Teknillinen korkeakoulu
Sähkö- ja tietoliikennetekniikan osasto
Tietoverkkolaboratorio
S-38.108 Tietoliikenneverkkojen arkkitehtuurit
4. laskuharjoitus 7.11.2001

Kotitehtävät palautetaan **21.11.2001 klo 10.00** mennessä kurssin lokeroon (G-siipi, 2. kerros) tai sähköpostitse osoitteeseen piia@tct.hut.fi.
Huomaa kotitehtävien poikkeava pisteytys: ykkös- ja kakkostehtävistä voi saada yhteensä puolet tämän laskarin pisteistä, toinen puolikas on tarjolla kolmostehtävästä.

DEMOTEHTÄVÄT

1. Mitä on bittijono 1000110101

   a) NRZ-koodattuna
   b) NRZI-koodattuna
   c) Manchester-koodattuna
   d) 4B/5B-koodattuna

2. Kehykset lähetetään vasemmalta alkaen. Generaattoripolynomi on 11100.

   a) Vastaanotettu kehys on 10011100010. Onko se virheetön?
   b) Lähetettävä viesti on 1101001. Mikä on sen CRC-tarkistussumma, ja minkälainen kehys lopulta lähtee vastaanottajalle?
   c) Voiko bitit laittaa matkaan kummasta päästä tahansa alkaen?

3. Tietoturvakäsitteitä

   a) symmetrinen ja asymmetrinen salaus
   b) todennus (authentication)
   c) valtuutus (authorization)
   d) DoS-hyökkäys (Denial of Service)
   e) Man-in-the-Middle –hyökkäys

KOTITEHTÄVÄT

1. Bittejä jonossa

   a) Kehykset lähetetään vasemmalta alkaen. Generaattoripolynomi on 1101.

   - Vastaanotettu kehys on 11001000111. Onko se virheetön?
   - Lähetettävä viesti on 101100. Mikä on sen CRC-tarkistussumma, ja minkälainen kehys lopulta lähtee vastaanottajalle?

   b) Johtokoodit

   - Mitä on NRZI-koodattuna bittijono 1100101011?
   - Mitä on Manchester-koodattuna bittijono 1011101000?

2. Käytännön tietoturvaa

   a) Emppu haluaa lähettää Tompalle PGP-kryptatun ja –allekirjoitetun sähköpostiviestin. Molemmilla on PGP-avainparit valmiina ja molemmilla on myös toistensa julkiset avaimet. Miten Emppu lähettää viestin ja mitä Tomppa tekee sen saatuaan?

   b) Empun ja Tompan kaverilla Masalla on kotona kiinteästi verkossa oleva Linux-palvelin, johon myös Empulla ja Tompalla on käyttäjätunnukset. Eräänä päivänä Masa kertoo, että ensi viikosta lähtien hänen koneeseensa ei enää saa yhteyttä Telnetillä, jota Emppu ja Tomppa ovat tähän asti käyttäneet. Miksi Masa teki tällaisen ratkaisun? Miten Emppu ja Tomppa nyt voivat ottaa yhteyden Masan koneeseen?

   c) Emppu on hankkinut itselleen verkkopankin käyttäjätunnuksen ja aikoo nyt maksaa laskun verkossa. Tompan mielestä verkkopankissa maksaminen on kuitenkin jonkin verran arveluttavaa, ja hän luettelee Empulle joukon olettamiaan tietoturvariskejä. Millaisista asioista Tomppa voisi olla huolissaan? Olisiko Empun sittenkin turvallisempaa mennä maksamaan lasku läheisen ostoskeskuksen maksuautomaatille?

3. Tässä tehtävässä on nimenomaan tarkoitus etsiä tietoa. Millintarkkoja oikeita vastauksia ei ole, vaan tarkoitus on etsiä, löytää ja oivaltaa. Omien aivojen käyttö on jopa suotavaa, ja esimerkiksi yleisestä yhteiskuntatietoudesta ja uutisten seuraamisesta voi tehtävässä olla yllättävää hyötyä. Ellet ota asioita omasta päästäsi, muista merkitä näkyviin käyttämäsi lähteet (esimerkiksi nettisivusta tarkka URL, sanomalehdestä nimi ja ilmestymispäivä... – jos kysyt isosiskolta tai kaverilta, merkitse sekin).

   Suomen kansalaisen perusoikeuksiin[1] kuuluu, että ”Kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton.” Miten vallan kolmijaon[2] eri osapuolet (eduskunta, presidentti ja valtioneuvosto sekä riippumattomat tuomioistuimet) ovat toisaalta turvanneet, toisaalta rajoittaneet lainkohdan toteutumista erityisesti teleliikenteessä ja sähköisessä viestinnässä?

[1] Yhteiskuntaopin kertaus suoraan perustuslaista
[2] Yhteiskuntaopin kertaus suoraan perustuslaista, osa 2