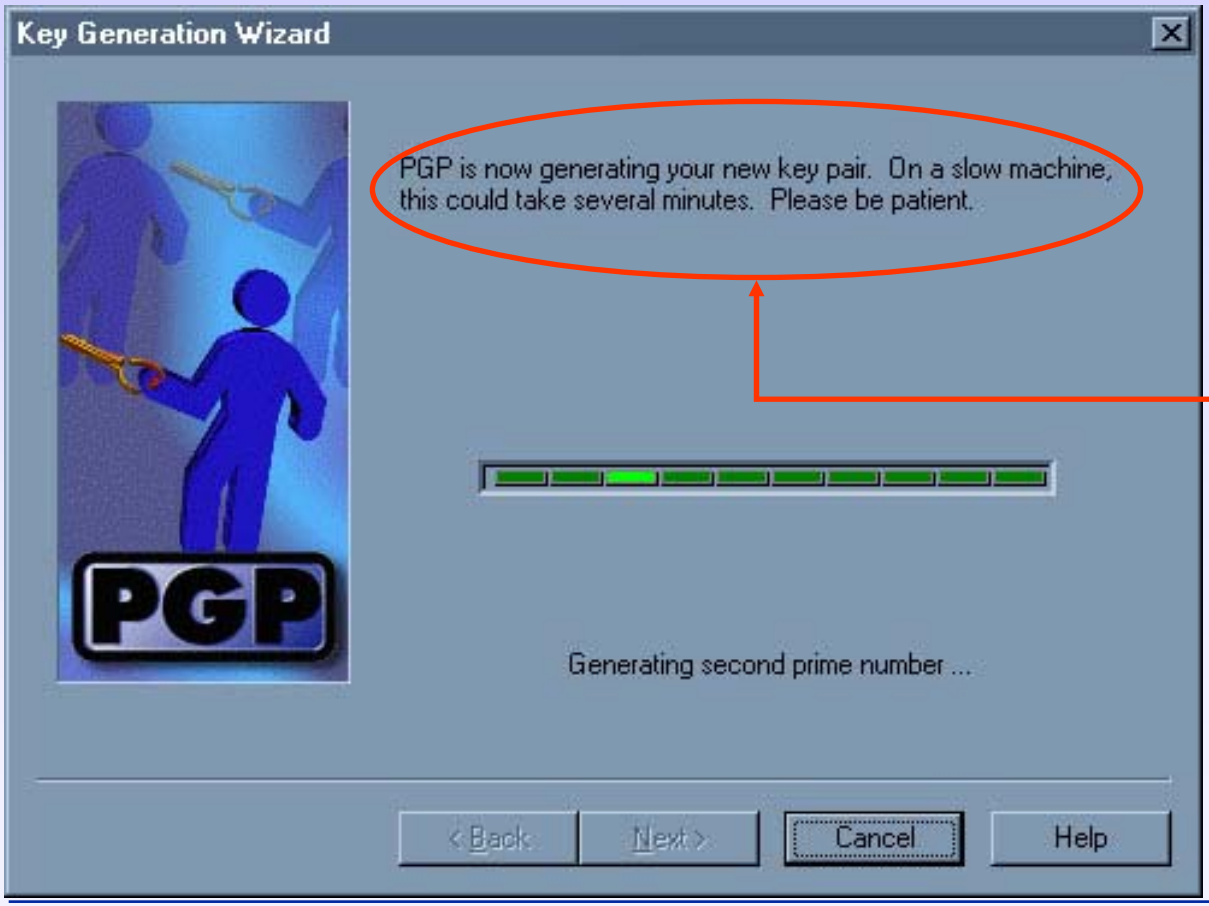
- komandnolinijski:

```
pgp -kg
```

- GUI:
  - odabrati u izborniku PGP pa zatim PGPkeys
  - mišem odabrati Keys pa zatim New key (ili pomoću kratica Ctrl+N)
  - unijeti podatke
  - pričekati neko vrijeme



PGP - stvaranje vlastitog ključa (3)



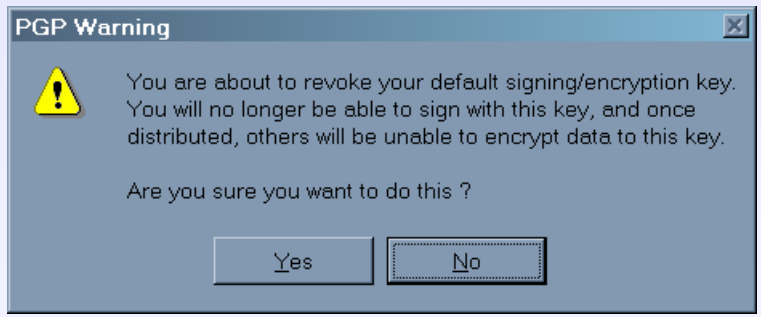
Generiranje slučajnih brojeva i samog novog PGP ključa u grafičkom programu nakon unosa svih potrebnih podataka

PGP - stvaranje vlastitog ključa (4)

- P: Što stvaranje ključa zapravo radi?
- O: Redom radi navedeno:
  - stvara privatni ključ zadane širine bitova koji se nalazi u vlastitom prstenu tajnih ključeva u datoteci "secring.skr"
  - upravo nam taj ključ omogućava potpisivanje i dešifriranje poruka
  - iz privatnog ključa moguće je stvoriti i javni ključ kojima se drugi koriste za slanje informacija **nama**

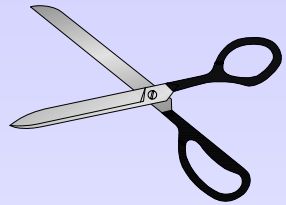
PGP - stvaranje vlastitog ključa (5)

- stvoreni tajni ključ se mora čuvati!
  - u slučaju krađe i/ili provale potrebno je stvoriti novi ključ kako smo već opisali
  - stari ključ se odbacuje, odnosno radi se "revoke" što opoziva ključ - proglašava nevrijedećim:
    - PGPkeys, označite ključ, Keys, Revoke, Yes
    - `pgp -e keyid`
  - takav nevrijedeći ključ treba "izložiti" (kao i novi vrijedeći!)



Sažetak (3)

- PGP CLI:
  - `pgp`
- PGP GUI:
  - PGPkeys, PGPtray, PGPtools
- vlastiti ključ:
  - ime, prezime, e-mail adresa, tip ključa, širina u bitovima, vrijeme trajanja, lozinka
- stvaranje ključa:
  - CLI: `pgp -kg` za stvaranje i `pgp -e <ključ>` za editiranje ključa
  - GUI: Ctrl+N, odnosno Keys, itd.



PGP - stvaranje vlastitog ključa, praktičan rad

- Zadatak - stvoriti **vlastiti** PGP ključ:
  - upisati točno *ime i prezime*
  - upisati točnu *e-mail adresu*
  - upisati proizvoljnu *lozinku* (potrebno je par riječi!) i zapamtiti je (preporučljivo zapisati na papir)
  - neka ključ bude *širine* 1024/1024 bitova
  - nakon što se generira **sačuvati** ga zbog vježbe u slijedećim poglavljima
- Predviđeno vrijeme: **15** minuta

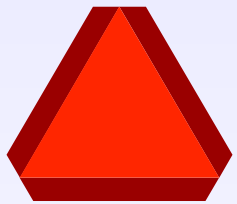
PGP - izlaganje javnog ključa (1)

- Zašto? Novostvoreni **javni** ključ potrebno je proširiti, dati drugim korisnicima da ga mogu koristiti – odnosno poslati šifrirani/potpisani mail **vama**
- Kako? Mogućnosti su razne:
  - http
  - ftp
  - PKS – HTTP/e-mail/LDAP
  - finger info
  - ...

