Dokumentacija

Projekat koristi:

- Asimetricno kriptovanje: RSA sa kljucem duzine 1024,2048 I 4096 bitova
- Simetricno priktovanje: 3DES sa EDE kongifuracijom I AES sa kljucem duzine 128 bitova
- Hash funkcije: SHA-1

Klase u paketu etf.openpgp.su182095dvv180421d:

- Config - U ovoj klasi se nalaze konstante vezane za projekat
- MainFrame - Glavni prozor aplikacije, ovde se nalazi main metoda koja pokrece instanciranje MainFrame klase I pokrece aplikaciju

---

Klase u paketu etf.openpgp.su182095dvv180421d.views:

- CreatePGPMessage
- DeletePrivateKeyDialog
- KeyGenerate
- KeysStoreLoad
- PrivateKeyRingView
- PublicKeyRingView
- ReadMessageView

Ovo su sve komponente koje se prikazuju na GUI-ju. Vecina njih ima samo konstruktor, dok kod odredjenih klasa je odradjena neka vrsta refaktorizacije, pa postoje neke metode koje grupisu neke bliske delove.

Klase u paketu etf.openpgp.su182095dvv180421d.model:

- AsymtetricKeyGenerator - postoji samo jedna metoda generate, koja generise par privatni I javni kljuc za RSA algoritam
- Callback - interfejs koji ima samo jedno metodu callback, koristi se u GUI klasama gde hoce da se izbaci logika vezano za samu implementaciju algoritama iz GUI klase I prebaci na drugo mesto
- KeyRing – osnova klasa iz koje su izvedeni PrivateKeyRing I PublicKeyRing I predstavlja projektni uzorak posmatrac, da kada se doda ili obrise novi kljuc iz date klase, da se data promena odmah prosledi do klasa za prikaz komponenata
- LoadStoreKeys – nalaze se 4 metode, po 2 koje snimaju kljuceve iz aplikacije u fajl na fajl sistemu (za privatni I javni kljuc) I po 2 koje ucitavaju kljuceve u aplikaciju
- Observer – drugi deo projektno uzorka posmatrac, interfejs koji implementiraju GUI klase da se obaveste da je doslo do promene podataka
- PGPMessageFactory – ima samo jednu metodu, koja sluzi za pravljenje PGP poruke

- PrivateKeyRing – klasa koja sadrzi private kljuceve. Ima metode za pronalazak, dodavanje I brisanje kljuceva. Takodje, nalaze se 2 staticke metode, koje obezbedjuju ucitavanje svih privatnih kljuceva sa diska pri pokretanju aplikacije, kao I snimanje svih kljuceva kad se aplikacija zavrsava
- PublicKeyRing - klasa koja sadrzi javne kljuceve. Ima metode za pronalazak, dodavanje I brisanje kljuceva. Takodje, nalaze se 2 staticke metode, koje obezbedjuju ucitavanje svih javnih kljuceva sa diska pri pokretanju aplikacije, kao I snimanje svih kljuceva kad se aplikacija zavrsava
- PublicKeyTrust – 3 metode:
    - getOwnerTrust – za prosledjeni javni kljuc vraca da li se veruje datom korisniku
    - getSignatureTrust – za prosledjeni javni kljuc vraca da li se veruje kljucu
    - getSignatureToString – vraca string od niza potpisa
- ReadPGPMessage – postoje 2 metode u klasi:
    - getPGPSecretKeyFromFile – proverava li da poruka koja se ucitava u aplikaciji je dekriptovana I ako jeste, vraca kljuc kojim je dekriptovana
    - decryptAndVerify – ucitava poruku iz fajla, I po potrebi dekriptuje, dekompresuje, prebaci iz radix64, kao I skine I proveri potpis I ako je sve u redu, snimi poruku u tekstu na fajlu sistemu I vrati poruku o uspesnosti
- RSAUtil – postoje 2 metode u klasi:
    - encrypt - enkriptuje prosledjeni tekst sa kljucem
    - decrypt - dekriptuje prosledjeni tekst sa kljucem
- Utils – mnogo usluznih metoda, koje omogucavaju rad sa privatnim I javnim kljucevima