CS/MATH111 EXTRA CREDIT ASSIGNMENT

For this assignment, you need to implement the RSA public-key cryptosystem in C++.

Input:

a) A public key (e, n) (you need to check whether the input is valid);

b) Choice of encryption or decryption (”e” for encryption and ”d” for decryption);

Additional input for encryption:

c1) English text (in a text file). You can use well known quotes.

Additional input for decryption:

c2) Cipher text (in a text file).
Note: in this part, you need to break RSA (follow your homework 2 (problem 2) instructions).

Output:

For encryption: cipher text (written into a text file).

For decryption: decoded message (written into a text file).

You can reuse the character - integer encoding schema from your Homework 2 (A is 2, B is 3, ..., Z is 27, and blank is 28) and append it with other characters if needed.

Example of input for encryption:
5 77 e message.txt,
where message.txt is a text file with a message to be incrypted.

Your output should be: ”incrypted.txt”, where incrypted.txt is the name of the file with the encrypted text; the text should look somewhat like: 12 34 56 21.

Example of input for decryption:
5 77 d ciphertext.txt,
where ciphertext.txt is a text file with a ciphertext to be decrypted.

Your output should be: p = 7, q = 11, ”decrypted.txt”
where decrypted.txt is the name of the file with the decrypted text.

Submission/Demo Instructions. The project is due Saturday, February 8, 11:50pm (on Gradescope).