Opgave i objektorienteret programmering

PGP

Vi kunne tænke os at implementere en simpel version af krypteringsprogrammet PGP (Pretty Good Privacy)

Hovedstrukturen i PGP er at hver bruger har en offentlig og en privat nøgle. Den private nøgle bruges til at åbne filer der er krypteret med den offentlige. Man bruger en anden brugers offentlige nøgle til at kryptere filer der skal kunne åbnes af vedkommende.

Hovedfokus for opgaven vil imidlertid ikke være på brugerdelen af programmet, men hovedsagligt dreje sig om at designe med genbrug for øje, ved at overholde grundlæggende designprincipper som løs kobling og abstraktion. Dette vil hovedsagligt ske ved at arbejde med designpatterns, og ved at designe til interfaces snarere end implementeringer.

Herudover vil implementeringen af de valgte krypteringsalgoritmer naturligvis også være en del af opgavens fokus. Som udgangspunkt ville vi gerne lave et program der kunne gøre brug af forskellige algoritmer afhængig af brugerens krav til sikkerhedsniveau og hastighed.

Systemet skal have følgende funktioner:

En bruger skal kunne
- tilmeldes systemet
- modtage en nøgle
- have adgang til offentlige nøgler

Systemet skal kunne
- generere nøgler og password
- kryptere filer efter brugerspecificerede krav (Sikre dataintegritet)
- have en signaturfunktion (Sikre dataautencitet)

Funktionerne er ikke opstillet i prioriteret orden. Dele af funktionaliteten kan eventuelt forenkles hvis nødvendigt.

Hovedformålet med opgaven er at opnå erfaring med design af kode til genbrug, og brug af designpatterns.

Gruppe 8
Louise Mann mann@ruc.dk
Peter Mann peterrm@ruc.dk