

# PGP

(Pretty Good Privacy)

# Trenutno stanje: e-mail

- Elektroska pošta nije baš siguran način komunikacije.
- Poruka na svom putu do primaoca prolazi kroz barem desetak mrežnih čvorova – na svakom od njih, poruka je u opasnosti da je neko pročita ili promeni bez znanja pošiljaoca.
- Iz tog razloga u porukama e-pošte nikako ne bismo trebali slati poverljive informacije poput brojeva bankovnih računa i kreditnih kartica ili podatke iz korisničkih profila.
- PGP je svojevrsna sigurnosna nadogradnja sistema elektronske pošte, koji korisnicima omogućuje da menaju datoteke ili poruke vodeći računa o poverljivosti, autentičnosti i praktičnosti.
- Poverljivost znači da samo oni kojima je poruka namenjena mogu poruku i pročitati, dok autentičnost znači da poruke zaista dolaze od onoga ko je naveden kao pošiljaoc. Praktičnost, koja proizlazi iz koncepta uređenog para ključeva, tzv. javnog i privatnog (tajnog) ključa, znači da su poverljivost i autentičnost osigurani bez dodatnog mehanizma izmene ključa za šifriranje.

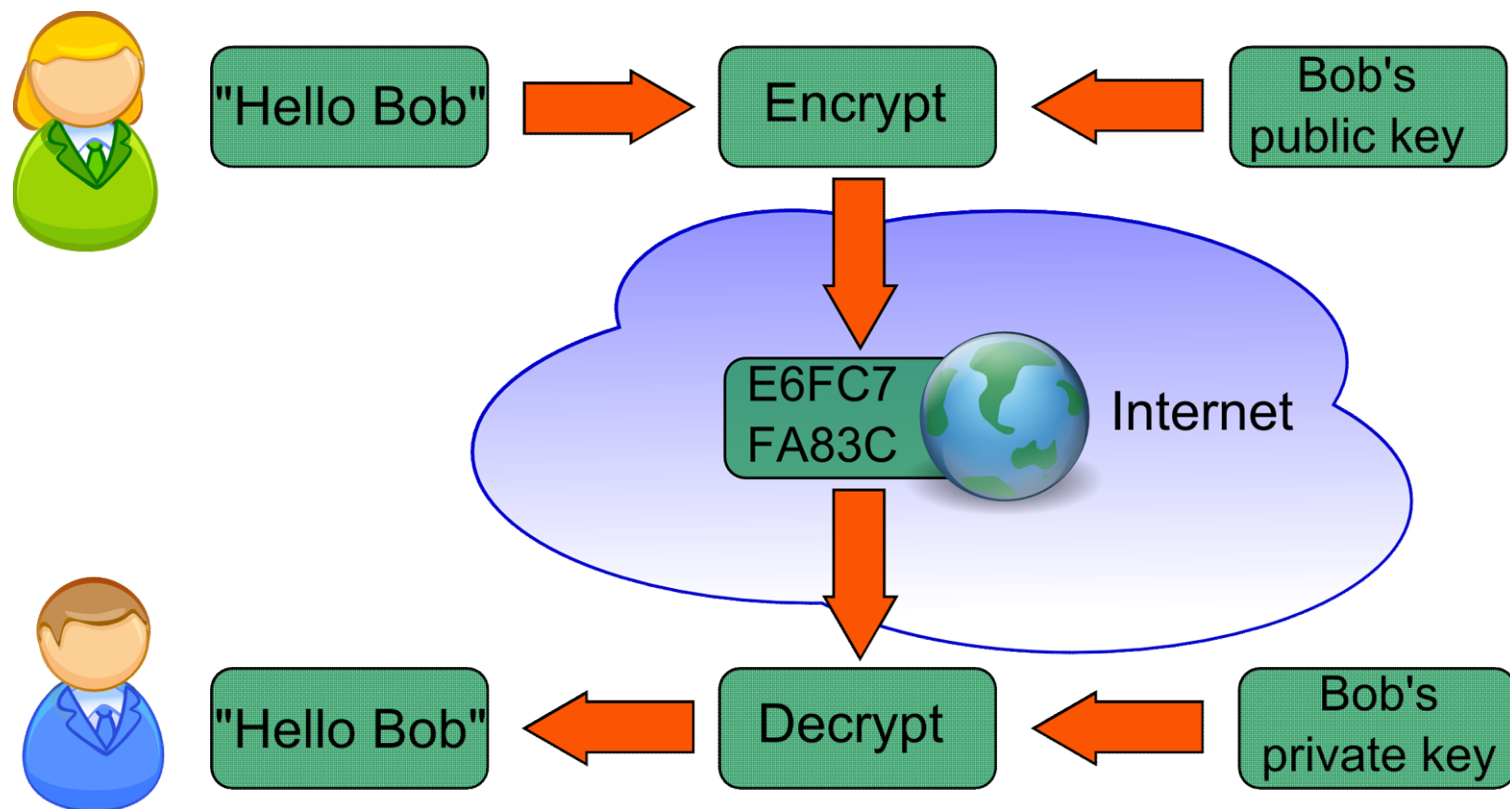
