Comp 7402 Computer Systems Technology January 2019

Cryptography and Cryptanalysis

Assignment #2

Due: To be completed by February 7, 1700 hrs.

Task:

- You have been provided with code examples for the Transposition cipher, together with a language detection module, and a dictionary. You are allowed to use those in this assignment.
- Your main task now is to design and implement an application that will make use of those modules to break a transposition cipher.
- The basic design will a brute force attack that will attempt every possible key length in the range [1..length (ciphertext)].
- For each attempted key length your application will match the results against dictionary words to find a match. If there is no match, the algorithm will move to the next key length and so on until it reaches the maximum key length.
- If a match is found the algorithm will stopped by a user intervention. This means that your algorithm will pause after a word match, display the plaintext found, and prompt the user to either continue the attack using "Enter" or stop the attack (meaning it is the correct key) with a key such as "y" for "yes".

- **Constraints:**
  - 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.

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 #2**".
- Submit a complete, zipped package that includes your report, tools that you used, and any supporting data (dumps, 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 **source code** and an **executable.**
- You are required to demo this assignment in the lab.

Assignment #2 Evaluation:

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