CSE 436 Computer and Networks Security

Assignment II – Data Encryption Standard

The objective of the following assignment is to implement a fully working DES algorithm that can encrypt or decrypt the given input. The DES cipher includes many stages and modules to implement, although none of them is difficult. As assistance, I am going to list the main concepts you need implemented to have a working DES cipher:

- Permutation Box – you need to implement how a permutation box works given a specific input and calculate the output whether it's 64-bit to 64-bit box or when the output is of different size than the input.
- S-Box – you need to implement how the S-box works; take an input of 6 bits, and output only 4 bits using the concept of S-Boxes as you will later do it with 8 S-Boxes and a 48-bit input in the DES cipher.
- Key Generator – you now need to implement the generator that takes a 64-bit key input, and outputs 16 keys whose size is 48-bit each.
- DES Function – finally, you will implement the DES function itself where the magic happens. Later, you will implement the 16-round functionality.
- After finishing your DES encryption algorithm, tweak it so that it does decryption instead of encryption. *Hint: Look at the key!*

• Implementation Notes

- You are free to use any programming language you prefer, but I recommend sticking to the same language in every assignment so in the end you will have a complete library of your own making that includes the encryption techniques you study.
- The input consists of 3 lines:
  The first line consists of 16 Hex characters which represent the key. The second line consists of 16 Hex characters which represent the plaintext. The third line consists of a single number which represents the number of times you should run the encryption.
- The output should consist of a single line that has 16 Hex characters and represents the ciphertext.

- Create an executable ".exe" file for your program in which you can input a plaintext, specify the, and run the program to print out the ciphertext output of the DES cipher.

Example

Input:
0000000000000000
FFFFFFFFFFFFFFFF
1
Output:
355550B2150E2451

Input:
0000000000000000
FFFFFFFFFFFFFFFF
2
Output:
FFFFFFFFFFFFFFFF

- ## Submission Details

  - You are required to submit your code files (not entire projects) along with the executable.
  - Write a one-page report about the design and documentation of your implementation.
  - Group all files including the code and executable into one folder and compress it.
  - Rename the compressed file to **"CSE436_Assignment2_StudentID.rar"** format, and submit it to google classroom.
  - Please adhere strictly to the above instructions as they will significantly facilitate marking your answers.