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

KOTITEHTÄVIEN RATKAISUT

1. Bittejä jonossa

a) Kehykset lähetetään vasemmalta alkaen. Generaattoripolynomi on 1101.

- Vastaanotettu kehys on 11001000111. Onko se virheetön?

  Jaetaan kehys generaattoripolynomilla:

```
        10010011
1101|11001000111
    1101
     0011
     0000
      0110
      0000
       1100
       1101
        0010
        0000
         0101
         0000
          1011
          1101
           1101
           1101
            000
```

  Jakojäännös on nolla, joten kehys on virheetön.

- Lähetettävä viesti on 101100. Mikä on sen CRC-tarkistussumma, ja minkälainen kehys lopulta lähtee vastaanottajalle?

  Viesti V = 101100
  Generaattoripolynomi G = 1101 (n+1 bittiä pitkä)
  Tarkistussumma FCS = ? (n bittiä pitkä)

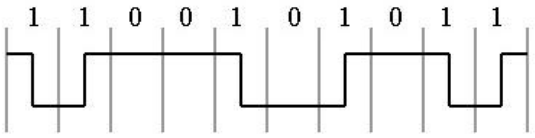
  Generaattoripolynomi voidaan kirjoittaa myös muotoon $x^3+x^2+x^0$. Koska G on kolmannen asteen polynomi, viestin loppuun lisätään kolme nollaa ennen kuin se jaetaan G:llä.

```
      110011
1101 | 101100000
     1101
      1100
      1101
       0010
       0000
        0100
        0000
         1000
         1101
          1010
          1101
           111
```

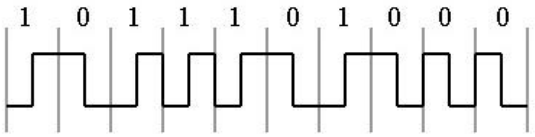
Viestin CRC-tarkistussumma on 111. Lähetettävä kehys saadaan laskemalla yhteen tarkistussumma ja viesti, jossa ovat edelleen mukana jakolaskua varten lisätyt nollat: 101100000 + 111 = 101100111.

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?

1. Emppu salaa viestin Tompan julkisella avaimella ja allekirjoittaa sen omalla salaisella avaimellaan.
2. Emppu lähettää viestin.
3. Tomppa vastaanottaa viestin ja purkaa sen omalla salaisella avaimellaan.
4. Allekirjoituksen Tomppa saa avattua (tarkistettua) Empun julkisella avaimella.

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?

Telnet-protokolla kuljettaa kaiken liikenteen selväkielisenä ASCII-tekstinä, myös salasanat. Kuka tahansa, joka pääsee tällaiseen yhteyteen käsiksi, eli verkossa lähettäjän ja vastaanottajan väliin, saa verkkoliikennettä tarkkailemall selville Empun ja Tompan käyttäjätunnukset ja salasanat. Masan huoli koneensa tietoturvasta on aivan aiheellinen.

Masa voi asentaa koneelleen SSH-palvelinohjelman, jolloin Emppu ja Tomppa voivat käyttää SSH-pääteohjelmaa yhteyden ottamiseen. SSH kryptaa kaiken verkkoliikenteensä, joten salasanoja(kaan) ei saa liikenteestä saa selville. Masan kannattaa kuitenkin hankkia SSH2-protokollaa käyttävän palvelinohjelman, koska nyt jo vanhentuneessa SSH1-protokollassa on turva-aukkoja. Myös Empun ja Tompan on tällöin hankittava itselleen SSH2-protokollaa käyttävät pääteohjelmat.

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?

Asioita, joista Tomppa esimerkiksi voisi olla huolissaan:

- Onko yhteys suojattu vai pystyykö kuka tahansa verkkourkkija kuuntelemaan liikennettä?
  > Suomalaisissa verkkopankeissa yhteydet on nykyään suojattu SSL-protokollan avulla, joten Emppu tuskin joutuu käyttämään suojaamatonta yhteyttä. Kannattaa silti tarkistaa, ettei vahingossakaan voi käyttää suojaamatonta yhteyttä.
- Onko Empulla käytössä SSL:n uusi versio? Miten pitkiä avaimia yhteyden salaamisessa käytetään?
  > Verkkopankeissa yhteyden suojaamiseen käytetään useimmiten SSL-protokollaa, jonka avaimen pituus oli aiemmin rajoitettu (USA:n vientimääräysten takia) 40 bittiin. Symmetrisen avaimen pituuden pitäisi kuitenkin olla 128 bittiä, jotta sitä voitaisiin pitää turvallisena. SSL:n uusin versio v3 saadaan käyttämään 128-bittisiä avaimia myös USA:n ulkopuolella, mutta jotta tästä olisi hyötyä, on myös vastapuolen pystyttävä käyttämään pitkiä avaimia. SSL v3:a kannattaa käyttää myös sen takia, että sitä ainakin toistaiseksi pidetään turvallisena protokollana, toisin kuin edeltäjiään, joista on löytynyt useita turva-aukkoja.
- Maksaako Emppu laskunsa varmasti oikeassa verkkopankissa vai paikassa, joka vain näyttää verkkopankilta?
  > Verkkopankin on pystyttävä tunnistamaan käyttäjä, mutta vähintään yhtä tärkeää on, että käyttäjä pystyy luotettavasti tunnistamaan verkkopankin. Tunnistamiseen ei riitä WWW-osoite tai sivujen ulkonäkö, vaan on käytettävä esimerkiksi sertifikaatteja.
- Jos Emppu maksaa laskun yleisellä koneella (esimerkiksi kirjastossa), on hänen muistettava tyhjentää selaimen välimuisti, jotta sinne ei jäisi mitään ylimääräisiä tietoja. Selain täytyy myös sulkea ennen poistumista koneelta.

