DEPARTMENT OF COMPUTER SCIENCE CSI454 Information Security Administration Assignment #1

Out: 06/04/2021 Due: 20/04/2021 @9am

You are given a research paper that describes a new cryptographic algorithm – a Modified Hybrid Caesar Cipher and Vigenere Cipher.

Your task is to read the paper and implement the algorithm in Java (or Python), keeping in mind the following:

- What type of cryptographic algorithm is it?
- Implementation (with Java or Python) should be method based. There should be at least two methods: encrypting and decrypting methods each taking appropriate values. We expect that there will be more than two methods.
- There is no need for a graphical user interface. However, command line arguments should be used instead of asking the user for input!
- A proper class design and modularization goes a long way.

You will be given code to decrypt a week before submission of your assignment.

Deliverables (2 files).

- A **report** summarizing the research paper mainly a "nice" presentation of the cryptographic algorithms and a discussion of whether you agree or disagree with the paper's conclusions. The report should also discuss why the paper has such a short list of references.
- 2. The **source code** of the implementation not screen shots of the source code.