# CE4024 Assignment 2 – Group 12

## Group Members

1. Tay Jin Heng
2. Kenny Seet
3. Yeoh Keng Wei U1120646A

## Techniques Used

There are three stages in our program. The first stage is the Load Phase which runs sequentially. After the Load Phase, the Password Transform Phase and the Password Validation Phase runs concurrently.

Password Transform Phase takes inputs from the words in dict.txt and outputs a new transformed word, which will be used as input for the Password Validation Phase. The transformation pattern found in passwords of hash.txt is as follows:

1. No transformation
2. Leetspeak substitution
   * ‘i’ substituted by ‘1’
   * ‘e’ – ‘3’
   * ‘a’ – ‘4’
   * ‘s’ – ‘5’
   * ‘t’ – ‘7’
   * ‘o’ – ‘0’
3. 1 or 2-digit prefix and suffix
4. 2-word combinations
5. 1-digit suffix and word combination.

During the Load Phase, all capital letters were transformed to lower case and all words which contained symbols, eg. $,#,@ etc, were omitted, due to the passwords made up of only lower case letters and digits as stated in the specifications. These words then go through the above transform and their output are inserted into 5 separate queues. These queues serve as inputs to the Password Validation Phase.

In the Password Validation Phase, 4 threads (or more depending on the available CPU processors, 4 being the minimum as 4-core CPU will be used stated in the specifications) will be spawned to consume input from the queues. Each thread will be assigned their own input queue. When the threads finished processing their own input queue, they will “help” the other threads by processing their input queues in the same order as above.

In each thread, the salt of each uncracked password hash are used with each word to generate the MD5 hash. The MD5 hash is then compared with the uncracked password hash. If they are not the same string, the process is continued with the same word and another uncracked password hash. If they are the same, the username and password are printed out and the corresponding hash is removed from the uncracked password hash list. This process is continued with all the words generated by the Password Transformation Phase. Eventually, the program stops when all the hashes are cracked or if there are no more inputs.