# PGP, enkripcija

- **Enkripcija** (engl. *encryption*) ili šifrovanje je proces u kriptografiji kojim se vrši izmena podataka tako da se podaci učine nečitljivim za osobe kojima nisu namenjeni i koje ne poseduju određenu šifru (ključ). Na taj način se dobija šifrovana informacija. Da bi ovi podaci postali ponovo razumljivi i upotrebljivi, potrebno je da se dešifruju, odnosno dekriptuju.
- **Pretty Good Privacy** (PGP) je program za enkripciju i dekripciju podataka kao i autentikaciju u elektronskim komunikacijama. Stvorio ga je Phill Zimmermann 1991. godine. Od tada je program promenio više vlasnika i danas više nije besplatan, ali je u međuvremenu licencirana besplatna verzija programa pod nazivom GPG (**GNU Privacy Guard**). Softver koji ćemo koristiti u ovu svrhu naziva se **GPG4Win** (gpg (PGP) za windows). On omogućava enkripciju i dekripciju podataka kao i digitalno potpisivanje, koje služi da potvrdi identitet pošiljaoca i autentičnost podataka.

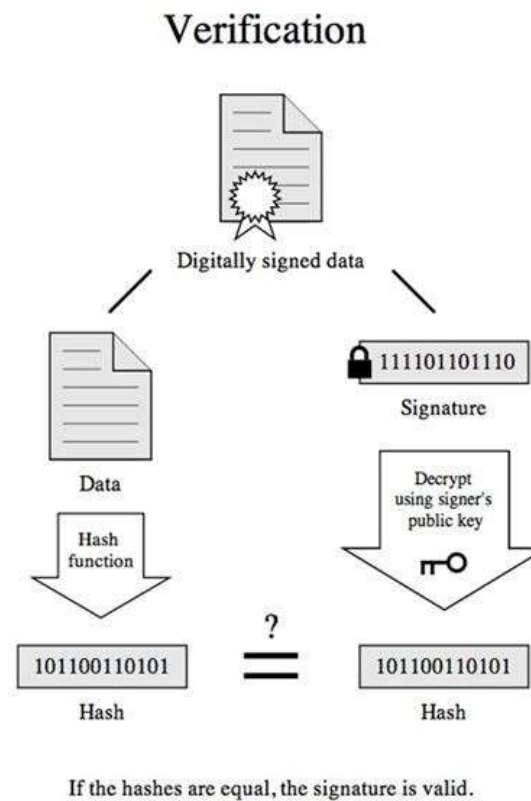
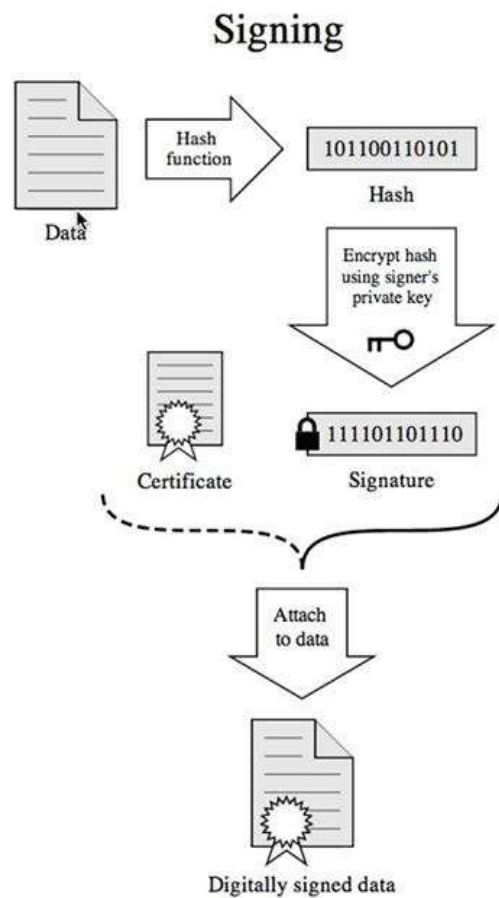
# Sistem javnih ključeva

