# Comp7402 Computer Systems Technology February 2019

## Cryptography and Cryptanalysis

## Assignment #3

**Due**: To be completed by February 14, 1700 hrs. This is an individual assignment.

**Task:**

- Your task is to design and implement a **one-time pad cipher using bit manipulation.**
- Your application will encrypt plaintext from a file specified by the user, and store the ciphertext in a file specified by the user.
- Alternatively, a user may select to read plain text from the keyboard and display the ciphertext only.
- Run the binary examples provided which illustrate the use of a one-time pad using a random key (otp), and a cipher that uses bit-manipulation to produce a string of completely unintelligible ciphertext (crypto).
- You will be combining these two techniques in your implementation.

- **Constraints:**
    - It is required that the key generation for encryption be random.
    - The bit-manipulation operator will be XOR.
    - You may use any language of your choice.
    - Your implementation should allow the user to specify whether the ciphertext will be read from a file or from the keyboard.
    - Your application must either prompt the user for the filenames, or specify them as command line arguments.
    - The ciphertext produced by your application must be completely unintelligible due to the bit-mangling process.

**To Be Submitted Electronically:**

- Submit a zip file containing all the code and documents as described below in the sharein folder for this course under "**Assignment #3**".
- Submit a complete, zipped package that includes your report, source code, and any supporting data (screenshots, etc), and references. Test results, complete with supporting data such as screen shots in **PDF format**.
- Hand in complete and well-documented design work and documents in PDF format.
- Also provide all your code **source code** and an **executable.**
- You are required to demo this assignment in the lab.

**Assignment #3 Evaluation:**

| | |
|---|---|
| Design: | 5 / 5 |
| Documentation (explanation, user guide, etc): | 5 / 5 |
| Test document and Supporting Data: | 10 / 10 |
| Functionality: | 30 / 30 |
| Total: | 50 / 50 |