PGP - izlaganje javnog ključa (2)

- PKS = javni poslužitelji javnih ključeva (Public Key Server) na Internetu:
  - rade preko: Weba (HTTP ili HTTPS), e-maila ili LDAP
  - ključevi im se šalju: iz PGP klijenta, odgovarajućih Web obrazaca ili pak e-mailom
  - većina PKS poslužitelja međusobno razmjenjuje ključeve – slanjem ključa na jedan poslali ste na sve umrežene!

- hrvatski PKS:
  - http://ds.carnet.hr:11371
  - http://pgp.rasip.fer.hr:11371



PGP - izlaganje javnog ključa (3)

- alternativni načini dostavljanja javnih ključeva:
  - npr. finger, ftp, e-mail, vlastiti Web
  - potrebno je imati ASCII (ASC) verziju javnog ključa (ASCII armoured) – čisti tekst
  - to se stvara "**iznošenjem**" ključa iz prstena ključeva pomoću odgovarajućih naredbi
  - obično je kompliciranije i nespretnije – danas je takav način pretežno izašao iz upotrebe zbog **nepreglednosti** i **slabe ažurnosti** – usporedite sa PKS

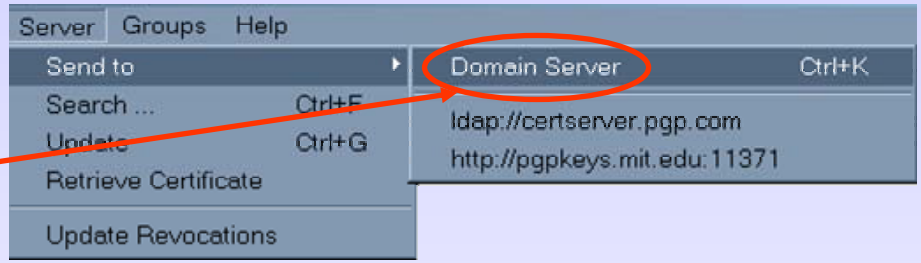
PGP - izlaganje javnog ključa (4)

- automatski iz GUI (PGPkeys) – šalje na PKS

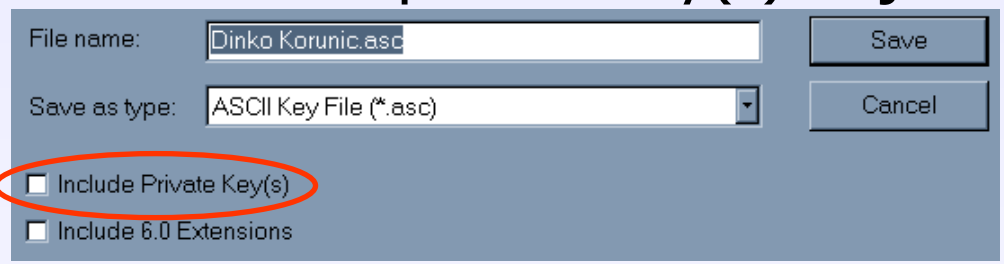
  označiti željeni ključ

  Server, Send to,

  Domain server



- ručno iz GUI (PGPkeys) – stvara ASC:
  - Keys, Export (ili Ctrl+K), odabrati ime datoteke
  - osigurati se kućica da "Include private key(s)" nije označena



PGP - izlaganje javnog ključa (5)

- ručno iz komandno-linijskog sučelja:

  `pgp -kx <userid> <prsten> <adresa>`

  – dotična naredba izvadi specificirani ključ iz specificiranog prstena i pošalje na dotičnu adresu

  – poslani ključ možete provjeriti pomoću:

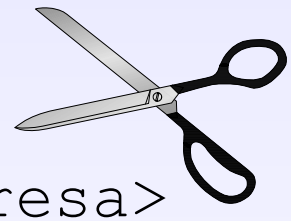
  `pgp -kv <userid> <adresa>`

  – dotična će naredba pokazati ključeve na udaljenom poslužitelju koji odgovaraju specificiranom ID-u

Sažetak (4)

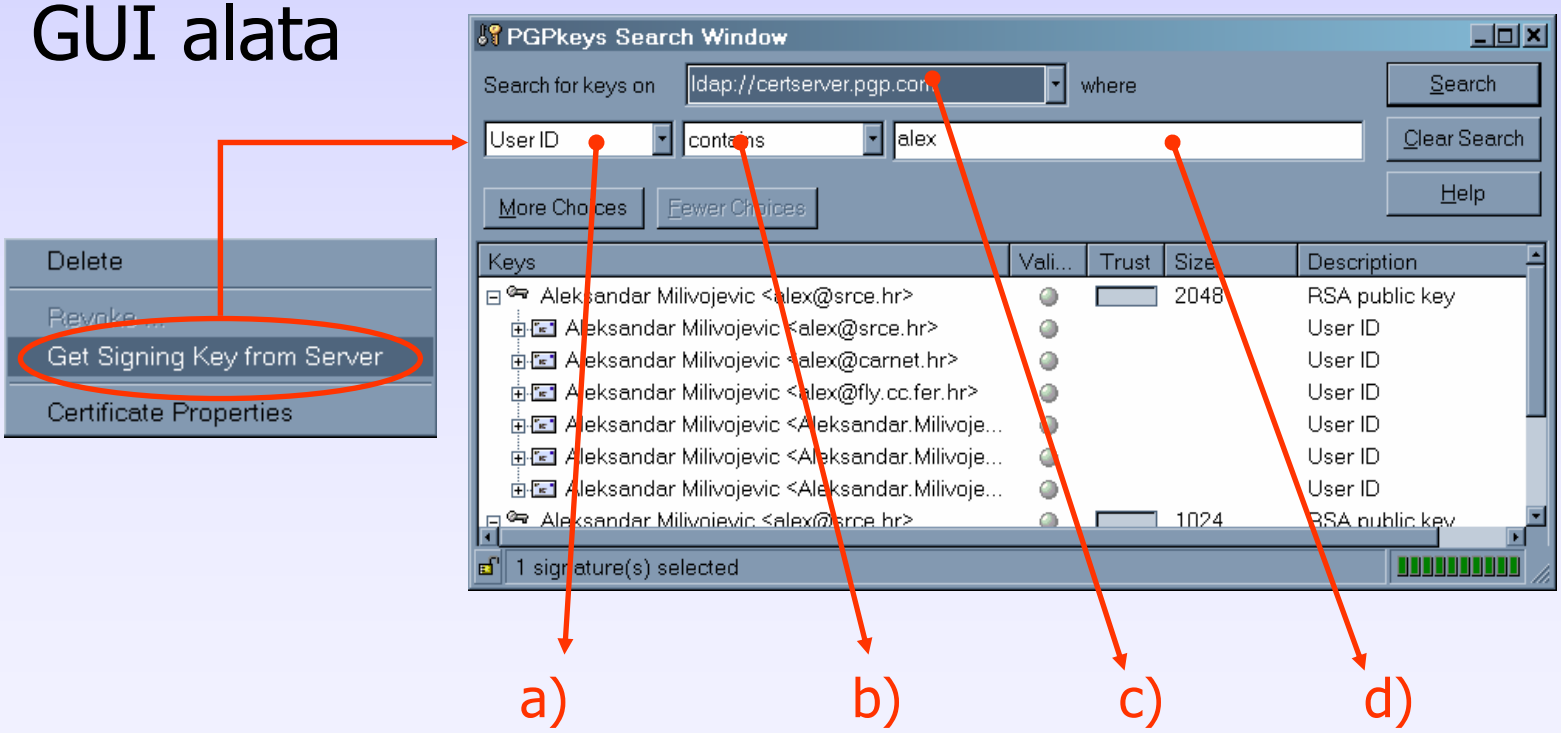
- izlaganje **javnog** ključa (i samo javnog!):
  - jedini način kako omogućiti drugima da **nama** šalju PGP osigurane poruke
  - moguće **preko PKS** (javni PGP poslužitelji) i **preko alternativnih metoda** (unutar e-maila, na Web stranicama, finger tekst, itd)
  - slanje na PKS: Server, Send to, Domain server
  - kako dobiti čisti tekst: Keys, Export
  - komandna linija:

```
pgp -kx <userid> <prsten> <adresa>
```



