TENTTI 22.5.2019
KYBERTURVALLISUUS I: PERUSTEET, TIE-30151

Marko Helenius
Tentissä ei saa käyttää oheismateriaalia eikä laskinta. Vastaa selkeästi.
Huomaa, että viimeinen viides tehtävä on toisella sivulla.

(6 pistettä/tehtävä)

Tehtävä 1

Mikä on? (lyhyt määrittely riittää)
a) Symmetrinen salaus
b) Käytettävä tietoturva
c) Varmenne
d) MD5
e) SHA-1
f) SHA-256

Tehtävä 2

Olet laatimassa yrityksen henkilöstölle salasanojen luomiseen ja käyttöön liittyvää ohjeistusta. Yrityksen sisäisten järjestelmien salasanat (3 eri järjestelmää) on muistettava ulkoa, jolloin niitä ei saa tallentaa salasananhallintaohjelmaan, mutta yrityksen ulkoisia salasanoja varten käytössä on salasananhallintaohjelma.

Millaisia ohjeita annat ja miten perustelet ne?

Tehtävä 3

Miten tilallinen ja tilaton palomuurisuodatus toimivat?
Ota mukaan esimerkkejä palomuurisäännöistä.

Tehtävä 4

Piirrä mahdollisimman täsmällinen kuva Diffie-Hellman -avaintenvaihdosta.
Selvennä kuvaa tarvittaessa tekstillä.

Tehtävä 5

Oikeusministeriön oppaassa "Miten valmistautua EU:n tietosuoja-asetukseen?" luvuissa 2 ja 3 kuvataan oheiset asiat. Mitä nämä tarkoittavat ja mitä nämä merkitsevät rekisteristä vastuullisen kannalta?

2. Tietosuojaperiaatteiden toteuttaminen
    2.1 Sisäänrakennettu ja oletusarvoinen tietosuoja
    2.2 Osoitusvelvollisuus
3. Riskiperusteinen lähestymistapa