Muhammad Ansari

COMP 424 Computer Security

March 6th, 2018

Project #2

**Design:**

The program is a C++ executable which asks the user for an integer number and a string that denote the number of rounds to run the Feistel Cipher and the plaintext input for the encryption process respectively. The input string is split into the ‘leftSplice’ and ‘rightSplice’ string variables. The initial key for the cipher is arbitrarily specified as 10 and is incremented and decremented in the encryption and decryption rounds respectively in the ‘subKey’ variable. Two ‘for’ loops are then used for the encryption and decryption processes respectively, with outputs shown accordingly. The loops both iterate for the number of rounds specified during input, and provide the output of each round at every iteration. In each iteration, the ‘roundFunction’ method is called and operates on the rightSplice string and the current subKey. The output of this function is then XOR’d with the leftSplice, and then a basic swap algorithm swaps the rightSplice as the leftSplice and vice versa to be utilized in the next iteration of the loop.

I chose C++ as the language for writing this program out of convenience and because C++ is a part of the C–family of languages. These languages allow for direct manipulation of the computer’s memory with the use of an allocation function, and also through the use of pointers. These features allow the programmer to have better control over the data in memory utilized by the program, and not allow outside interference. This is useful when implementing encryption and decryption algorithms.

**Code:**

#include <iostream>

**using** **namespace** std;

**int** roundFunction(**int** key, string rightSplice){

**int** result = 0;

**for**(**int** i = 0; i < rightSplice.length(); i++)

result += rightSplice[i];

result / key;

**return** result;

}

**int** main(){

**int** numOfIterations;

**int** initialKey = 10;

**int** subKey = initialKey;

string input;

string leftSplice = "";

string rightSplice = "";

string temp;

cout << "Enter number of rounds to run the Feistel Cipher: ";

cin >> numOfIterations;

cout << "\nEnter string to be encrypted: ";

cin >> input;

**int** i = 0;

**for**(i; i < input.length()/2; i++)

leftSplice += input[i];

**for**(i; i < input.length(); i++)

rightSplice += input[i];

**for**(**int** i = 0; i < numOfIterations; i++){

**int** functionResult = roundFunction(subKey, rightSplice);

**for**(**int** j = 0; j < leftSplice.length(); j++)

leftSplice[j] = leftSplice[j] ^ functionResult;

temp = rightSplice;

rightSplice = leftSplice;

leftSplice = temp;

**if**(i != numOfIterations - 1)

subKey++;

cout << "\nEncryption Round " << i + 1 << " Output:\t" << "Left: " << leftSplice << "\t" << "Right: " << rightSplice << "\n";

}

temp = rightSplice;

rightSplice = leftSplice;

leftSplice = temp;

cout << "\nEncryption Final Output: " << leftSplice + rightSplice << "\n";

**for**(**int** i = 0; i < numOfIterations; i++){

**int** functionResult = roundFunction(subKey, rightSplice);

**for**(**int** j = 0; j < leftSplice.length(); j++)

leftSplice[j] = leftSplice[j] ^ functionResult;

temp = rightSplice;

rightSplice = leftSplice;

leftSplice = temp;

subKey--;

cout << "\nDecryption Round " << i + 1 << " Output:\t" << "Left: " << leftSplice << "\t" << "Right: " << rightSplice << "\n";

}

temp = rightSplice;

rightSplice = leftSplice;

leftSplice = temp;

cout << "\nDecryption Final Output: " << leftSplice + rightSplice << "\n";

**return** 0;

}

**Output Examples:**