PGP – pronalaženje javnih ključeva (1)

- danas posve automatiziran postupak preko GUI alata



PGP – pronalaženje javnih ključeva (2)

- a) kategorije odabira:
  - User ID = korisničko ime, ime ili prezime korisnika ili e-mail adresa
  - Key ID = jedinstveni 32bitni broj ključa
  - Key Type = tip ključa, RSA ili DSA
  - Creation Date = vrijeme stvaranja ključa
  - Expiration Date = vrijeme prestanka rada ključa
  - Key Status = status ključa (valjan i radi, opozvan je ili isključen)
  - Key Size = veličina ključa u bitovima: 512, 768, 1024, 2048, 4096 bitova

PGP – pronalaženje javnih ključeva (3)

- b) logički prekidači:
  - is = je
  - is not = nije
  - is at least = je barem velik dotične veličine
  - is at most = najviše može dostići dotičnu veličinu
  - is on = je postavljen tog datuma
  - is on or before = postavljen je tog datuma ili prije
  - is on or after = postavljen je tog datuma ili poslije
  - contains = sadržava
  - does not contain = ne sadržava
  - is signed by = potpisan je od
  - is not signed by = nije potpisan od

PGP – pronalaženje javnih ključeva (4)

- c) odabir PKS:
  - ldap://certserver.pgp.com
  - http://pgpkeys.mit.edu:11371
  - Current Search Results = pretraživanje već dobivenih rezultata
  - Local Keyring = pretraživanje lokalnih prstenova

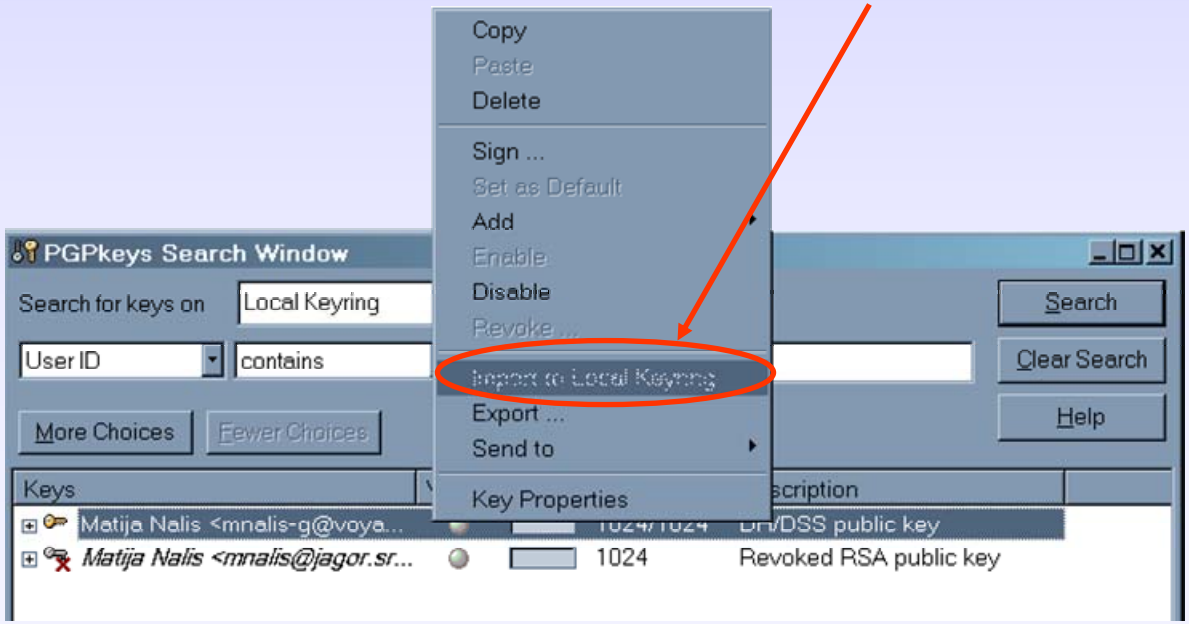
- d) polje koje sadržava odabire u skladu sa *a* i *b* ili u koje se može upisati proizvoljne podatke

Pauza

10 minuta

PGP – lokalno spremanje javnih ključeva (1)

- pronađene ključeve obično treba dodati u vlastiti prsten ključeva:
  - desni klik mišem na ključ, Import to local keyring



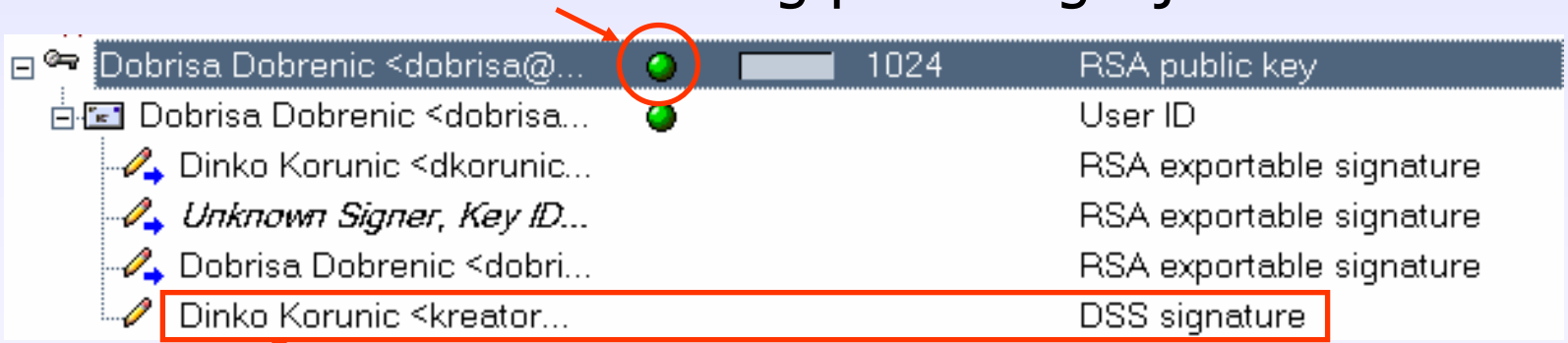
PGP – lokalno spremanje javnih ključeva (2)

- pronađeni ključevi **možda nisu** originalni vlasnikovi!
- zbog toga se provjerava otisak (fingerprint) "prstiju" samog unesenog ključa:
  - niz heksadecimalnih brojeva
  - uspoređuje se otisak lokalnog ključa sa onim od originalnog vlasnika (telefon, Web, itd.)
  - kada ste sigurni da je to **ispravan** ključ – trebate ga **potpisati** čime ga označavate ispravnim i tek sada spremnim za korištenje (valid)
  - moguće je i preko osoba koje potpisuju takav ključ a označili ste ih osobama od povjerenja (ultimate-trust introducer)

PGP – lokalno spremanje javnih ključeva (3)

- upute:
  - označiti ključ u PGPkeys, Keys, Properties

  - usporediti dobiveni otisak sa vlasnikovim otiskom
  - ako se podudaraju: Keys, Sign (ili Ctrl+S), OK i ukucati lozinku vlastitog privatnog ključa



PGP – lokalno spremanje javnih ključeva (4)

- komandno-linijsko sučelje:
  - ponešto kompliciranije i ne tako ugodno - obično se koriste različite skripte koje pojednostavljuju pretraživanje u ručno dodavanje: pksxywrap i sl.

