11174 Datasikkerhet

Øving 7

1. PGP bruker ElGamal for kryptering av sesjonsnøkler, selv om det i oppsettet for PGP påstås at man bruker Diffie-Hellman. Ville det faktisk være mulig å bruke Diffie-Hellman for et system som PGP? Hvordan skulle dette i så fall gjøres?

2. Hvordan bør en privat nøkkel beskyttes når den lagres på disk?

3. Forklar hva PGP gjør for å få den krypterte private nøkkelen på disk frem i klartekst slik at den kan brukes til å kryptere en melding.

4. Hvor tror du det er naturlig å finne den offentlige PGP-nøkkelen til foreleseren i 11174 Datasikkerhet?

5. Praktisk oppgave: Gå til http://www.pgpi.com og last ned PGP (evt. GPG – GNU Privacy Guard). Følg bruksanvisningen og generer et nøkkelpar for deg selv. Send deretter en kryptert melding til foreleseren der du skryter av hvor flink du har vært (beskjedenhet er jo en dyd, så du vil vel ikke at andre skal vite at du skryter av deg selv...).

6. Bruk så PGP til å verifisere signaturen på denne oppgaven! (Signaturen er i en egen fil)