Andrew Dopson

Login ID : adopson

WVU ID : 701017103

Programming Assignment 1

09/22/2014

Program Status

This program fully compiles.

The only aspect that I do not believe works correctly is the decryption algorithm. It still produces an output, but I do not believe that the output is correct.

Documentation

This program was written in Java using Eclipse IDE. Java universal libraries that were used are as follows:

java.util.ArrayList

java.util.Scanner

java.io.BufferedReader

java.io.File

java.io.FileNotFoundException

java.io.FileReader

java.io.IOException

This program is used to perform DES encryption on a text given by the user. It starts out by prompting the user for a file to read from, which contains text. The user is then prompted to input an 8 digit password containing only letters and numbers. The key is then converted to a binary string representation.

Once the key has been established, the program then creates the key schedule, which contains 16 sub-keys, which will be used for 16 different instances of the DES algorithm, which is explained later.

Once the key schedule has been created, then the data is separated into 64 bit blocks. Each of these blocks are run through the DES algorithm one by one.

The DES algorithm first runs the 64-bit text through an initial permutation. Then program splits the 64-bit block into two parts, Left and Right, each containing 32 bits. After the initial permutation, the DES algorithm performs a series of instructions that are repeated 16 times, each with its respective key (first cycle uses key1, second cycle uses key2, etc.). These instructions consist of the following:

* Next Left block is represented by current Right block.
* Right block is then run through a permutation to create a 48 bit block.
* Modulo 2 addition of new Right block and respective Key
* S-box substitution is then used to convert the 48 bit block back to 32 bits. This is done by taking 6 bit sections of the 48 bit block. Each section uses the first and last bit of that section to represent a 2 bit binary number for the row number and the middle 4 bits as a binary representation of the column number of S. The 4 bit value at that location in S then represents a 4 bit string that will be part of the new 32 bit block.
* New right block is then permuted with a 32 bit permutation table.
* Modulo 2 addition is then performed on the Left block with the resulting Right block.
* The next right block is represented by the above instruction.

This is completed 16 times for each key. Then the result is run through an inverse permutation. The DES algorithm is then run again for each 64 bit text block.