- pregled postojećih ključeva na PKS koji zadovoljavaju dotični kriterij:

```
pgp -kv <userid> <URL>
```

- ekstrakcija ključa u datoteku

```
pgp -kx <userid> <datoteka> <URL>
```

PGP – lokalno spremanje javnih ključeva (5)

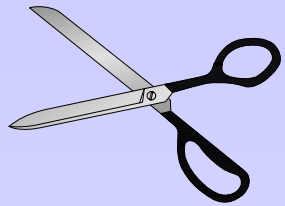
- dodavanje ključa iz datoteke u vlastiti prsten

  `pgp -ka <datoteka>`
- brisanje ključa iz prstena

  `pgp -kr <userid>`
- provjera otiska ključa

  `pgp -kvc <userid>`
- napomene:
  - kao adresa se koriste već spomenuti PKS
  - datoteku je kasnije potrebno obrisati

Sažetak (4)



- ključeve **pretražujemo** prema njihovim karakteristikama:
  - key ID, user ID, tip ključa, vrijeme stvaranja ili prestanka ispravnosti, status ključa, itd.
- unesene ključeve treba **provjeriti**:
  - otisak ključa se provjerava sa vlasnikom preko nekog drugog načina osim PKS: potpis u e-mailu, Web, telefonom, GSM-om, itd.
  - ako otisci pašu ključ je potrebno **potpisati** da postane **punovrijedan - stvaramo certifikat**

PGP – pronalaženje i spremanje, praktičan rad

- Zadatak – **pronalaženje** i **dodavanje** ključeva
  - koristiti adresu **http://ds.carnet.hr:11371** za rad
  - pronaći i dodati ključeve koji pripadaju osobama: *Dobriša Dobrenić, Aleksandar Milivojević*
  - pronaći i dodati ključ *0xEA160D0B*
  - pronaći i dodati ključeve svih osoba čije prezime sadržava slovo K, imaju opozvani ključ i iz Hrvatske su (koristiti metodu pretraživanja zadnjih rezultata!)
  - potpisati unesene ključeve ako im otisci odgovaraju onima na ploči (opcionalno, za one najbrže)
- Predviđeno vrijeme: **15** minuta

PGP i MS Outlook Express

Osnove rada

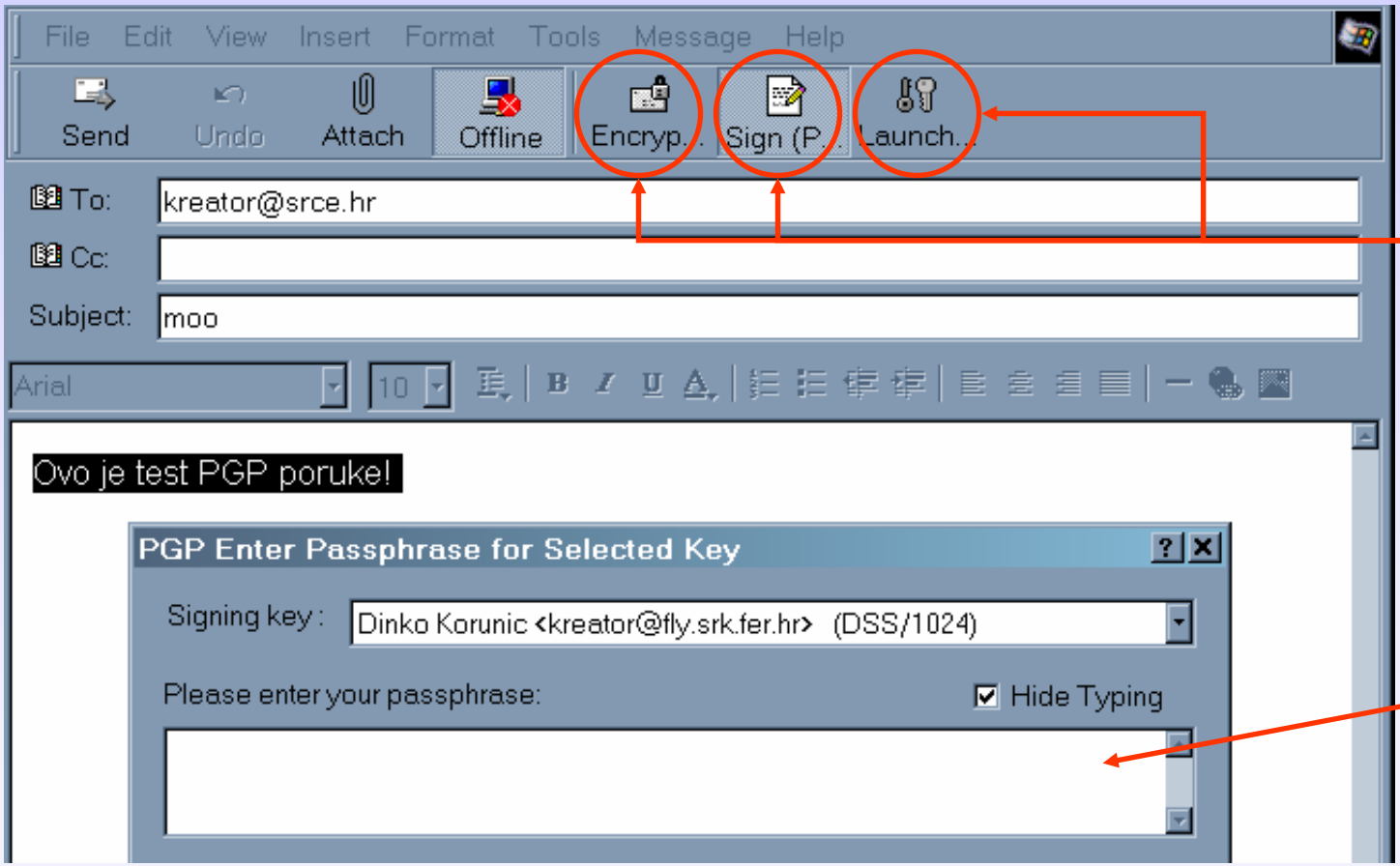
šifriranje/dešifriranje poruke

Potpisivanje/provjera potpisa

PGP i Outlook – osnove rada (1)

- MS Outlook Express
  - jedan od poznatijih e-mail klijenata (MUA odnosno Mail User Agent)
  - predstavlja pojednostavljenu inačicu MS Outlook programa koji dolaze u MS Office paketima
  - instalira se zajedno sa operativnim sistemom i uvijek je dostupan
  - alternative: Eudora Lite / Eudora Pro
  - potrebno je **uvijek** imati pokrenut PGPtray – dotični stvara **3** dodatna gumba u Outlooku

PGP i Outlook – osnove rada (2)



dodatni PGP izbornici

upisivanje lozinke za PGP ključ

PGP i Outlook – osnove rada (3)

- sve mogućnosti koje se nude preko grafičkog sučelja je moguće ručno (u komandnoj liniji) izvesti:
- dešifriranje poruke ili provjeravanje potpisa:

```
pgp <datoteka>
```

- šifriranje poruke:

```
pgp –e <datoteka> <userid>
```

- potpisivanje poruke s tajnim ključem:

