Comp 7402 Computer Systems Technology February 2019

Cryptography and Cryptanalysis

Assignment #4

Due: To be completed by March 7, 1700 hrs. You may work in groups of two.

Task:

- Your task is to design and implement an 8-round Feistel Cipher.
- 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.

- **Constraints:**

  - Your implementation must have encryption and decryption functionality.
  - For this assignment you will use the same key for all rounds.
  - The default cryptographic mode will be ECB.
  - 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.
  - Analyze the Diffusion and Confusion characteristics of your cipher. Comment on how these could be improved.

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 #4**".
- 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:	15 / 15
Analysis (Diffusion and Confusion):	5 / 5
Functionality:	40 / 40
Total:	70 / 70