- Funkcionisanje ovakvog sistema zaštite podataka zasniva se na **PKI** sistemu (*Public Key Infrastructure*) - sistemu javnih ključeva.
- Sistem privatnih i javnih ključeva funkcioniše tako što prvo u vašem programu na računaru kreirate par ključeva (sertifikat). Ključ je skup od 256 (ili više) karaktera (slova, brojevi, specijalni karakteri) koji služe da se njima neki podatak enkriptuje, odnosno dekriptuje. Dva ključa dobijena u programu su matematički povezana tako da ono što jednim ključem enkriptujete možete samo njegovim parom da dekriptujete, i obratno. Javni ključ ste slobodni da date svima koji žele nešto da enkriptuju za vas. Pošto javni ključ služi za enkripciju njime može svako samo da enkriptuje, ali samo vi možete taj podatak da dekriptujete svojim privatnim ključem. Zato privatni ključ stoji u računaru zaštićen šifrom koju ste vi osmislili, pošto bi bilo teško pamtići privatni ključ od 256 i više karaktera.

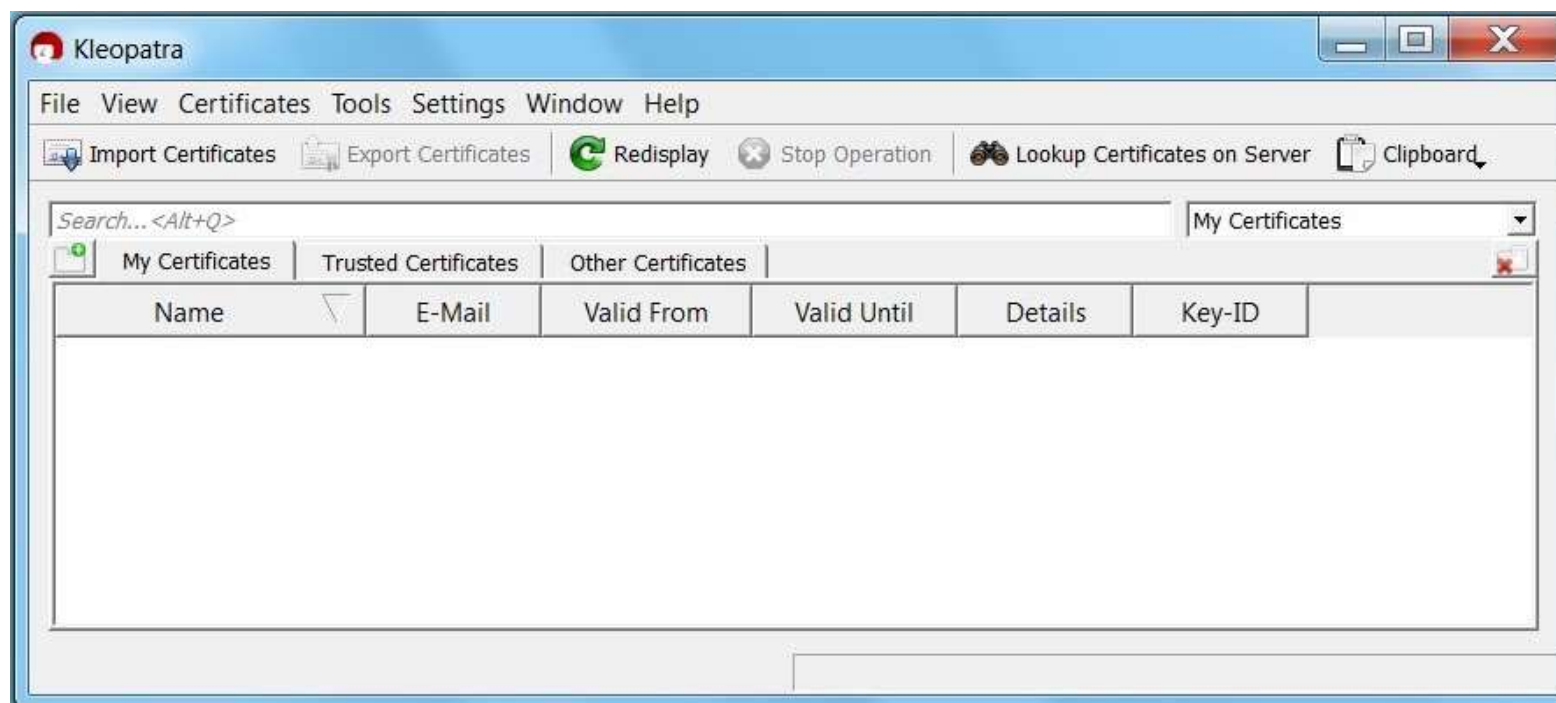
# Alice, Bob, enkripcija, dekripcija



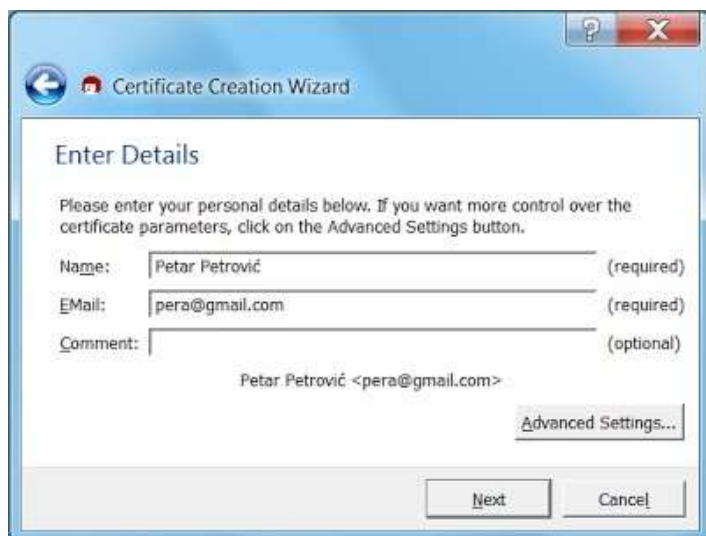
# Potpisivanje



# Kreiranje novog sertifikata



# Čarobnjak za kreiranje ključa



**Certificate Creation Wizard**

**Enter Details**

Please enter your personal details below. If you want more control over the certificate parameters, click on the *Advanced Settings* button.

Name:  (required)

E-Mail:  (required)

Comment:  (optional)

Petar Petrović <pera@gmail.com>

[Advanced Settings...](#)

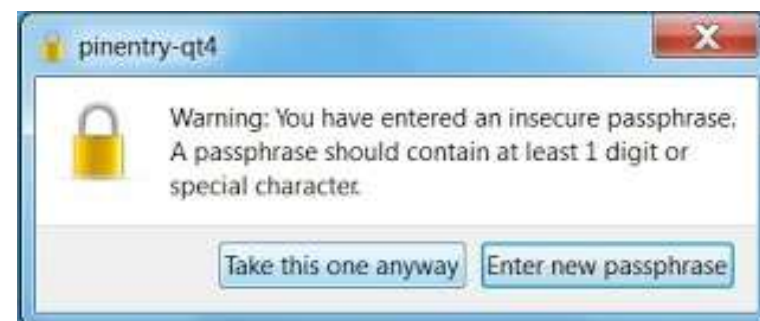


**pinentry**

Enter passphrase

Passphrase:

