TENTTI 12.2.2019
KYBERTURVALLISUUS I: PERUSTEET, TIE-30151

Marko Helenius

Tentissä ei saa käyttää oheismateriaalia eikä laskinta. Vastaa selkeästi.
Huomaa, että neljäs ja viides tehtävä ovat toisella sivulla.

(6 pistettä/tehtävä)

Tehtävä 1

Mikä on? (lyhyt määrittely riittää)
a) Lohkosalausmoodi
b) HTTPS
c) RSA
d) Hajautettu palvelunestohyökkäys
e) Hyökkäyspuu
f) IPsec

Tehtävä 2

Miksi tietoturvaohjelman kehittäjän tulisi huomioida käytettävyys ohjelmassaan? Mitä ongelmia tietoturvaohjelman käytettävyyteen voi liittyä ohjelman kehittäjän näkökulmasta?

Tehtävä 3

Piirrä kuva, josta selviää mahdollisimman hyvin, miten varmenne sekä varmennejärjestelmä toimivat. Täydennä kuvaa tarvittaessa tekstillä. Sisällytä myös varmenteen sisältämät tiedot. Huomaathan, että avaintenhallinta liittyy läheisesti myös varmenteisiin.

Tehtävä 4

Millaisia ominaisuuksia tiivisteiden laskemiseen käytetyillä Hash-funktioilla on? Miksi salasanat pitäisi tallentaa tiivisteinä selkotekstin sijasta? Millaisia etuja tiivisteen käytöllä on salasanojen tapauksessa? Entä voiko niistä olla jotakin haittaa?

Tehtävä 5

Ohjelmistokehitysyritys Hipster Oy tuottaa toisille yrityksille ja valtionhallinnolle ohjelmistoja asiakkaiden tarpeiden perusteella. Ohjelmistot ovat internet-pohjaisia ja niihin tallennetaan kuluttaja-asiakkaiden tietoja, jotka vaihtelevat ohjelmistokohtaisesti, mutta mm. luotokorttien tietoja, henkilötunnuksia, asiakkaiden yhteystietoja, tuotteiden takuutodistuksia ja ostohistoriatietoja tallennetaan. Ohjelmistoilla on mahdollista tehdä myös personoitua mainontaa. Miten EU:n tietosuoja-asetukset eri vaatimukset tulee ohjelmistoissa ottaa huomioon?