1 Description

In this project, you will write a develop an application that can encrypt and decrypt texts using well known and simple encryption schemes from history.

2 Work plan

The work consists of the following units:

- √ Create a simple console application that allows to specify a text, an operation (decrypt or encrypt), a method (i.e., which encryption alogrithm to use), and an optional password as user-inputs.
- √ Implement the Cesar Cipher [1] as a first encryption algorithm to encrypt an decrypt your texts.
- √ Next, implement the Vigenère cipher [2] and make sure it can be used to encrypt and decrypt texts. This cipher algorithm should re-use the existing cesar cipher implementation.
- √ Add functionality that does not rely on text input on the console, but accepts a text file as an input instead and can encrypt, decrypt it by writing the output in another file.
- √ Add a function that counts the characters in a text and displays to you the number of occurence for every individual character in a text (i.e., the character histogram).
- ♢ Implement the Vernam cipher algorithm [3] to encrypt and decrypt your data.
- ♢ Implement a small GUI application with a text field and buttons to encrypt and decrypt text quickly with different cipher algorithms.

3 Scope

The project counts as completed if the system can be demonstrated implementing the functionality of all √-items. The ♢-items are optional items for extra points.

[1] https://en.wikipedia.org/wiki/Caesar_cipher
[2] https://en.wikipedia.org/wiki/Vigenère_cipher
[3] https://en.wikipedia.org/wiki/Gilbert_Vernam