Exercises Classical Cryptography 2a

crypto@os3.nl

Tuesday, February 14, 2023

(version 22.5, 2023/02/08 10:23:00 UTC)

Problem 1: **A simple substitution**

From TMoS, page 31. Use legacy encoding, if you want to compare with paragraph 1.5 in the book.

But modern encoding should work just as well.

(a) Make a script to count letters and make a table of frequencies

(b) Generate a frequency diagram, using a spreadsheet

(c) Make a script to calculate the Index of Coincidence

(d) Is it an additive cipher?

(e) Try to solve the cryptogram by assuming it is affine

Hints:

1. Lw lv qrw dq dgglwlyh flskhu.
2. Wkhuh lv dq reylrxv fkrlfh iru wkh hqfubswlrq ri wkh ohwwhu H.
3. Wkhuh duh wzr fdqglgdwhv iru wkh hqfubswlrq ri wkh ohwwhu W.
4. A ghfubswv wr H dqg T ru O ghfubswv wr W.

Problem 2: **A homophonic simple substitution**

From TMoS, page 36. Use legacy encoding, if you want to compare with paragraph 1.5 in the book.

But modern encoding should work just as well.

(a) Count symbols and make a table of frequencies.

(b) Generate frequency diagrams, using a spreadsheet.

(c) Calculate the Index of Coincidence for all symbols and for only the letters.

(d) Is it a monoalphabetic cipher?

(e) Identify homophones and solve the cryptogram.

Hints:

1. Rxwvlgh wkh vshfldo fkdudfwhuv lw lv d vlpsoh dgglwlyh flskhu.
2. Wkh vshfldo vbperov duh krprskrqhv iru wkh yrzhov.
3. Orrn dw brxu nhberdug iru d klqw.

Problem 3: **Solve a Porta with the help of a crib**

(a) Solve the Porta of Prac 4.1 by using the crib `COLLISION` and finding a matching pattern in the cryptogram corresponding to both halves of the alphabet. First read the introduction given in "Practicumboek Cryptografie".

Hints:

1. Uhdg wkh hasodqdwlrq lq wkh whaw ri wkh hahuflvh lq Sudf.
2. Wkh nhb skudvh lv hadfwob dv orqj dv wkh zrunlqj vfkhph vxjjhvwv.
3. Wkh nhb skudvh lv yhub lpsruwdqw iru wkh Xqlwhg Vwdwhv.

Problem 4: **Solve a Beaufort with the help of a crib**

(a) Solve the Beaufort of Prac 4.2 by trying the crib `AMMUNITION` in different offsets in the cryptogram.