**EC7020: COMPUTER AND NETWORK SECURITY**

**LABORATORY EXPERIMENT: 06**

**CRYPTOGRAPHY**

Reg No: 22/11/2022, from 13:00 to 16:00

**AIM**: Students will learn the fundamental principles of computer and network security by studying cryptographic techniques and their usage in computer and network systems.

**OBJECTIVES:**

* To understand asymmetric key encryption techniques.

**Following are the tasks for this lab session.**

1. You have to write about the BigInteger and BigDecimal classes of java. (5 Marks)
2. Identify the purpose for the implementation of these methods. (5 Marks)
3. RSA Encryption.
   1. Write Down the importance of selecting large prime numbers. (By using an example) (5 Marks)
   2. Drawback of choosing large prime numbers. (5 Marks)
   3. Implement RSA algorithm in Java using Big Integer Class with 1024 or 2048bit kit. (Comment your code)

(50 Marks)

* 1. Encrypt the following text using RSA and Decrypt it to plaintext. (20 marks)

“If you think cryptography will solve your problem, either you don’t understand cryptography, or you don’t understand your problem.”

**Discussion** (Write the analysis of this lab experiment) (5 Marks)

**Conclusion** (Include the concise summary of those which have already been presented in the report) (5 Marks)

**(5 Marks - Own work, Report Structure and Content)**

**This is individual work. Write your answers in this Lab Instruction sheet with the file name EC7020\_L1\_YourRegNo. Submit it as a pdf document, archive all files, and upload them to the teams. The same name conversion applies to the Zip.**