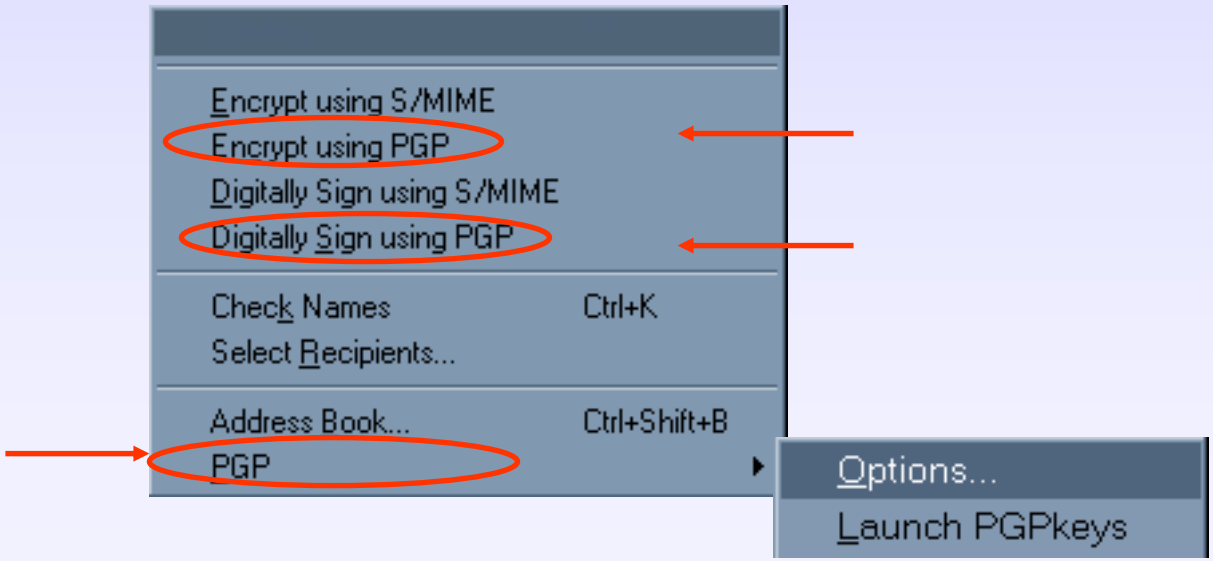
```
pgp –s <datoteka>
```

PGP i Outlook – osnove rada (4)

- korištenje je trivijalno jednostavno:
  - prilikom slanja poruke ili primanja poruke selektiramo i pritisnemo željenu akciju (*šifriraj*, *dešifriraj*, *potpiši*) te se ona izvršava
  - svako baratanje ključevima i datotekama je na ovaj način izbjegnuto
  - od korisnika se jedino traži *unos lozinke* za vlastiti privatni ključ
  - iz Outlooka je moguće direktno pozvati PGPkeys za baratanje ključevima (npr. dodavanje ključa koji nam upravo nedostaje)

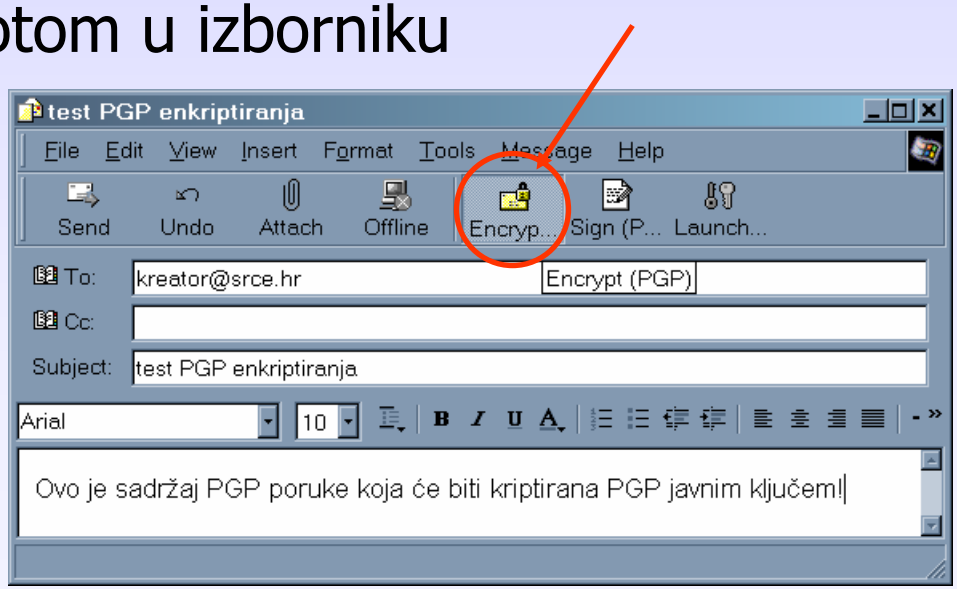
PGP i Outlook – osnove rada (5)

- sve navedene akcije se osim u izborniku sa gumbima nalaze (najčešće – ovisno o verziji Outlook Expressa) i u Tools izborniku:



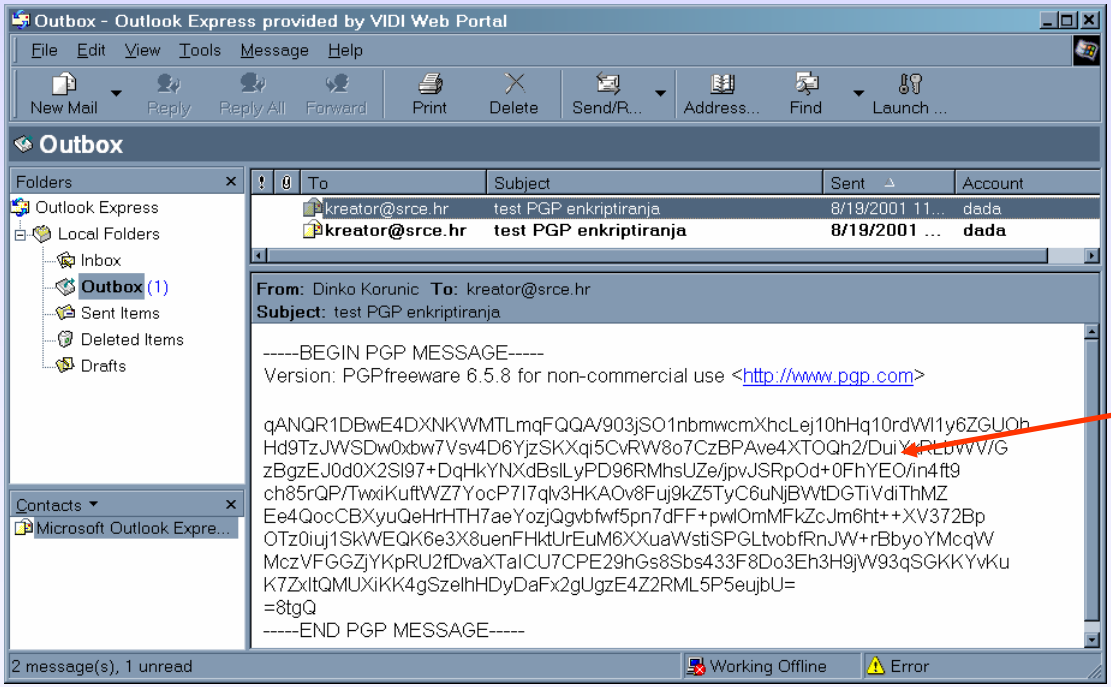
PGP i Outlook – šifriranje poruke (1)

- MS Outlook:
  - za stvaranje nove poruke: File, New, Mail message
  - napišemo tekst i kliknemo na gumb “Encrypt” sa lokotom u izborniku



PGP i Outlook – šifriranje poruke (2)

