Tietoturvan perusteet, erilliskoe 1.2.2011

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

1. Esittele seitsemän mielestäsi tärkeintä implementointisääntöä.
2. Miksi salalohkot suositellaan ketjutettavaksi. Esittele ketjutusmenetelmät CBC ja Laskurimoodi. Analysoi yhden bitin tiedonsiirtovirheen vaikutusta vastaanottajalla. Tarvitseeko tällaisesta välittää, vai hoitaako TCP aina pakettien saapumisen oikeanmuotoisena perille?
3. Piirrä seuraavat palomuuriratkaisut ja selitä niiden hyvät ja huonot puolet tai sovellustilanteet: yksinkertainen yhdyskäytävä, kaksoisyhdyskäytävä, rajoitusaliverkkopalomuuri.
4. Tarkastellaan varmenteita. Vastaa lyhyesti seuraaviin kysymyksiin:
   a) Mikä on varmenne?
   b) Miksi varmenteita tarvitaan?
   c) Minkälaisia ongelmia liittyy peruutuslistoihin?
   d) Mikä on OSCP?