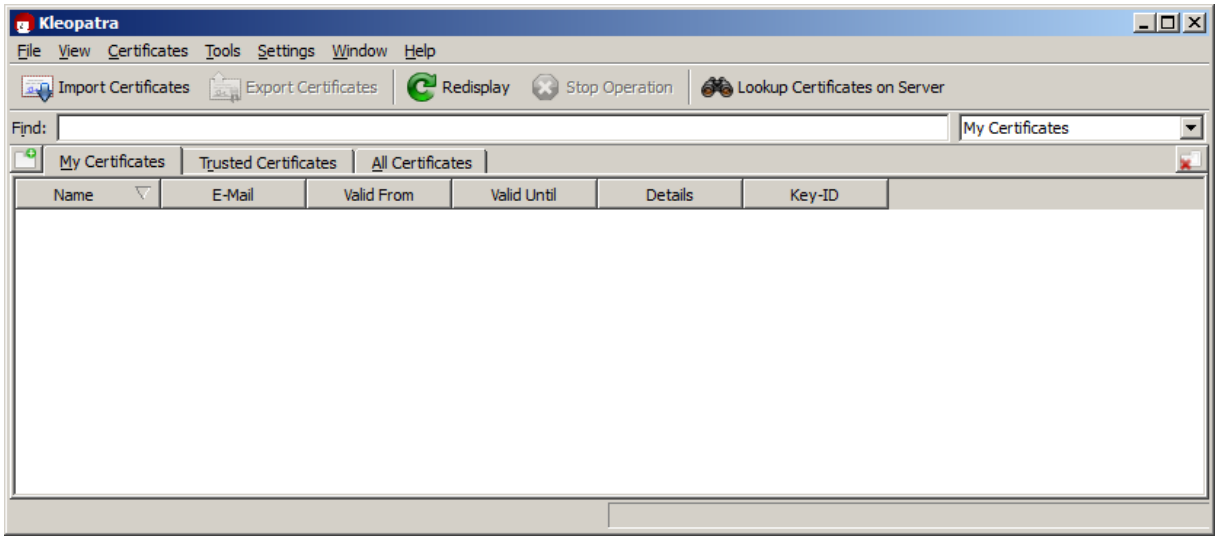
Uporaba asimetričnih šifrirnih postopkov

Izdelava para ključev

Z uporabo aplikacije **Gpg4win** izdelajte par ključev. Uporabite **OpenPGP** metodo.

Sledite 7. poglavju navodil.



Slika 1: Uporabniški vmesnik programa Kleopatra

Shranjevanje ključev

- izvozite **privatni ključ** in ga shranite na varnem mestu (npr. na vašem USB ključku).
- izvozite **javni ključ** in ga poimenujte s svojim imenom in priimkom.

Objavljanje javnega ključa

Navadno je potrebno javni ključ objaviti na javnih strežnikih. Ker bomo izdelali javni ključ za testne namene, z njim ne bomo »onesnaževali« javnih strežnikov. Uporabljali bomo javno mapo na **Google Drive**, ki se nahaja na spodnji povezavi:

https://drive.google.com/folderview?id=0B2hs2UIvRsekSV93NmltUXpLNm8&usp=sharing

prenesite svoj javni ključ na mesto, ki ga določa gornja povezava, kjer bo dostopen ostalim.

Šifriranje in podpisovanje

- Izberite si 3 sošolce in jim pripravite sporočilo.
- Sporočilo shranite kot tekstovno datoteko, ki jo poimenujete tako, da bo iz imena datoteke razvidno, kdo je pošiljatelj in kdo prejemnik (npr. *od_MajeNovak_za_JanezaNovaka*)
- Na svoj računalnik prenesite javne ključe oseb, katerim je sporočilo namenjeno.
- Certifikate uvozite v program in jih certificirajte.
- Tekstovno datoteko šifrirajte **z javnim ključem osebe, kateri je sporočilo namenjeno**.
- Tekstovno datoteko podpišite **z vašim privatnim ključem**.
- Tekstovno datoteko prenesite na na **Google Drive**.

Dešifriranje in preverjanje identitete

- Na **Google Drive** preverite, če vas čakajo sporočila.
- Prenesite vse datoteke, ki so vam namenjene.
- Na svoj računalnik prenesite javne ključe oseb, od katerih ste prejeli sporočilo.
- Certifikate uvozite v program in jih certificirajte.
- Vse datoteke **dešifrirajte s svojim privatnim ključem** in **preverite, kdo je njihov pošiljatelj**. Pošiljateljev certifikat mora biti cerificiran.
- S spletnega mesta prenesite tudi nekaj datotek, ki niso namenjene vam, in jih prav tako poskušajte dešifrirati.

Počistite za seboj

Iz programa Kleopatra odstranite vse izdelane in vse uvožene ključe.

Z računalnika odstranite vse datoteke, ki ste jih izdelali med vajo.