Track B
INFA723 Homework 2

The homework assignment will be graded based on the following criteria:

- Accuracy: 1) the solution meets specific requirements in the problem description; 2) the solution produces correct results; 2) the procedures adopted in the solution are technically sound.
- Efficiency: efficiency will be one of the criteria when grading programing assignment. The solution should produce the desired results efficiently.
- Effort/neatness: the solution includes excellent effort, and all relate work is shown neatly and organized well.

Homework assignment feedback will be available through the DropBox folder on D2L.

Note: For all the programming assignments, you can choose any operating systems to develop your code. A README.txt is required to submit any programming assignments. In the README.txt, you need to provide the following information:

1) How to compile your program?
2) How to run your program?
3) What is the output and the results when I run your program?
4) Any descriptions which can help me understand, compile, run, and verify your answers. (FYI: I check every programming assignment turned in!)

Zip all you source code, project files, supporting files, and README.txt and submit the all-in-one zip file together to the D2L Dropbox.

(50 points) 1. Three binary files are provided in this exercise, q1-file1, q2-file2, and q3-file3. There three files include a firmware image, an encrypted file, and a compressed file.

a) (20 points) Write a program to classify if a file is encrypted or not.
b) (10 points) Explain what you use in the code to determine if a file is encrypted.
c) (10 points) Identify each file's category including firmware image, encrypted file, and compressed file.
d) (10 points) If you can identify the compressed file, are you able to identify which algorithm is used to compress the file and un-compress the file.

(50 points) 2. Cipher.txt is an encrypted file. The cipher.txt is created using AES algorithm. The key size is 192. The mode of operations is CBC. The key and initial vector are listed as below:

key=0294E7143C2DF135DAEFE9D74DF8BDCC488EDBA8FE5239A8

iv =F3BC6E5B281EBF67210CD68837FFDE9A

a) Write a program to decrypt the cipher.txt.
b) Submit a copy of the plaintext you decrypt.