Lab 3

RSA is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large integers. A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message.

In this Lab, you are required to write a program in C++/ JAVA(any programming language) to implement the RSA algorithm.

Requirements:

1) Generate two large random numbers
2) Test if the number generated is prime number
3) Implement RSA Algorithm to generate public and private key
4) Use keys generated from RSA to Encrypt and Decrypted files and messages