Ostoskeskuksessa Emppua vaanivat toisenlaiset vaarat kuin koneen ääressä. Joku voi kurkkia kortin tunnusluvun Empun olan yli ja ryövätä myöhemmin kortin ja tyhjentää Empun tilin. Maksuautomaattiin voi olla myös asennettu ”irtokuoret”, jolloin valenäppäimistö tallentaa

Empun näppäilemän tunnusluvun ja korttiaukon päällä oleva lukija kortin magneettinauhan. Lopputulos on sama kuin aikaisemminkin: Empun tili ammottaa pian tyhjyyttään. Laskun maksaminen ostoskeskuksessa ei siis välttämättä ole yhtään sen turvallisempaa kuin sen maksaminen verkossa, ja joissain tapauksissa ostoskeskukseen meno voi olla paljon vaarallisempaakin.

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

   Suomen lait, asetukset ja säädökset (sekä paljon muuta) ovat verkossa osoitteessa <http://www.finlex.fi>. Eduskunnalle annetut lakiesitykset ja muuta tietoa Arkadianmäen tapahtumista on tarjolla osoitteessa <http://www.eduskunta.fi>. Liikenne- ja viestintäministeriön kotisivuilla <http://www.mintc.fi> esitellään ministeriön omia lakivalmisteluja ja kerrotaan muitakin ajankohtaisia asioita ministeriön toimialueelta.

   Eduskunta säätää lait, mutta myös presidentti ja valtioneuvosto osallistuvat niiden laatimiseen, joten nämä kaksi vallan kolmijaon osapuolta voidaan niputtaa lainsäädäntöpuolta edustaviksi. Riippumattomat tuomioistuimet ovat lakien varsinaisia käyttäjiä, eli ne tulkitsevat lainsäätäjän kirjaamia pykäliä.

   Lainsäädännössä viestintäsalaisuutta turvataan useammassakin kohdassa:
   - Rikoslain 38. luku Tieto- ja viestintärikoksista (578/1995)
   - Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta (565/1999)
   - Laki yksityisyyden suojasta työelämässä (477/2001)

   Rikoslaki kieltää myös salakuuntelun (Laki rikoslain muuttamisesta 531/2000 5§).

   Lainsäädäntö antaa myös mahdollisuuden loukata viestintäsalaisuutta. Tosin oikeus on vain harvoilla ja valituilla, ja heilläkin ainoastaan erikoistilanteissa.
   - Pakkokeinolain luku 5 a 2§ - telekuuntelun edellytykset, 3§ - televalvonnan edellytykset ja 4§ - teknisen tarkkailun edellytykset (1026/1995)
   - Puolustustilalaissa viittauksia sensuuriin ja salassapitovelvollisuuteen (Puolustustilalaki 1083/1991)

Tietosuojavaltuutettukin on ottanut kantaa sähköpostin käyttöön työpaikalla. Tulkinnan mukaan työnantajalla on oikeus määritellä, mihin työpaikan sähköpostiosoitetta käytetään, mutta luvatta ei työntekijän sähköposteja saa lukea.
<http://www.tietosuoja.fi/3282.htm>

Oikeuden laintulkinnat rajoittavat toisinaan viestintäsalaisuutta.

- Johan Helsingiuksen anonyymipalvelinta käytettiin scientologien tekstien levittämiseen. Scientologit vaativat Helsingiusta kertomaan, kuka oli lähettänyt viestit, ja kun Helsingius ei suostunut, scientologit tekivät rikosilmoituksen. Hovioikeus velvoitti Helsingiuksen paljastamaan viestien lähettäjän.
  <http://www.helsinginsanomat.fi/uutisarkisto/19970605/koti/970605ko02.html>
  Hovioikeuden päätös:
  <http://www.helsinginsanomat.fi/uutisarkisto/19970605/koti/970605ko30.html>

Ongelmatapauksia:

- Soneran johtajat lukivat entisen työntekijän sähköpostia.
  <http://www.helsinginsanomat.fi/uutisarkisto/19991202/talo/991202ta06.html>
  Osapuolet sopivat jutun ennen oikeuskäsittelyä.
- Helsingin Sanomien artikkelin mukaan sähköpostin ja Internetin käyttöä tarkkaillaan yleisesti työpaikoilla.
  <http://www.helsinginsanomat.fi/arkisto/juttu.asp?id=20010115KO9>