TIE-30300 Tietoturvallisuuden jatkokurssi
Tentti 11.2.2015 / Jarmo Harju

Ei laskimia.

Tehtäviä on viisi ja ne arvostellaan asteikolla 0-6 pistettä eli maksimipistemäärä on 30 p. Tähän lisätään välikokeen bonuspisteet ja siitä vähennetään harjoitustöiden mahdolliset sakkopisteet, jolloin saadaan kokonaispistemäärä. Läpipääsyyn tarvitaan normaalisti kokonaispistemäärä 15 p.

1. Kerro lyhyesti (max puoli sivua per kohta), mitä tiedät seuraavista tietoturvaohjeistoista tai -organisaatioista. Riittää, että valitset kaksi alla olevista kolmesta kohdasta, eli yhden voit jättää vastaamatta:

   a) Vahti-ohjeistot yleensä

   b) KATAKRI

   c) CERT.

2. a) Millaisia asioita salasanajärjestelmän toteuttamisessa pitää ottaa huomioon? Voit käyttää esimerkkinä UNIX-järjestelmään toteutettuja piirteitä.

   b) Mitä salasanajärjestelmiin liittyen tarkoitetaan toiminnoilla "suolan lisäys" ja "venyttäminen eli stretching"? Kerro erityisesti, miten ne vaikeuttavat salasanan murtoyrityksiä.

3. a) Kerro RSA:n toimintaperiaate kompaktissa muodossa. Selvitä erityisesti, mistä osista (parametreista) julkinen ja salainen avain on muodostettu, ja miten nämä osat liittyvät toisiinsa.

   b) Mihin matemaattiseen ominaisuuteen RSA:n turvallisuus perustuu? Miten turvallisuus pettää (toisin sanoen, mitä hyökkääjä voi tehdä), jos tuo mainittu ominaisuus osoittautuukin paikkansa pitämättömäksi?

4. a) Mitä tarkoitetaan sokealla allekirjoituksella ja mitä sovelluksia sillä voisi olla?

   b) Miten RSA:n avulla voisi toteuttaa sokean allekirjoituksen?

5. a) Anna yleiskuva SSL/TLS-protokollasta ja sen toiminnasta.

   b) Kerro hieman tarkemmin kyseisen protokollan yksityiskohdista sanomakaaviota apuna käyttäen.