Kryptografian alkeet
1. harjoitukset, ratkaisuja
Jesse Jääsaari (jesse.jaasaari@helsinki.fi)

1. Esitä esimerkki siitä, miksi

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

ei ole koodi.

Ratkaisu. Jotta kyseinen muunnos olisi koodi, sen pitäisi olla injektiivinen. Näin ei kuitenkaan ole, sillä esimerkiksi $IS \to 010011$, kuin myös $TEAA \to 010011$.

2. 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.

Ratkaisu. Ensin on laskettava tekstissä esiintyvien kirjainten lukumäärät. Osoitteesta

http://jumk.de/wortanalyse/word-analysis.php löytyvä laskuri antaa seuraavan taulukon:[1]

Kirjain	Esiintymiskertoja	Kirjain	Esiintymiskertoja
A	0	P	141
B	32	Q	1
C	23	R	100
D	0	S	78
E	78	T	39
F	5	U	25
G	26	V	107
H	79	W	29
I	9	X	0
J	68	Y	24
K	20	Z	0
L	151	Å	10
M	167	Ä	0
N	94	Ö	0
O	4		

Seuraavaksi on pääteltävä miten kirjaimet muuntuvat. Yllä olevasta taulukosta nähdään, että tekstissä kaikkein useimmin esiintyvä kirjain on M. Koska Kielikellon artikkelin mukaan suomen kielessä useimmin esiintyvä kirjain on A, niin on luonnollista kokeilla mitä tapahtuu kun $M \to A$. Ideana on nyt katsoa tekstissä olevia lyhyitä sanoja, joissa on kirjain M. Suomen kielessä on vain vähän tällaisia sanoja, joten niistä on helppo arvata lisää muunnoksia. Epäselvissä tilanteissa (eli kun on vaikka kaksi järkevää vaihtoehtoa) Kielikellon artikkelin taulukkoon vertaamalla pystyy päättelemään oikean muunnoksen. Kun muunnoksia kertyy enemmän, niin aletaan katsomaan pidempiä sanoja, joissa on kirjaimia joiden muunnokset tiedetään. Näin saadaan lopulta selville kaikki muunnokset. Emme käy tässä koko päättelyä läpi, mutta vähän sen alkua selvennykseksi.

Tekstistä löytyy sana BM. Ainoa suomen kielen kaksikirjaiminen sana, joka loppuu kirjaimeen A on "JA". Siten päätellään, että $B \to J$. Seuraavaksi katsotaan sanaa VMM, mikä on muotoa ?AA. Suomen kielessä on kaksi tätä muotoa olevaa sanaa: "MAA" ja "SAA". Vertaamalla Kielikellon taulukkoon päätellään, että $V \to S$. Tällöin sana VN olisi muotoa S?, mistä voi arvata, että $N \to E$. Tämän jälkeen sanasta VNL voi nähdä, että $L \to N$. Jatkamalla tällaista päättelyä saadaan seuraavanlainen muuntotaulukko:[2]

$B \to$ J	$O \to$ Ö
$C \to$ P	$P \to I$
$E \to$ Ä	$Q \to P$
$F \to$ B	$R \to$ T
$G \to$ M	$S \to$ K
$H \to$ L	$T \to$ O
$I \to$ G	$U \to$ V
$J \to$ U	$V \to$ S
$K \to$ R	$W \to$ H
$L \to$ N	$Y \to$ Y
$M \to$ A	Ä$\to$ D
$N \to$ E	

Siten ratkaisuksi saadaan:[3]

[1] Huom. laskuri ei tunnista kirjainta Å, joten sen esiintymiset pitää laskea erikseen käsin.
[2] Ilmeisesti sekä $C \to P$, että $Q \to P$. Tämä on ainoa tapa, jolla teksti on järkevä.
[3] Huomaa, että tekstissä on joitakin pieniä kielioppivirheitä, koska niitä on alkuperäisessä tekstissä.

