MATH 1P40 Winter 2020
Assignment #2
Due: Monday March 2 by 4:00 pm

Your mission is to design an "ENIGMA" program that will make it quick and easy for spies to encode and decode messages on the run, according to the RSA method. Your program should have a very friendly interface that is COMPLETELY self explanatory. Your RSA project will be graded as follows:

I - Your RSA program (90%)

Part A) 40%

Mode 1) The interface allows the user to enter n, e and a number to be encoded and on a button click displays the encoded number.

Mode 2) The interface allows the user to enter n, d and a number to be decoded and on a button click displays the decoded number.

Part B) 20%
Every time the user clicks a button, the program randomly generates two new primes with 3 digits each and displays the two primes and the corresponding values of n, e and d.

Part C) 10%
The program has an original extra feature of your own choosing. The interface will have a button saying "Extra Feature". When that button is clicked a message box comes up describing the extra feature of your program (i.e. tell your marker what to look for in your message).

Interface 10%: The interface is extremely "spy friendly", self-explanatory and attractive.

Programming style 10%: The program has good programming style. It uses comments, functions and sub procedures, and it is efficient.

II - Your (hand-written or typed) Report 10%
Your written document will consist of three parts under the following headings:

1. INTRODUCTION. Write a short paragraph about what RSA and your project are about. If you use resources (internet, book, article, etc.), give the reference(s) — up to 10 lines
2. DESCRIPTION OF RSA METHOD USING AN EXAMPLE. First use your program to generate an example with your first name (i.e., encode/decode your first name). Then briefly describe all steps of the RSA method by using your first name as an example of message to encode and decode (use specific values of n, p, q, e, and d) – show steps only for one number group of your first name, and show results for the rest of your name
3. DISCUSSION. Briefly discuss the safety and current use in our life of this encryption method; if you use resources, give the reference(s) — up to half a page