Tietoturvan perusteet, erilliskoe 17.8.2010

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

1. Esittele omasta mielestäsi viisi tärkeintä implementointi- tai hallintosääntöä. Perustele, miksi ne ovat tärkeämpiä kuin muut säännöt.
2. Miksi salalohkot yleensä ketjutetaan ennen lähetystä? Esittele ketjutustekniikat CBC (cipher block chaining, salalohkojen ketjutus) ja laskurimoodi CTR. Analysoi yhden bitin siirtovirheen vaikutusta vastaanottajalla.
3. Selitä lyhyesti seuraavat asiat:
   a) Salasanojen suolaus.
   b) Sääntöpohjainen (mandatory) pääsynvalvonta. (Anna myös esimerkki.)
   c) Symboliset linkit.
4. Pohdi X.509-varmenteiden peruuttamiseen liittyviä ongelmia. Esittele samalla myös OCSP:n hyviä ja huonoja puolia.