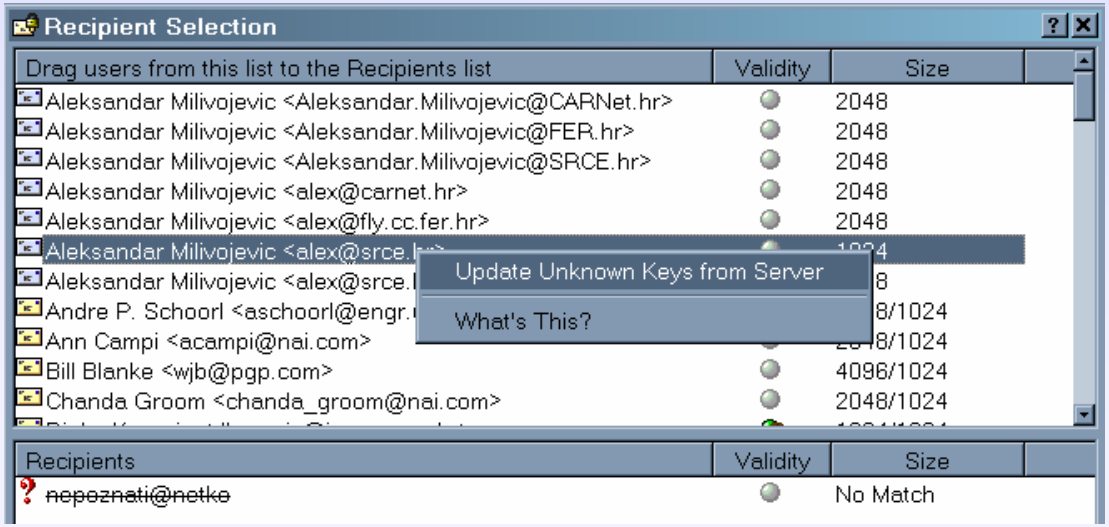
- nakon toga ne unosimo lozinku – poruka se šifrira **javnim ključem** primatelja!



ovo je naša još neposlana **šifrirana** poruka

PGP i Outlook – šifriranje poruke (3)

- PGP će iz To: i Cc: polja (standardno zaglavlje e-mail poruke) pokupiti adrese te potražiti u vlastitoj bazi ključeva (prstenu) uz mogućnost dodavanja novih

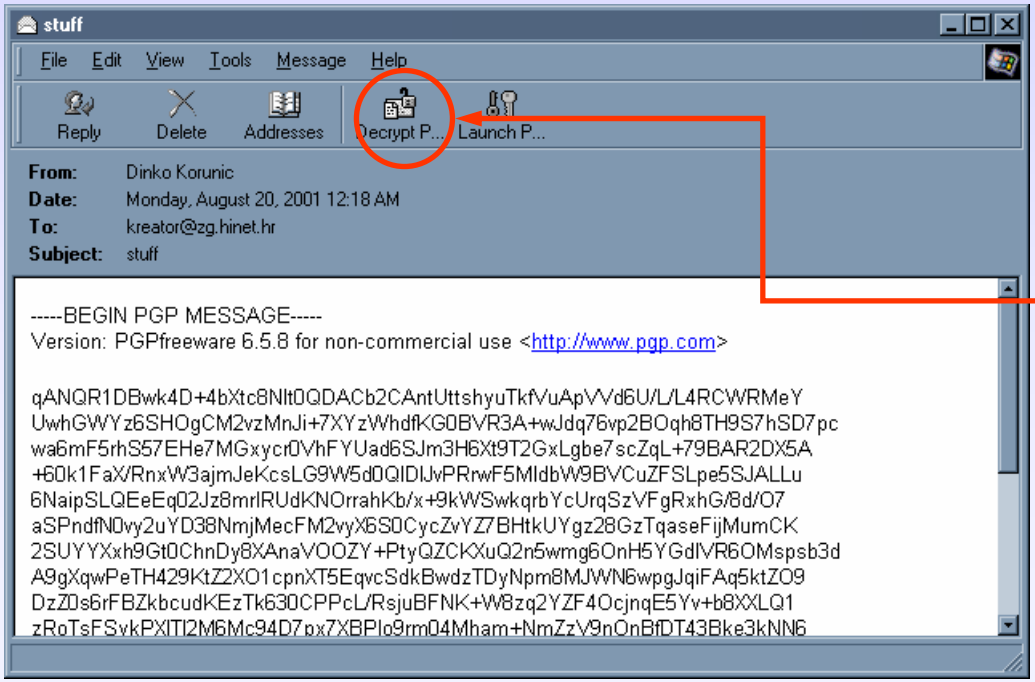


Pauza

10 minuta

PGP i Outlook – dešifriranje poruke (1)

- primljena šifrirana poruka je nerazumljiva u originalnom obliku i vama kao i ostalima



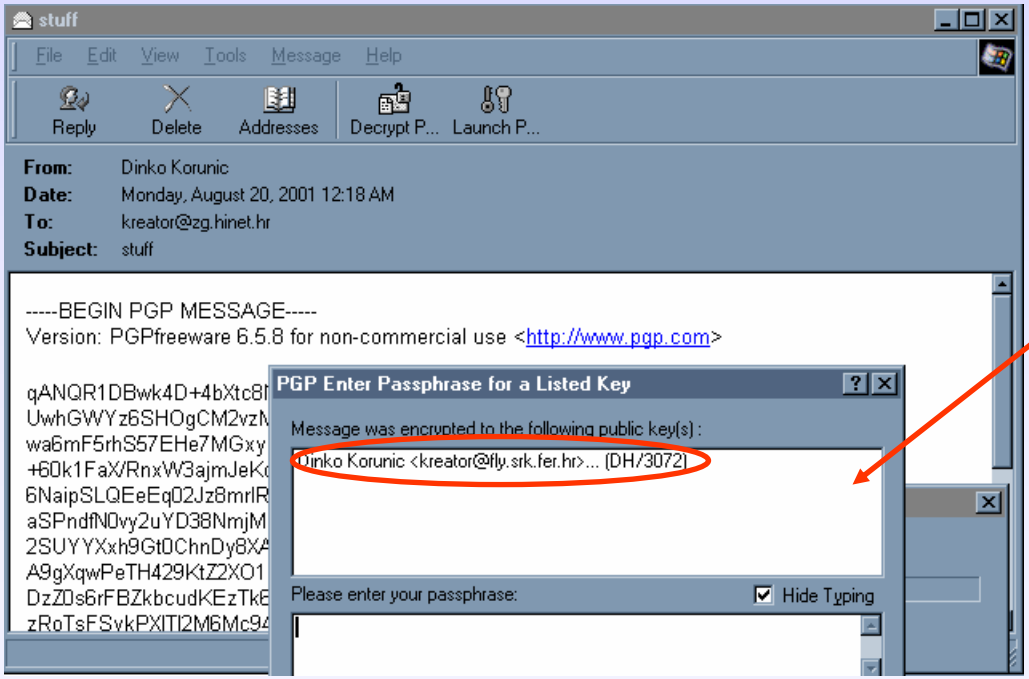
klikom na "Decrypt PGP" poruka se automatski dešifrira uz unos tajne lozinke

napomena:

- isto je moguće postići i preko Tools izbornika

PGP i Outlook – dešifriranje poruke (2)

