Tietoturvan perusteet, erilliskoe 16. 11. 2012

Kirjoita jokaiseen vastauspaperiin kokeen nimi, pvm, oma nimesi, henkilötunnuksesi tai opiskelijanumerosi ja allekirjoituksesi. Numeroi sivut. Jätä ensimmäisen sivun yläreunaan leveä marginaali.

1. Vastaa seuraaviin kysymyksiin.
   a) Mikä on RSA-järjestelmässä nykyään suositeltu avaimen pituus?
   b) Mikä on suositeltu minimaalinen avaimen pituus AES:ssä?
   c) Mikä on suositeltu minimaalinen tiivistefunktion tuloksen pituus?
   d) Mitä tarkoittaa sääntöpohjainen (mandatory) pääsynvalvonta?
   e) Mitä tarkoittaa yksilöpohjainen (discreatory) pääsynvalvonta?
2. Miten ketjutusmenetelmät ECB (electronic code book), CBC (cipher block chaining) ja CTR (counter mode) toimivat?
3. Esittele käytäntöjä ja vastatoimenpiteitä, joilla estetään haittaohjelmien tarttuminen.
4. **a)** Mitä tietoja X.509-varmenne sisältää?
   b) Miten varmennetta käytetään todennuksen yhteydessä?