TIE-30300 Tietoturvallisuuden jatkokurssi Ei laskimia.
Tentti 25.3.2015 / Jarmo Harju

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. Valitse vain kaksi alla olevista kolmesta kohdasta, eli yhden voit jättää vastaamatta (3 p per kohta):

   a) ISO/IEC 27000 -sarja

   b) KATAKRI

   c) CERT.

2. a) Mitkä ovat käyttöjärjestelmän keskeiset käsitteet? Miten tietoturvatoiminnot liittyvät käyttöjärjestelmään? (3 p)

   b) Mitä ovat kryptoprimitiivit? Listaa vähintään kuusi kryptoprimitiiviä. (3 p)

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. Valaise asiaa pieniä lukuja käyttävällä esimerkillä, jossa laskuja ei ole tarpeen tehdä tarkemmin kuin mitä kynällä ja paperilla saa kohtuudella aikaiseksi. (4 p)

   b) Mihin matemaattiseen ominaisuuteen RSA:n turvallisuus perustuu? Miten turvallisuus pettää (toisin sanoen, mitä hyökkääjä voi tehdä), jos tuo mainittu ominaisuus osoittautuukin paikkansa pitämättömäksi? (2 p)

4. a) Kerro vuosalauksen periaatteet ja mahdolliset edut lohkosalaukseen verrattuna. (4 p)

   b) Miten siirtorekisterit liittyvät vuosalaukseen? (2 p)

5. a) Kuvaa tilattoman palomuurin toimintaperiaatetta. (3 p)

   b) Mitä tilallinen palomuuri tekee eri tavalla kuin tilaton, ja mitä hyötyä ja/tai haittaa tilallisuudesta on? (3 p)