TENTTI 15.12.2017
JOHDATUS TIETOTURVALLISUUTEEN, TIE-30150

Marko Helenius

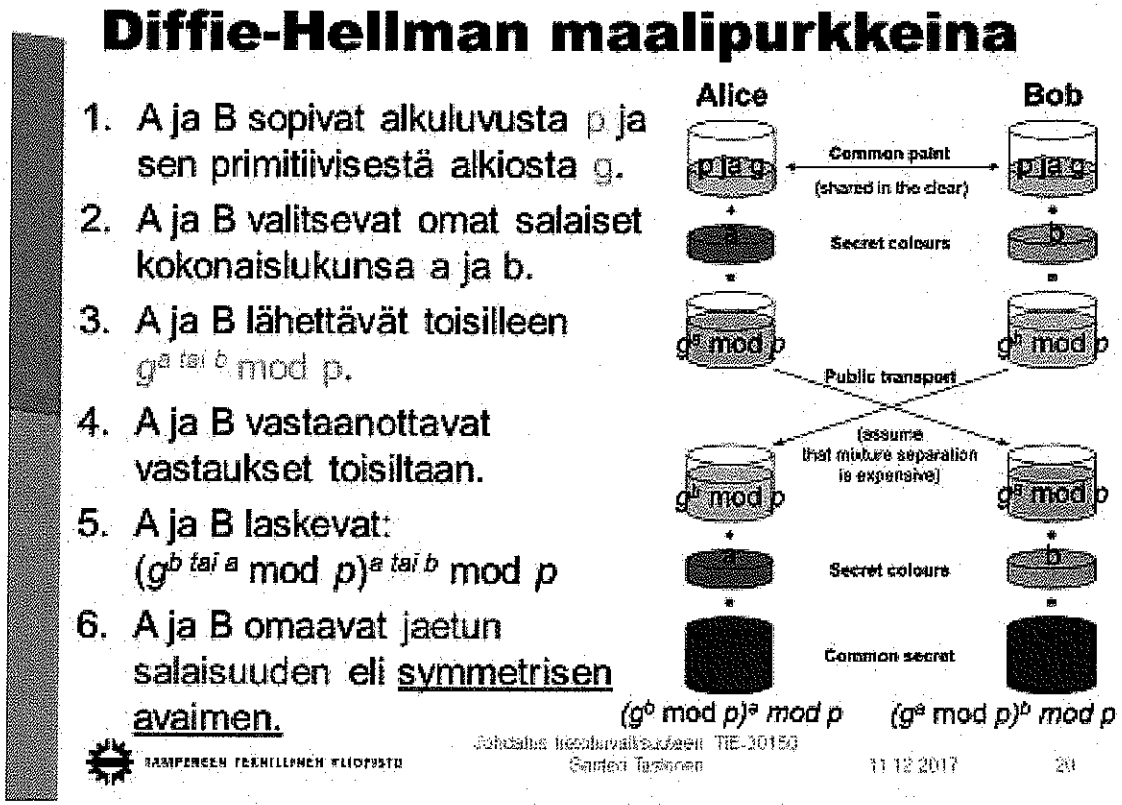
Tentissä ei saa käyttää oheismateriaalia eikä laskinta. Vastaa selkeästi.

(6 pistettä/tehtävä)

1. Hipster Oy on päättänyt aloittaa verkkokaupan. Asiakkaista tallennetaan mm. yhteystiedot, ostohistoria ja luottokorttitiedot. Yhtenä uhkana on asiakastietojen vuotaminen palvelimelta. Tee tästä uhka-analyysi hyökkäyspuuta käyttäen. Muista oheiset osa-alueet:
   - Prevent – Estä hyökkäyksen onnistuminen täysin
   - Deter – Tee hyökkäämisestä hyvin kallista tai vaivalloista
   - Deflect – Tee toisesta kohteesta houkuttelevampi
   - Mitigate – Vähennä onnistuneen hyökkäyksen vaikutuksia
   - Detect – Havaitse hyökkäys tai sen yritys
   - Recover – Toivu seurauksista

2. Mitä käytettävyyteen ja turvallisuuteen liittyviä asioita pitäisi huomioida salasanamanageria suunniteltaessa ja kehitettäessä? Pohdi erityisesti, minkälaisia ristiriitoja näiden välillä voi olla salasanamanagerien tapauksessa. Jäsentele vastauksesi ennen sen kirjoittamista. Jätä jäsentely näkyviin vastaukseesi.

3. Kerro oheisen kuvan perusteella, miten Diffie-Hellman -avaintenvaihtoprotokolla toimii.



4. Olet 300 hengen yrityksen tietoturvapäällikkö. Yritys asentaa ja ylläpitää muihin yrityksiin sekä kotitalouksiin hälytys- ja valvontakamerajärjestelmiä. Yrityksellä on valvontakeskuksia, joihin asiakkaat voivat halutessaan ulkoistaa valvonnan. Miten toimit, että yritys toimii 25.5.2018 voimaan astuvan EU:n tietosuoja-asetuksen mukaisesti? Mitä eri asioita yrityksessä pitää asetuksen vuoksi ottaa huomioon? Huomaathan, että yritys tarvitsee myös asiakasrekisterin.

Muistamisen helpottamiseksi ohessa on tenttimateriaalina olleen
Oikeusministeriön oppaan sisällysluettelo.

Miten valmistautua EU:n tietosuoja-asetukseen?

JOHDANTO

1 Henkilötietojen käsittelyn arviointi

2. Tietosuojaperiaatteiden toteuttaminen

2.1 Sisäänrakennettu ja oletusarvoinen tietosuoja

2.2 Osoitusvelvollisuus

3. Riskiperusteinen lähestymistapa

4. Tietosuojaa koskeva vaikutustenarviointi ja ennakkokuuleminen

5. Henkilötietojen käsittelyn oikeusperusteet

6. Henkilötietojen käsittelyn ulkoistaminen

7. Rekisteröidyn oikeudet

7.1 Oikeus saada läpinäkyvää informaatiota henkilötietojen käsittelystä

7.2 Rekisteröidyn oikeus saada pääsy tietoihin

7.3 Oikeus tietojen oikaisemiseen ja oikeus tulla unohdetuksi

7.4 Oikeus käsittelyn rajoittamiseen ja rekisterinpitäjän velvollisuus ilmoittaa rajoituksesta

7.5 Oikeus siirtää tiedot järjestelmästä toiseen

7.6 Vastustamisoikeus

7.7 Automatisoidut yksittäispäätökset ja profilointi

8. Organisaation toimiminen useassa EU:n jäsenvaltiossa

9. Tietoturva

10. Henkilötietojen tietoturvaloukkauksiin valmistautuminen

11. Tietosuojavastaavan nimittäminen

12. Tietosuoja-asetuksen tulkinta ja tuleva ohjeistus