silloin tuli äkkiä esiin ihmiskäsi ja se alkoi kirjoittaa lampun viereen kuninkaan palatsin kalkittuun seinään kuningas näki käden joka kirjoitti silloin hän kalpeni ja pelko täytti hänen mielensä hänen jäsenesä lamaantuivat ja hänen polvensa tutisivat kovalla äänellä huutaen kuningas käski tuoda eteensä loitsupapit kaldealaiset viisaat ja manaajat hän julisti babylonian viisaille joka pystyy lukemaan tämän ja esittämään sen tulkinnan minulle hänet puetaan purppuraan hän saa kultakäädyt kaulaansa ja pääsee arvossa kolmanneksi tässä valtakunnassa kaikki kuninkaan viisaat tulivat sisään mutta kukaan ei pystynyt lukemaan kirjoitusta eikä esittämään sen selitystä kuninkaalle silloin kuningas belsassar joutui kauhun valtaan ja hänen kasvonsa valahtivat valkeiksi myös hänen ylimyksensä järkyttyivät kuninkaan ja hänen ylimystensä puheen kuullessaan astui leskikuningatar pitosaliin hän sanoi ikuisesti eläköön kuningas älä antaudu pelon valtaan älä turhaan kalpene sinun valtakunnassasi on mies jossa asuu pyhien jumalien henki sinun isäsi aikana hänellä havaittiin olevan ymmärrystä älyä ja viisautta yhtä paljon kuin jumalilla isäsi kuningas nebukadnessar korotti hänet enteidenselittäjien loitsupappien kaldealaisten viisaiden ja manaajien päämieheksi niin teki isäsi kuningas danielissa jolle kuningas antoö nimen beltesassar asuu erityinen henki ja hänellä on taito ja viisaus selittää unia ja ratkaista arvoituksia ja ongalmia kutsuttakoon nyt hänet tänne hän osaa selittää tämän kirjoituksen

3. Seuraava englanninkielinen teksti on kryptattu käyttäen Hillin järjestelmää matriisilla

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

WWFMODFJDYTTEECUOEODJG. Pura kryptaus.

Ratkaisu. Merkitään tehtävän matriisia kirjaimella M. Nyt

$$M^{-1} = \begin{pmatrix} -2 & 3 \\ 3 & -4 \end{pmatrix}.$$

Jaetaan sana kahden mittaisiin osiin: $WW, FM, OD, FJ, DY, TT, EE, CU, OE, OD, JG$. Indeksoidaan kirjaimet siten, että $A = 0, B = 1, ..., Z = 25$. Nyt voidaan suorittaa dekryptaus:

$$M^{-1}\begin{pmatrix} 22 \\ 22 \end{pmatrix} = \begin{pmatrix} 22 \\ -22 \end{pmatrix} \equiv \begin{pmatrix} 22 \\ 4 \end{pmatrix} \pmod{26} = \begin{pmatrix} W \\ E \end{pmatrix}$$

$$M^{-1}\begin{pmatrix} 5 \\ 12 \end{pmatrix} = \begin{pmatrix} 26 \\ -33 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 19 \end{pmatrix} \pmod{26} = \begin{pmatrix} A \\ T \end{pmatrix}$$

$$M^{-1}\begin{pmatrix} 14 \\ 3 \end{pmatrix} = \begin{pmatrix} -19 \\ 30 \end{pmatrix} \equiv \begin{pmatrix} 7 \\ 4 \end{pmatrix} \pmod{26} = \begin{pmatrix} H \\ E \end{pmatrix}$$

$$M^{-1}\begin{pmatrix} 5 \\ 9 \end{pmatrix} = \begin{pmatrix} 17 \\ -21 \end{pmatrix} \equiv \begin{pmatrix} 17 \\ 5 \end{pmatrix} \pmod{26} = \begin{pmatrix} R \\ F \end{pmatrix}$$

$$M^{-1}\begin{pmatrix} 3 \\ 24 \end{pmatrix} = \begin{pmatrix} 66 \\ -87 \end{pmatrix} \equiv \begin{pmatrix} 14 \\ 17 \end{pmatrix} \pmod{26} = \begin{pmatrix} O \\ R \end{pmatrix}$$

