COMP 7402 Assignment 4 Report

Peyman / Dimitry

Goal

For this assignment our goal was to create a simple Feistel cipher with 8 rounds.

Design

This application was written in Python 3 and works from the command line. It takes blocks of 64 bits from the input and cycles them through 8 rounds of encryption.

Analysis

It was noted that for the same key the code generates the same exact ciphertext each time. While it is better than a Caesar cipher due to an increase in diffusion (larger cipherspace). The confusion is not as high as it could be because of many factors. Firstly, the key never changes and secondly we are not doing a lot with the data since I used the f(x,i) function from the lab experiment.

Pseudocode

```
main()
        Read Inputs
        Load Data
        Format Inputs into 64 bit blocks
        For each 64 bit block {
                For each round of encryption {
                        Split into left and right sections
                        For each bit {
                                Set left bit as Xor of f(right bit)
                        }
                Yield Right and Left blocks
        }
        Output encrypted Data
```

Usage

Encrypting

1. Type ./feistel.py -e <filename>
2. Program will output the desired text.

Decrypting

1. Type ./feistel.py -d <filename>
2. Program will output decrypted text