Exercises Classical Cryptography 3a

crypto@os3.nl

Tuesday, February 21, 2023

(version 22.5, 2023/02/08 11:01:53 UTC)

Problem 1: **Simple columnar transpositions**

(a) Decrypt the completely filled

```
AOANS BUYTE NBIEB ELNDA REVBL DDEAL
```

Hints:

1. Grq'w eh diudlg li brx grq'w uhfrjqlvh wkh vwduw ri wkh whaw.
2. Wkh eorfn kdv ilyh urzv dqg vla froxpqv.

(b) Decrypt the incompletely filled

```
DMAIN TATLR EITVE SBJSS HEDKA ANMIN BEL
```

Hints:

1. Grq'w eh diudlg li wkh vwduw ri wkh whaw lv vwudqjh.
2. Brx vkrxog wub irxu froxpqv.
3. Wkh iluvw froxpq lv rqh orqjhu wkdq wkh rwkhuv.

(c) Decrypt the completely filled

```
PTIEO OGTBI NEYRA SICEY AYTRR DOISA FKFRL
NGVWE GITOC APIHO EILCT RLIOO EDIEH DNNIR
TNPNE NMEIS HTONR UFITR EIOGN RLDLG WGES
```

Hint: Wkh eorfn kdv rqob d ihz froxpqv.

(d) Decrypt the incompletely filled

```
FMGEO DFKOY AAOYL HIOIE ITUOY EFTBN UOLAN
RNTNH LIOAM HODDU WTGKD HLAON ULOAN IOSOE
TSIIT VGMON TUFNT NGOON FYEIA TESSY TITOW
```

Hints:

1. Brx vkrxog xvh vla froxpqv.
2. Wkh iluvw wkuhh froxpqv duh orqjhu wkdq wkh odvw wkuhh.

Problem 2: **Keyword columnar transpositions**

(a) Use the crib PEACH BASKET to decrypt

```
IDHTE NCLEX MECEH ACLHX AHPAO OAROA
NTABF HDEFB SSAKT POATL IUESR OSBRL
```

Hints:

1. Wkh srvlwlrqv ri wkh A'v duh yhub xvhixo.
2. Wkh nhbzrug ohqjwk lv vla.

(b) Use the crib AT CHRISTMAS to decrypt

```
RSRDI HILGS LDRGL GBHTS WLOTA
SIDAD SGGTA NDNHD ORSET ROIEH
ATUJT GIREB EENAA OTRUY LHATC
MEJDD NHORD HHIYD JMAAE ADSRT
TKYNI IWEEN CTGEI DOTCH EOEAI
MUYME NEEAA IITLO FEBEE GKH
```

Hints:

1. Brx qhhg wr xvh vla froxpqv.
2. Wkh froxpq ohqjwkv duh voooov.

Problem 3: **Kappa test**

(a) Implement the kappa test.

(b) Apply the kappa test to the exercises in Prac 4.6.

The following two problems from The Mathematics of Secrets book are optional.

Problem 4: **Vowels versus consonants**

(a) Write a little script to calculate the variance in the number of vowels with respect to the number of expected vowels as described in TMoS, paragraph 3.6.

(b) Check the calculations from the text (the hardcover first edition has errata).

Problem 5: **Anagramming**

(a) Complete the partial solution of TMoS, table 3.4, page 104.

(b) Complete the partial solution of TMoS, table 3.6, page 106.