Lab 2: Cryptology

Deadline: Friday 23/9 17:00

This lab can be done by at most two persons

To be approved on this lab, you must demonstrate your program during a lab session before the deadline expires, or book a time with Pierangelo.

RSA implementation in Java

Write an implementation of the RSA algorithm in java.

Your program must have the following functionalities. It must be able to

- generate public and private keys.
- encrypt a plain text message given one key.
- decrypt the ciphertext message given the other key.

Your program must be commented in a clear and informative way.

Tip: Have a look at the Java class BigInteger in the package java.math at http://docs.oracle.com/javase/8/docs/api/