

**ISEC2000 Fundamental Concepts of Cryptography  
& ISEC5002 Introduction to Cryptography  
Assignment 1, 2021  
@ Computing, Curtin University**

**Weighting:**

This assignment contains 3 questions, for a total of 100 points, which weights for 25% of the final mark.

**Submission:**

You should submit a **single ZIP** file to Blackboard. Name the file as <studentID>\_<name>\_assignment01.zip. It should contain the code, report, and text files. Use the Declaration\_of\_originality.pdf as the cover page of your report. The due date is **18 April 2021 11:59 PM**.

**Academic Integrity:**

This is an **individual** assignment so that any form of collaboration is not permitted. This is an **open-book** assignment so that you are allowed to use external materials, but make sure you properly **cite the references**. It is your responsibility to understand Curtin's Academic Misconduct Rules, for example, post assessment questions online and ask for answers is considered as contract cheating and not permitted.

## Attack a cipher

1. Please download the file *cipher.txt* and try to decrypt it, assuming the plaintext is plain English that makes sense. You need to do the following.
  - (a) (10 points) Write a program (C/C++, Java, Python) to perform the letter frequency analysis attack.
  - (b) (10 points) Write a program (C/C++, Java, Python) to perform the brute-force attack (exhaustive key search), assuming that you know it is encrypted by Affine Cipher. (Hint: apply decryption of Affine Cipher to the file and find the key that gives you intelligible decrypted text)
  - (c) (10 points) Write a report to state
    - What you have done in your code step-by-step
    - The substitution table obtained by letter frequency analysis
    - The key found by brute-force attack

## Implement DES

2. (30 points) Please implement the Data Encryption Standard (DES) algorithm (C/C++, Java, Python). The requirements are as follows:
  - Implement each component as a separate function, such as key schedule, permutation, SBox, f function, encryption, decryption.
  - Ask the user to input the key of any length, which means you need to do padding or chopping if necessary. Think about your padding strategy.
  - Implement both encryption and decryption of DES. Encryption takes a txt file as input and output another txt file containing ciphertext (use hexadecimal for easy readability). Decryption should recover the plaintext.
  - your code should encrypt and decrypt standard keyboard characters, including letters, numbers, and symbols.
  - Use the provided file DES-test.txt to test your code.

After implementing your code, please **answer the following questions** in your report:

- (a) (10 points) What are the lessons you learned, and difficulties you met, in the process of implementing DES?
- (b) (10 points) (**ISEC2000**) What will happen if the key is initialised as all 0-bits? (**ISEC5002**) Which operations are confusion, which operations are diffusion, in DES? Explain your reasoning. (answer one of them based on your enrollment)

## Lab demo

- 3. (20 points) After the assignment due, you will perform a brief demonstration of your code, during the practical sessions. Each of you will be given around 5 minutes, so make sure your code is working and it is consistent with your submission.