Open your mind. LUT.
Lappeenranta University of Technology
LUT Tietotekniikka

8.11.2012

CT50A2000 Tietojenkäsittelyn perusteet I

Lasse Lensu

Ongelmavirike 5

Yksi tietojenkäsittelyn tyypillisimpiä tehtäviä on muuntaa tietoa toiseen, algoritmin, sovelluksen tai käyttäjän kannalta tarkoituksenmukaisempaan tai informatiivisempaan muotoon. Talletetussa ja siirrettävässä tiedossa on useimmiten päällekkäisyyttä eli redundanssia eli se ei ole informaatioteorian mukaisessa tiiveimmässä mahdollisessa muodossa. Tätä käytetään hyväksi tietoa tiivistettäessä, mikä vaatii tiedon koodaamisen uudelleen joko häviöttömästi tai häviöllisesti. Uudelleen koodattu tieto ei välttämättä muistuta alkuperäistä, suoraviivaisesti tulkittavissa olevaa informaatiota. Tuleekin helposti mieleen, että tuotettu koodi on kuin salakirjoitusta.

a) Mitä alla olevassa suomenkielisessä kooditekstissä mahtaa lukea? Huom. välilyöntiä tarkoittavat merkit on korvattu esityksessä alaviivoilla '_'.

```
POHFMNBOSBULBJTV_PO_NJFMFOLJJOUPJTUB_KB_PQFUUBWBJTUB
```

Tämähän on liian suoraviivaista. Entä seuraava?

```
YOMEESAE,PKIUTLSAS_OSSKTIATTSSIEAÄ__IIUT_EIVSMI.OITNSÄEU__R_I,ES_OTUAME_MSEDIUVI
TAPÄIOEDIEOLA__SDEILJGATOSOLVEEONILANLAENR_EE._EINKITD__KES,ÄTAOITONE_SMISNÄO_SE
II_SFTDKTTTNIAOÄAOITT,N_R_AO_ÄE_FOMKMDT_LSONAÄIAUTYOR_AYSTLUNVMUTTETKO_EASIENUIT
TLTEOT__TEYLIITÄUTTTYUIMEÄUIATPKVMONDEVUISIIR_ETI_LESTIHLOSKLNEEAYL_SOI_MNNVEEAO
STP__ÄEI_DIAAPMKN_OIMIAÄUS_VL_P_NÄKIJÄEOIK_LA_OLVNÄÄMLITKTA__YUESIOTAKTTOKEE_Ä_U
ETTKSTHMIIHÄOÄSOÄÄNNTJOIAAVTF_ÄÄNS__ITOSVN.YTTÖÄRAI__YIIT_MLÄKTTIITMAA_AATVVÖUAK
ONLÄEIMITINNL_ISÄSIR_AEEMTSTOJMLTLMETUTOUTEIÄTITAIUAT_ST_A.TN_URSÄT__UTTSEÄEAATS
AASD_SILUTARAUMS_KLA_K_NAÄHUE.TOJDH,ÄPE_IIAAD_VEK_ET_NOMIRI_TUSSLIÖÄN_OKISLKLI__
ASIIIÄLSH__ERAS_ITE_TNR_EVSÄL_
```

Voi olla, ettei edellisenkään kooditekstin selväkielistä versiota ole kovin hankalaa saada selville. Millaisella menetelmällä salaaminen kannattaisi tehdä turvallisesti?

b) Laatikaa 20 merkkiä pitkä viesti. Kollegat toisessa OLO-ryhmässä salaavat valitsemallaan menetelmällä ryhmänne laatiman viestin ja palauttavat kooditekstin ryhmällenne. Pystyttekö selvittämään millaisella menetelmällä viesti on salattu, kun tiedätte selväkielisen tekstin? Miten kyseisellä menetelmällä salattuja viestejä pystyisi avaamaan ilman tietoa selväkielisestä tekstistä?

PL 20
53851 LAPPEENRANTA
Sähköposti: lasse.lensu@lut.fi