**Programing Assignment 4**

**Problem Submission Rules:**

1. **Detection of plagiarism will result in Failing grade. Students must do this assignment by themselves.**
2. **After completion, your work must be submitted to an assignment folder in D2L by a corresponding deadline.**

**Problems:**

The aim of this assignment is to implement the RSA algorithm. Specifically, the implementation should include the following functions:

The key generation function takes as input two prime numbers and outputs a public/private key pair. Let’s assume that the prime numbers are between . You can store them in an array and pick two distinct one randomly.

**2.**   
The encryption function (note that RSA uses the same function for both encryption and decryption) takes as input a plaintext and a public key then outputs a ciphertext. Also, it takes as input a ciphertext and a private key then outputs a plaintext.

Hint: To find a multiplicative inverse, you may use a brute-force strategy.

Note: For all other requirements and specifications not defined here, please refer to them in the textbook.

**3. Combining with Assignment 1**Improve your implementation for 1 by using your Text Converter, so it can handle a string from a user and output a string.

Hint: you can execute the RSA function once for each letter, i.e., the plaintext “hello” needs five executions. For example, the input “hello” will be encrypted as follows:

(a) “hello” is converted to a list of characters: [‘h’,’e’,’l’,’l’,’o’]

(b) the list of characters is converted to a list of decimals as per ASCII code: [104, 101, 108, 108, 111]

(c) each decimal in the list is encrypted by the “RSA” function implemented for 2.

**Complier requirement:**

The code must be implemented using Python version 3.9.x or higher. Students must use Python official libraries that are accessible from the webpage (<https://docs.python.org/3/library/index.html>). All used libraries and their purpose should be described in the report.

**Submission instructions:**

Please submit your deliverables to D2L Assignments folder: PA 4. You need to submit 4 different things:

1. Your Python code saved as yourlastname.py
2. Your Python code saved as yourlastname.txt - copy and paste your entire Python code, save
3. Your report yourlastname\_Report\_PA3.doc as a word document
4. A short video demo: (3-5 minutes)
   1. Explaining your code
   2. Use your first and last name as an input strings
      1. Show the prime number your code has chosen and the calculated private and public keys.
      2. Show the encrypted output strings.
      3. Show the decrypted string back to orginal
   3. Do b for a sentence of your choice.

Once you submit, D2L will perform similarity check for your submission and show you the result. Your similarity score must be lower than 30% unless something essential is described in the report. Otherwise, (the score -50%) will be deducted.

**Project Report:**

The report does not have any specific format. Three things you must include:

1. What you did for the project, i.e., explain the project with your own word.
2. Explain your program/code.
3. Explain output, include screen shot.

You could add anything else you like.