KRYPTOGRAFIAN ALKEET

1. LASKUHARJOITUKSET

(1) Esitä esimerkki siitä, miksi

$$A \to 1,\ E \to 00, I \to 010, S \to 011, T \to 01$$

ei ole koodi.

(2) **(Tämä tehtävä on kolmen normaalin laskuharjoitustehtävän arvoinen.)** Seuraava teksti on suomenkielisestä alkutekstistä kryptattu käyttäen kirjainten korvaamista toisilla aakkoston kirjaimilla. (Vrt. esim. Ernvallin monisteen esimerkki 28.) Pura salaus.

VPHHTPL RJHP ESSPE NVPPL PWGPVSEVP BM VN MHSTP SPKBTPRRMM HMGCJL
UPNKNNL SJLPLSMML CMHMRVPL SMHSPRRJJL VNPLEEL SJLPLIMV LESP SEÅNL
BTSM SPKBTPRRP VPHHTPL WEL SMHCNLP BM CNHST REYRRP WELNL GPNHNLVE
WELNL BEVNLNVE HMGMMLRJPUMR BM WELNL CTHUNLSM RJRPVPUMR STUMHHM
EELNHHE WJJRMNL SJLPLIMV SEVSP RJTÅM NRNNLVE HTPRVJCMCPR
SMHÅNMHMPVNR UPPVMMR BM GMLMMBMR WEL BJHPVRP FMFYHTLPML
UPPVMPHHN BTSM CYVRYY HJSNGMML REGEL BM NVPRREGEEL VNL RJHSPLLML
GPLJHHN WELNR CJNNRMML CJKCCJKMML WEL VMM SJHRMSEEÅYR SMJHMMLVM
BM CEEVNN MKUTVVM STHGMLLNSVP REVVE UMHRMSJLLMVVM SMPSSP SJLPLSMML
UPPVMMR RJHPUMR VPVEEL GJRRM SJSMML NP CYVRYLYR HJSNGMML
SPKBTPRJVRM NPSE NVPRREGEEL VNL VNHPRYVRE SJLPLSMMHHN VPHHTPL
SJLPLIMV FNHVMVVMK BTJRJP SMJWJL UMHRMML BM WELNL SMVUTLVM
UMHMWRPUMR UMHSNPSVP GYOV WELNL YHPGYSVNLVE BEKSYRRYPUER
SJLPLSMML BM WELNL YHPGYVRNLVE CJWNNL SJJHHNVVMML MVRJP
HNVSPSJLPLIMRMK CPRTVMHPPL WEL VMLTP PSJPVNVRP NHESOOL SJLPLIMV
EHE MLRMJÅJ QNHTL UMHRMML EHE RJKWMML SMHCNLN VPLJL
UMHRMSJLLMVVMVP TL GPNV BTVVM MVJJ CYWPNL BJGMHPNL WNLSP VPLJL PVEVP
MPSMLM WELNHHW WMUMPRRPPL THNUML YGGEKKYVRE EHYE BM UPPVMJRRM
YWRE CMHBTL SJPL BJGMHPHHM PVEVP SJLPLIMV LNFJSMÅLNVVMK STKTRRP
WELNR NLRNPÅNLVNHPRREBPNL HTPRVJCMCCPNL SMHÅNMHMPVRNL UPPVMPÅNL
BM GMLMMBPNL CEEGPNWNSVP LPPL RNSP PVEVP SJLPLIMV ÅMLPNHPVVM BTHHN
SJLPLIMV MLRTO LPGNL FNHRNVMVVMK MVJJ NKPRYPLNL WNLSP BM WELNHHE TL
RMPRT BM UPPVMJV VNHPRREE JLPM BM KMRSMPVRM MKUTPRJSVPM BM TLIMHGPM
SJRVJRRMSTTL LYR WELNR RELLN WEL TVMM VNHPRREE REGEL SPKBTPRJSVNL

Teksti on napattu Simon Singhin Koodikirjan tehtävistä. Tässä tehtävässä lienee iloa esimerkiksi sivulta

http://www.cs.tut.fi/~jkorpela/kielikello/kirjtil.html

löytyvästä kopiosta Kielikellossa ilmestyneestä jutusta, jossa on esimerkiksi tilasto suomen kielen kirjainten yleisyydestä. Lisäksi googlaamalla voi esimerkiksi löytää verkkosivun, jossa saa laskettua kirjainten lukumäärän annetussa tekstissä. Tämä teksti toimitetaan myös sähköpostilla kaikille kurssilaisille, jotta analyysi olisi mahdollisimman helppo suorittaa.

(3) Seuraava englanninkielinen teksti on kryptattu käyttäen Hillin järjestelmää matriisilla

$$\begin{bmatrix} 4 & 3 \\ 3 & 2 \end{bmatrix}$$

WWFMODFJDYTTEECUOEODJG. Pura kryptaus.

(4) Olkoon avainsana LUMISADE. Käytetään avainsanan ohjaamaa kryptausta kuten Ernvallin monisteessa sivulla 21. Koodaa teksti (erikoismerkkejä ja numeroita ei tarvitse kryptausta):

Maan itäosassa verrattain pilvistä ja paikoin heikkoa lumisadetta. Maan länsiosassa sekä Pohjois-Pohjanmaalla ja Kainuussa enimmäkseen poutaa ja ajoittain selkeämpää. Lämpötila tänään päivällä -8...-18 astetta, huomenna pohjoisessa vähän alempi. Yölämpötila on pilvisyydestä riippuen -10...-20, paikoin -25 astetta. Heikkenevää pohjoisenpuoleista tuulta.