TTM4135 Practical

1 Background

This assignment consists of practical experiments with historical ciphers. It is expected that you will use the CrypTool Online package (`https://www.cryptool.org/en/cto/`) to perform the experiments. In this document CTO stands for CrypTool Online. Although no other tools should be necessary, you are free to use any other software or to write your own. For Task 2.3 it can be helpful to make use of JCryptTool, the Java implementation of CrypTool (`https://www.cryptool.org/en/jct/`).

There are 8 marks available in total for this assignment with part marks as shown. Your answers should be submitted by the due date of **7 February 2022**. Your answers must be delivered through Blackboard in the answer fields provided. Each question also describes what you need to enter. Answers can be added and saved as you go along. This is an individual assignment. It is acceptable to discuss the general approach with other students but your answers should be your own.

You need to obtain your individual folder of four ciphertext files. The folders, as well as instructions on how to obtain them, are on Blackboard. The original plaintexts are all written in English from one or more novels written around 100 years ago. Each text is different and each is encrypted with a different classical cipher algorithm. The four algorithms used, in random order in your set, are:

- random simple substitution
- Vigenère
- transposition cipher (split into columns, permute columns, output by row)
- 2 x 2 Hill cipher

2 Questions

2.1 Vigenère analysis (2 marks)

Use the autocorrelation tool in CTO to find which ciphertext has a clear autocorrelation pattern and hence identify the Vigenère cipher in your set. Then use the Vigenère analysis tool in CTO to find the plaintext.

In the provided answers fields give the number (0, 1, 2 or 3) of your ciphertext, and the key (in the same format used in CTO).

2.2 Substitution analysis (2 marks)

Use the frequency analysis for 1-grams, 2-grams and 3-grams in CTO to identify the simple substitution cipher in your set. Find which ciphertext 3-gram corresponds to the letters THE (upper or lower case). The spaces and punctuation in the plaintext is preserved, which will help eliminate wrong guesses. There is no need to find a complete key or plaintext.

In the provided answers fields give the number (0, 1, 2 or 3) of your ciphertext, and your assumed encryption of THE.

2.3 Transposition analysis (2 marks)

Use the frequency analysis in CTO to identify the transposition cipher in your set. Given that the transposition block has 7 characters, find the plaintext. You can do this by hand or make use of the JCrypTool transposition analysis tool.

In the provided answers fields, give the number (0, 1, 2 or 3) of your ciphertext and the key (the column order, which is the same format used in JCrypTool).

2.4 Hill cipher analysis (2 marks)

Find the key for the remaining Hill cipher. This can be challenging. The following process is recommended.

1. Use CTO to determine the digram (letter pair) frequencies. Try to find the digrams which map to 'th' and to 'he'. These are probably two of the most common of your digrams. Because spaces in the plaintext are preserved in the ciphertext you can use the word structure of the original ciphertext to rule out most options. For example, 'th' will not occur on its own as a word and you are likely to see it at the start of some 3-letter words.

2. Once you have identified likely candidates for two digrams, test them by trying to solve for the key. (This is similar to the known-plaintext attack covered in Lecture 4.)

3. Once you have the key, CTO can help decrypt the whole ciphertext.

In the provided answers fields give the number (0, 1, 2 or 3) of your Hill ciphertext[1], and the key in the format used in CTO. **If you have not found the key** you can obtain credit for good guesses for the encryption of TH and HE; use the field provided to enter up to three plausible encryptions of TH and HE.

[1] There is no credit for identifying the Hill cipher since this is already decided once the other ciphertexts are identified.