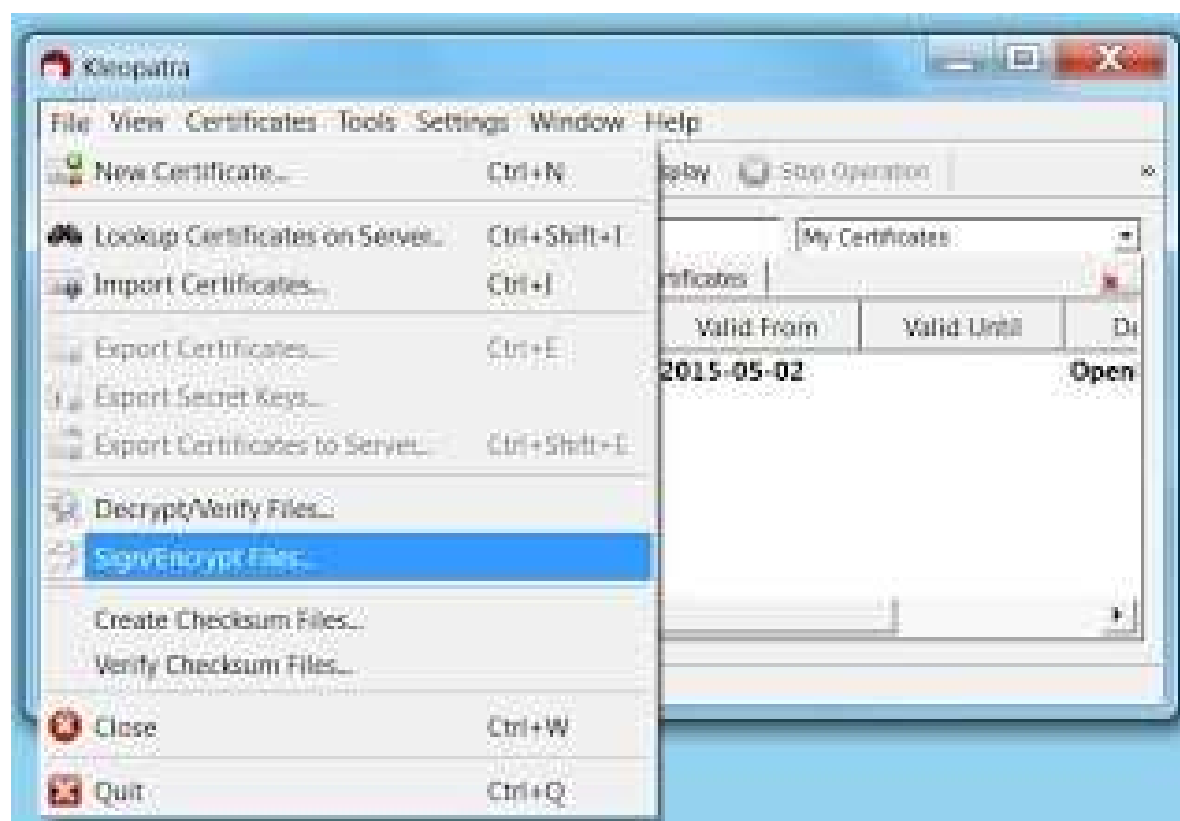
Quality:  50%



**pinentry-qt4**

 Warning: You have entered an insecure passphrase, A passphrase should contain at least 1 digit or special character.

# Digitalno potpisivanje



# Zadatak za vežbu

- Preuzmite dokument koji treba da enkriptujete javnim ključem sa veb sajta i potpišete setifikatom koji ćete za tu priliku napraviti. Na mrežni disk šaljete vaš sertifikat i potpisan i enkriptovan dokument.
- Za uspešno potpisan i enkriptovan dokument koji na mrežni disk stigne za manje od 4 minuta dobija se 100% poena. Za svaki minut više ocena je manja za 10%.