Tietoturvan perusteet, kurssikoe 4.5.2010

Kirjoita jokaiseen vastauspaperiin kokeen nimi, pvm, oma nimesi, henkilötunnuksesi tai opiskelijanumerosi ja allekirjoituksesi. Numeroi sivut.

1. **a)** Selitä, mitä suolaus (salting) tarkoittaa salasanojen yhteydessä. (7 p)
   b) Selitä, miten tiedostoihin liittyvät oikeudet otetaan huomioon, kun käyttäjä tekee muutoksen salasanatiedostoon salasanaa vaihtaessaan unix-järjestelmässä. (Eli selitä, miten eri uid:t tulevat käyttöön.) (7 p)
2. Esittele tyypillisiä ohjelmistovirheitä. Kutakin virhetyyppiä kohti mainitse implementointi- tai hallintosääntö, jota noudattamalla virhe olisi voitu välttää. (14 p)
3. Esittele palomuurityypit. (12 p)
4. Pohdi X.509-varmenteiden peruuttamiseen liittyviä ongelmia. Esittele samalla myös OCSP:n hyviä ja huonoja puolia. (14 p)