TTY / TLT / M.Helenius

TLT-3201 Tietoturvallisuuden jatkokurssi

Tentti I 13. 12. 2010

Tentissä ei saa käyttää oheismateriaalia eikä laskinta.

Vastaa oheisiin kysymyksiin selkeästi. Jokaisesta tehtävästä maksimipistemäärä on 6 pistettä.

1. Harjoitustöistä poimittu kysymys: Mille eri asioille aikaleima on tärkeä ja miksi?

2. Oletetaan, että olet tuhannen työntekijän teollisuusautomaatiorobotteja kehittävän, valmistavan ja omia tuotteita markkinoivan yrityksen tietoturvapäällikkö. Yrityksellä ei ole aikaisemmin luokiteltu tietoaineistoja ja luokittelu ja käsittely uudistetaan nyt kokonaan. Miten toteutat yrityksen tietoaineistojen luokituksen ja käsittelyn?

3. Mitä keinoja on roskasähköpostin suodattamiseksi?

4. Mitä tarkoittaa lohkosalaus ja miten se toteutetaan?

5. Kuvaa oheisilla merkinnöillä miten PGP muodostaa osapuolen A viestin osapuolelle B
   a) allekirjoitus (2p)
   b) salaus (2p) ja
   c) sekä allekirjoitus että salaus (2p)

Z = ZIP = tiivistys
H = hash = yksisuuntainen tiivistys
E_K = kryptaus avaimella K (joka on symmetrinen tai julkinen)
E_K^{-1} = allekirjoitus julkista avainta K vastaavalla yksityisellä avaimella K^{-1}
|| = katenaatio
K_s = istuntoavain, symmetrinen, joka viestille omansa
M = alkuperäinen viesti

Vinkkejä:

- Tiivistyksellä Z viesti saadaan pienempään tilaan. Ei ole siis protokollan toiminnan kannalta olennaista, mutta pakkaaminen sisällytetään kaikkiin lopputuloksena saataviin viesteihin.
- Suluilla ilmaistaan toimintojen järjestys, Esimerkiksi. $E_{Ks}(Z(M))$ ensin tiivistää (pakkaa) viestin M ja kryptaa sitten tiivistetyn viestin istuntoavaimella K_s.
- Yksisuuntaista tiivistämistä käytetään allekirjoituksessa, koska on laskennallisesti kevyempää allekirjoittaa tiiviste kuin itse viesti.
- Istuntoavaimella tehdään laskennasta kevyempää. Siis kryptataan symmetrinen istuntoavain viestin M sijaan ja istuntoavaimella puolestaan kryptataan viesti M.
- Istuntoavaimen muodostamiseen ei tarvitse tässä ottaa kantaa, sillä viestin muodostaja luo kertakäyttöisen istuntoavaimen satunnaisesti.
- Jos et ole varma merkintöjen oikeellisuudesta, sanallisesti kuvaamalla voit ilmaista, mitä olet ajatellut.