MAT 331-Fall 20: Project 1

In this project, you can use any code from the previous homeworks.

You are **NOT allowed** to use the functions pow, **sqrt**, or any external library except the string library.

You are allowed to use any previous homework code, as long as it does not break the above rule.

For each exercice, each student has to decrypt a unique file. Take your student id, the caesar encrypted files are "**caesar_encrypted_(your id).txt**" where "(your id)" is replaced by your student id number.

For example if my student id is "123456", then the associated filenames are:
caesar_encrypted_123456.txt,
vigenere_encrypted_123456.txt
rsa_encrypted_123456.txt

Exercice 1. *(Caesar cryptography) The file* ***"caesar_encrypted_(your id).txt"*** *has been encrypted using a Caesar cypher (Hint: the first line of the real message contains the word "the").*

1. *Write a program that decrypts it (using a python code) and creates a file with the decrypted message inside "caesar_decrypted_(your id).txt".*

2. *(Math part) Explain your algorithm and describe its complexity.*

Exercice 2. *(Vigenère cryptography) Alice has a message written in English, with only lowercase letters, breaklines and spaces.*

She encrypts her message in the file ***"vigenere_encrypted_(your id).txt"*** *by replacing the letters using a Vigenère cypher with 2 characters and transfers it to Bob. You intercept her file and want to decypher her message.*

For example, if her message was :
*"**abcd\nefghi**" and her key is "ab", then the encrypted file would contain "acdd\n ffhhj"*

1. *Write a program that decrypts it (using a python code) and creates a file with the decrypted message inside "vigenere_decrypted_(your id).txt".*

2. *(Math part) Explain your algorithm and describe its complexity.*

In the following exercice, you can use the functions *str.strip*(), the function *chr*(), and the function *ord*().

Exercice 3. *(RSA) Alice and Bob communicate using a RSA cypher. We denote by* (e, n) *the public key,* (d, n) *the private key only known to Bob. Message has an original message containing 5830 characters. To send the encrypted message to Bob, she proceeds as follows:*

Step 1 She creates a file called ***"rsa_encrypted_(your id).txt"****.*

Step 2 *She writes in this file "exponent = " and puts her encryption exponent and breaks a line.*

Step 3 *She then writes "integer n = " and writes the value of n and breaks a line.*

Step 4 *She converts her message into a sequence of numbers with three digits using the ASCII convention, for example the text with 15 characters "This is a test" would be converted to the list of numbers*

$$[084, 104, 105, 115, 032, 105, 115, 032, 097, 032, 116, 101, 115, 116, 046]. \quad (1)$$

Step 5 *She then regroups all the numbers 5 by 5. For example, for the above sentence "This is a test" she would then get the list:*

$$[84104105115032, 105115032097032, 116101115116046] \quad (2)$$

Step 6 *She encrypts each of these numbers using the RSA method by raising each of these integers at the power e modulo n. She obtains a list of numbers and writes them in the file separating each one by a comma.*

You intercept her message. Your goal is to decrypt her message.

1) Write a program that decrypts her message and write the decrypted message inside a file called "rsa_ decrypted_ (your id).txt".

2) (Math part) Explain your algorithm and describe its complexity.