- prozor za upis lozinke se **automatski** pojavljuje kada je potrebno

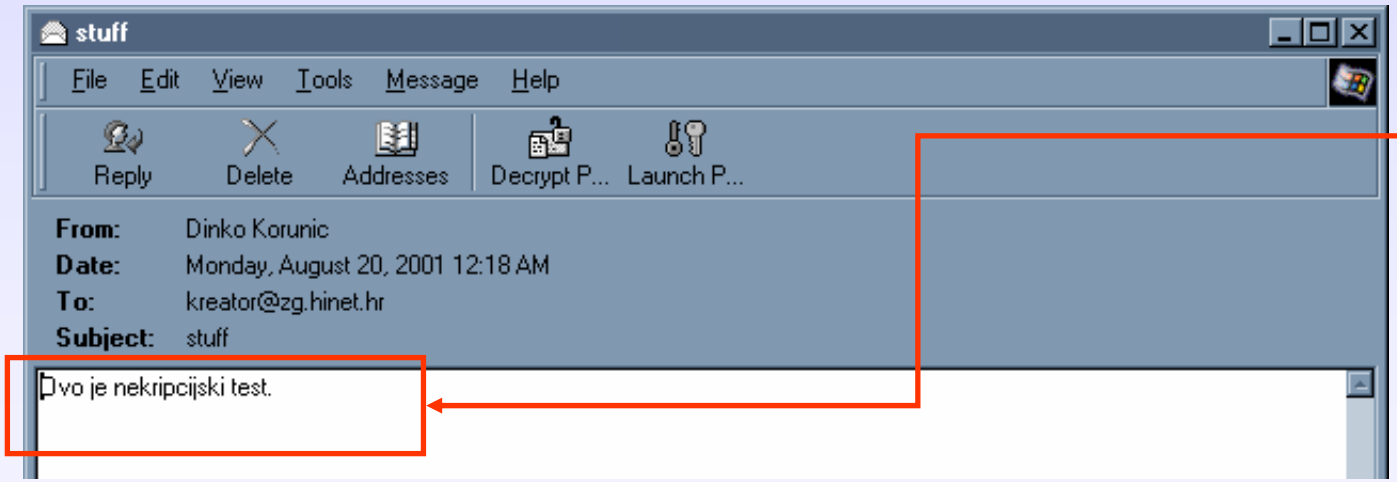


napomene:

- lozinka se ne vidi tijekom upisivanja
- PGPtray je moguće konfigurirati tako da izvjesno vrijeme pamti lozinke
- u prozorčiću se vidi koji ključ se upravo koristi za dešifriranje

PGP i Outlook – dešifriranje poruke (3)

- iz finalne poruke nestaje šifrirani sadržaj i sva PGP zaglavlja te možete pročitati **čisti sadržaj** kakav bi bio bez PGP-a:



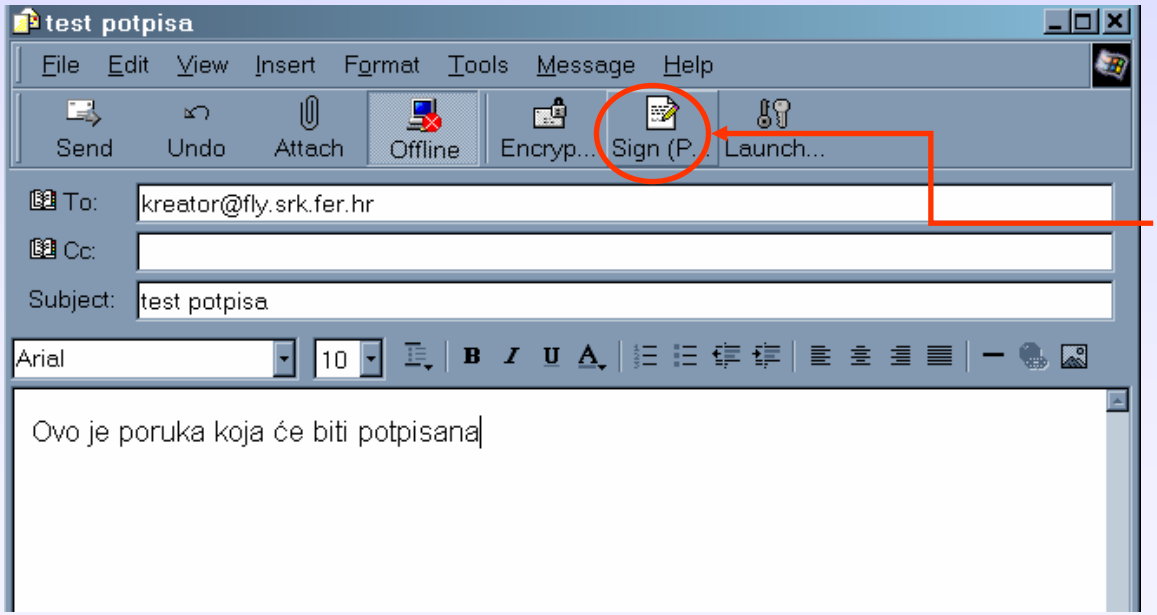
dobiveni originalni sadržaj

PGP i Outlook – šifriranje i dešifriranje, praktični rad

- Zadatak – **šifrirati** vlastitu poruku:
  - napisati e-mail *proizvoljnog sadržaja*
  - poslati na *vlastitu adresu* koristeći već gotov *vlastiti ključ* iz prethodnih vježbi
- Zadatak – **dešifrirati** vlastitu poruku:
  - pokupiti *šifrirani* e-mail sa vlastite adrese
  - uz već opisanu metodu *dešifrirati* e-mail i provjeriti sadržaj
- Ukupno predviđeno vrijeme: **10** minuta

PGP i Outlook – potpisivanje poruke (1)

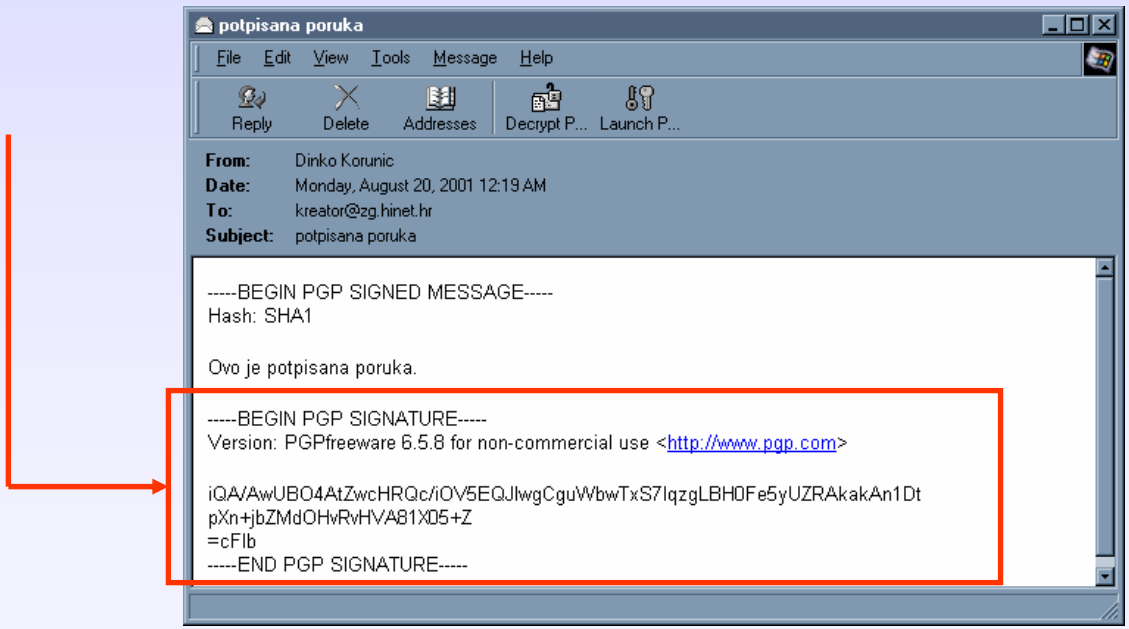
- potpisivanje se obavlja na analogno jednostavan način:



klikom na "Sign PGP" se vaša poruka potpisuje vašim ključem koji garantira autentičnost poruke

