# KRYPTOGRAFIAN ALKEET

1. RÄKNEÖVNINGEN

(1) Ge ett exempel på värför

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

inte är en kod.

(2) **(Denna uppgift är värd tre normala räkneövningsuppgifter.)** Följande, ursprungligen finskspråkiga text är krypterad genom att ersätta varje bokstav med en annan bokstav i alfabetet (se t.ex. exempel 28 i Ernvalls kompendium). Dekryptera texten.

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

Texten är tagen från Simon Singhs bok Koodikirja. I denna uppgift kan man ha nytt av artikelkopian från tidningen Kielikello som hittas på sidan

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

I artikeln finns bl.a. statistik över hur ofta olika bokstäver förekommer i finsk text. Genom att googla kan man hitta t.ex. en sida, som räknar hur många gånger varje bokstav förekommer i texten. Texten kommer att skickas per e-post åt alla som deltar i kursen för att analysen skall kunna genomföras möjligtvis enkelt.

(3) Följande engelskspråkiga text har krypterats med Hills metod med krypteringsmatrisen

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

WWFMODFJDYTTEECUOEODJG. Dekryptera texten.

(4) Låt nyckelordet vara LUMISADE. Kryptera följande text med nyckelordsstyrd kryptering såsom det görs på sidan 21 i Ernvalls kompendium (specialtecken och siffror behöver ej krypteras):

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.