**Assignment #6: RSA Encryption and Decryption DUE: April 25, 2020**

**\*\*NOTE: THIS IS THE FINAL ASSIGNMENT AND THERE IS NO LATE DEADLINE FOR THIS ASSIGNMENT, SO SUMBIT NO LATER THAN THE 25TH OF APRIL. ALSO YOU MAY DROP THE LOWEST ASSIGNMENT.\*\***

In this assignment you will be using the RSA cryptosystem to encrypt and decrypt messages. This is a programming assignment that will prompt user to enter the prime values of “p” and “q” and then calculate the modulus “n”, “e”, and “d” values. It will then take the user message and convert each of the values to its ASCII representation in decimal format. Once converted the values will be encrypted based on the equation for encryption in RSA: Me mod n. Once encrypted the ciphertext will be decrypted with the following equation for decryption in RSA: Cd mod n. You should then add a function/if-else statement that checks whether or not the decrypted message matches the user’s input message. This assignment can be done in any language, but must be done from scratch, no RSA libraries are permitted.

Deliverables:

* 1 paragraph summary of what you did and how you did it.
* Source code uploaded to the drobox separately (if you are having issues with uploading src code, copy src code into text file and upload that)
* Screenshots of the following cases:
  + p = 199, q = 197, message = “Last One”
  + p = 23, q = 11, message = “Finally”

Your screenshot should have the values of p, q, e, n, d, original message in decimal, ciphertext in decimal, and decrypted message in decimal.

Sample Output:

