King Fahd University of Petroleum & Minerals
Information and Computer Science Department

ICS 254: Discrete Structures II
Project
(Due: Saturday 11 December 2021 at midnight)

You will implement the RSA technique in Java using the `long` integer data type, with values that range between -9,223,372,036,854,775,808 and 9,223,372,036,854,775,807. You will implement both, the encryption and the decryption according to the following requirements.

Question 1 [50 points] Encryption Implementation

1) Your alphabet includes the

   a) 52 letters (capital letters and small letters),

   b) 10 digits (0..9),

   c) Punctuation marks: period **.** , question mark **?** , exclamation point **!** , comma **,** , semicolon **;** , colon **:** , hyphen **-**, parentheses **(** , **)** , brackets **[** , **]** , braces **{** , **}** , apostrophe **'** , quotation marks **"** , the space and the new line characters, ordered as *A..Z*a..z0..9<.><?><!><,><;><:><-><(>,<)>,<[>,<]><{><}><'><">< *space* ><*NewLine*>.

2) Your input is read from a text file with file extension "*.txt*", containing the following data:

   (a) The first line contains the public key values e and n, separated by a white space. n should not exceed 9,223,372,036,854,775,807.

   (b) The second line, onward, contains the text that needs to be encrypted.

3) You may assume that the text file will contain characters coming only from the alphabet mentioned in Part 1.

4) The output file should contain the encrypted message only. The file extension of the output file should be "*.rsa*", with the same filename as that of the input "*.txt*" file.

5) Note that you need to determine the block size dynamically, based on the value of n.

Question 2 [40 points] Decryption Implementation

1. Based on your encryption implementation, develop a decryption method that takes as input an encrypted file with "*.rsa*" extension and asks the user to input the private key values, d and n.

2. The file extension of the output file should be "*.dec*". The filename should be exactly the same as that of the decrypted file.

Question 3 [10 points] README file

Include a *README* file that explains the following:

1. Clear instructions on how to compile and run your code.

Question 4 [50 points] BONUS

After the deadline of the submission of the assignment, two encrypted files *p1.rsa* and *p2.rsa* will be posted on blackboard. You need to submit the following for this part:

1. (**15 points**) The first correctly decrypted file, *p1.dec,* with the first line containing the decryption key value d. The value of n used to encrypt the text file is 797527.
2. (**15 points**) The second correctly decrypted file, *p2.dec,* with the first line containing the decryption key values d and n. The value of n consists of 4 digits.
3. (**10 points**) Explanation of the strategy and/or algorithms used to decrypt the file *p1.rsa*.
4. (**10 points**) Explanation of the strategy and/or algorithms used to decrypt the file *p2.rsa*.

IMPORTANT NOTES REGARDING THIS ASSIGNMENT

1. This assignment will be done in groups of 2 students.
2. Your first submission must be a zip file containing all the programs and the README file. You may also submit a sample input document that can be used to encrypt and then decrypt.
3. Your second submission must be a zip file containing all the programs used for decryption, the README file containing explanation of the strategies and/or algorithms used in the successful decryption, and the decrypted file(s). Note that another assignment for the bonus will be used to submit it. Also, note that I will interview all teams who submit the bonus.