UNIVERSITY OF ONTARIO INSTITUTE OF TECHNOLOGY | FACULTY OF BUSINESS AND INFORMATION TECHNOLOGY

Final Project Description
Cryptography and Network Security (INFR 3600U)

Prepared by: Miguel V. Martin, PhD, PEng

Fall 2018

The final project is worth 40% of the final grade for this course. This project is to be prepared in groups.

Write a command line-based "Swiss Army cryptographic toolset for beginners" in Python. The program must have five cryptographic tasks implemented. These tasks can be anything covered in this course, from TripleDES to X.509 Certificates. Use cryptographic libraries; don't re-invent the wheel. The goal of this program is to provide a user-friendly interface for beginners allowing them to perform cryptographic tasks while educating them along the way. For example, suppose the program suggests the user to sign using RSA; after the program computes and displays the signature, it should also display some educational information about what just happened. After presenting such information the program asks the user if they would like to learn more about what happened behind the scenes; for example, the program would show the values of the RSA parameters (e.g., public values *n* and *e*) and their use for signing/verification.

Submit, by **November 7th**, a three (3) page user manual with screenshots, and add the source code as appendix; there is no page limit for the appendix.

Each group will present their program to the class between **November 8th and December 3rd**. It will be randomly determined right before the presentation how the five tasks will be split amongst the group members.