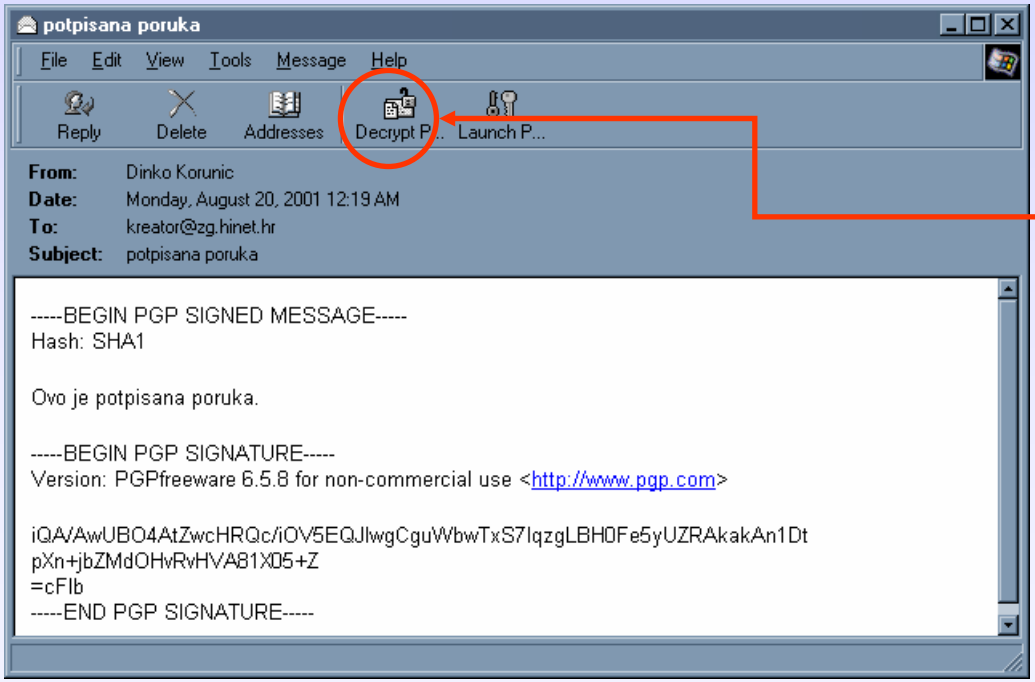
PGP i Outlook – potpisivanje poruke (2)

- potpisana poruka dobiva ekstra sadržaj na dnu u vidu PGP **sufiksa** (naravno, ovdje je potrebno unijeti **vlastitu lozinku**!):



PGP i Outlook – provjera potpisa (1)

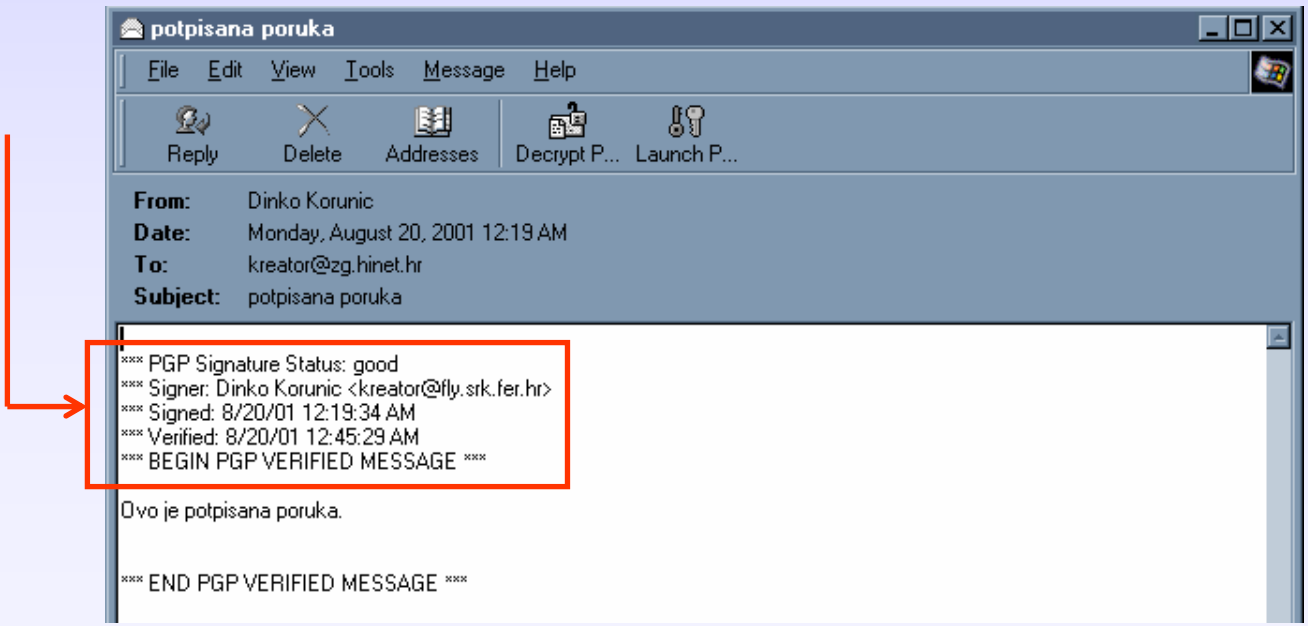
- primljenu poruku sa PGP potpisom moguće je verificirati istim načinom kao kod dekripcije:



napomena:
- u ovom slučaju dešifriranje (odnosno gumb za dešifriranje) radi provjeru potpisa!

PGP i Outlook – provjera potpisa (2)

- te potpisana poruka dobiva **zaglavlja** u kojima piše rezultat odnosno **uspješnost** provjere potpisa

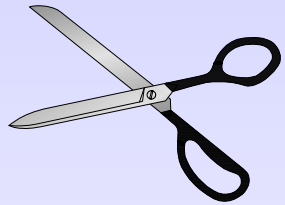


PGP i Outlook – potpisivanje i provjera, praktični rad

- Zadatak – **potpisati** vlastitu poruku:
  - napisati e-mail *proizvoljnog* sadržaja
  - potpisati ga i unijeti *pravilnu* vlastitu *lozinku* te poslati mail na *vlastitu adresu*
- Zadatak – **provjeriti potpis** vlastite poruke:
  - pokupiti e-mail sa *vlastite adrese*
  - *provjeriti potpis* koristeći već opisani postupak
  - *pročitati* rezultat provjere potpisa
- Ukupno predviđeno vrijeme: **10** minuta

Sažetak (5)

- poruke koje se **šalju**:
  - šifriranje = Encrypt (PGP)
  - potpisivanje = Sign (PGP)
- poruke koje su **pristigle**:
  - dešifriranje = Decrypt (PGP)
  - provjera potpisa = Decrypt (PGP)
- **lozinku** je potrebno unijeti kod:
  - dekripcije
  - potpisivanja



Sažetak ukupnog predavanja

- PGP je alat iznimne **jednostavnosti** (za "obične" korisnike) koji nudi **kompletnu** zaštitu podataka (ne samo e-mailova) **jakom kriptografijom**
- PGP je "**slobodan**" softver i moguće ga je koristiti **bez restrikcija** u većini zemalja što ga čini izuzetno **popularnim**
- PGP poslužitelji ključeva omogućavaju **laku razmjenu ključeva** i **globalno korištenje**

Literatura (1)

- dostupno u standardnoj PGP instalaciji:
  - Intro to Crypto.pdf
  - PGP Command Line Guide.pdf
  - PGP User's Guide.pdf
- glavne adrese projekta:
  - http://www.pgpi.com
  - http://www.pgp.com
- dodatna dokumentacija:
  - PGP attacks
  - PGP Intro
  - Secret key protection
  - PassPhrase FAQ

Literatura (2)

- dodatna dokumentacija na Webu:
  - http://www.pgpi.org/doc
  - http://www.rubin.ch/pgp
  - http://www.pgp.com/phil
  - itd.