$$M^{-1}\begin{pmatrix} 19 \\ 19 \end{pmatrix} = \begin{pmatrix} 19 \\ -19 \end{pmatrix} \equiv \begin{pmatrix} 19 \\ 7 \end{pmatrix} \pmod{26} = \begin{pmatrix} T \\ H \end{pmatrix}$$

$$M^{-1}\begin{pmatrix} 4 \\ 4 \end{pmatrix} = \begin{pmatrix} 4 \\ -4 \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 22 \end{pmatrix} \pmod{26} = \begin{pmatrix} E \\ W \end{pmatrix}$$

$$M^{-1}\begin{pmatrix} 2 \\ 20 \end{pmatrix} = \begin{pmatrix} 56 \\ -74 \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 4 \end{pmatrix} \pmod{26} = \begin{pmatrix} E \\ E \end{pmatrix}$$

$$M^{-1}\begin{pmatrix}14\\4\end{pmatrix} = \begin{pmatrix}-16\\26\end{pmatrix} \equiv \begin{pmatrix}10\\0\end{pmatrix} \pmod{26} = \begin{pmatrix}K\\A\end{pmatrix}$$

$$M^{-1}\begin{pmatrix}14\\3\end{pmatrix} = \begin{pmatrix}-19\\30\end{pmatrix} \equiv \begin{pmatrix}7\\4\end{pmatrix} \pmod{26} = \begin{pmatrix}H\\E\end{pmatrix}$$

$$M^{-1}\begin{pmatrix}9\\6\end{pmatrix} = \begin{pmatrix}0\\3\end{pmatrix} \equiv \begin{pmatrix}0\\3\end{pmatrix} \pmod{26} = \begin{pmatrix}A\\D\end{pmatrix}.$$

Siten kyseinen viesti on *WEATHER FOR THE WEEK AHEAD*.

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 $-8 \ldots -18$ astetta, huomenna pohjoisessa vähän alempi. Yölämpötila on pilvisyydestä riippuen $-10 \ldots -20$, paikoin -25 astetta. Heikkenevää pohjoisenpuoleista tuulta.

Ratkaisu. Tehtävän kannalta oleellinen Vigenére-taulu löytyy esimerkiksi osoitteesta:

http://user.it.uu.se/∼olgag/Cryptology/vigenere.html

Se, mitä avainsanan kirjainta mikäkin tekstin kirjain vastaa nähdään seuraavasti (tässä taulukon alku, idea lienee selvä):

M	A	A	N	I	T	O	S	A	S	S	A	V	E	R	R	A	T	T	A	I
L	U	M	I	S	A	D	E	L	U	M	I	S	A	D	E	L	U	M	I	S

Huomaa, että tässä kirjaimet Ä ja Ö ajatellaan erikoismerkkeinä, joita ei kryptata.

Nyt kryptaus luetaan Vigenére-taulusta. Ensimmäinen kirjain on rivin M ja sarakkeen L yhteinen alkion eli X. Toinen kirjain on rivin A ja sarakkeen U yhteinen alkion eli U, jne... Siten kryptattu viesti näyttää seuraavalta:

Xumv atärwlmei neuvlnfian smwpualä jd tlcwwan kitewws lxqtmmlwtwe. Xumv dänvmzmmaka vivä Japbolw-Aitrsnpelfxi ba Nethgcksd iycyuäcshiy jaclad nl uvwatweth emdkhäqaää. Fäyxölioe eähääz xäaväopä $-8 \ldots -18$ lmfmltd, lfiymfnd tzbvwashwdu häpäf aoixju. Gödämsöxtfm wf plpgcegqdhweä luqhpxiy $-10 \ldots -20$, jmqcolr -25 lmfmltd. Lpcwswnhzää aitrgiviyjgwdelweu fcmlwe.

Huomautus. Jos käyttää erilaista Vigenére-taulua, vaikka seuraavaa:

	A	B	C	D	E	...
A	B	C	D	E	F	...
B	C	D	E	F	G	...
C	D	E	F	G	H	...
D	E	F	G	H	I	...
E	F	G	H	I	J	...
⋮	⋮	⋮	⋮	⋮	⋮	...

niin päätyy hieman erilaiseen vastaukseen. Tällöin viesti alkaisi: Yvmw bsäsxmnfj...