**Name:** Faizan Safdar Ali
**Roll No:** 2017-10-0152
**Assignment:** 1

## Part 1: Primer to OpenSSL library:

This part is already complete and has been marked. The solution is in the assignment1Answers.pdf file.

## Part 2: Using OpenSSL in our programs:

### a. Task 1: One-Way Property vs. Collision-Free Property:

You can run the files named collision.c and one-way.c to check the main code is implemented in these files. the descriptive answer is in assignment1Answers.pdf.

### b. Task 2: Programming using the Crypto Library:

You can run the file named crypto.c to check the main code is implemented in that files. the descriptive answer is in assignment1Answers.pdf. I am also submitting the compiled part named 'enc'. The process to run this file is "./enc plain.txt words.txt".

## Part 3: Secure Email System using PKI (Design Problem):

The whole methode and the description is written in the file question3.pdf.

## Part 4: Decrypt Vignere Cipher:

You can run the file named vigenere.cpp to check the main code is implemented in that files. the descriptive answer is in assignment1Answers.pdf. This first display possible keys and then ask to pick one and then shows the required result.