Lab 2: RSA Encryption

Kelli Ruddy and Daniel Williamson

February 2, 2016

Section 01

1. Problem Statement

For this lab we were asked to encrypt then decrypt a given number. After figuring out that the given numbers were working correctly, we used the probable prime method to create random prime numbers and then worked with those.

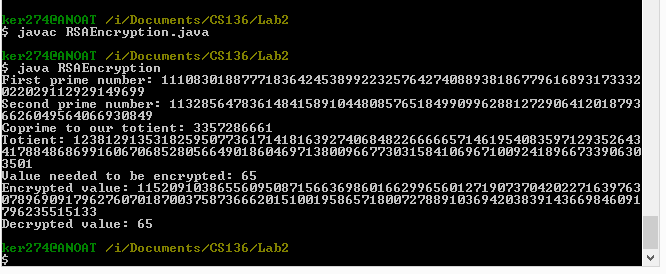
Features Used:

* BigInteger
* Probable prime
* Mod inverse
* Print
* Multiplication/subtraction with big integer
* Mod pow

1. Planning

For this lab we first started by looking at the requirements for the lab and talking about how we might go about it. We had to import a few things in the beginning which went along with the planning process. We looked over each formula and used static numbers instead of random ones to make sure our calculations were correct. Once completed, we used random numbers.

1. Implementation and Testing



We successfully ran this program with no errors.

1. Reflection

We could have created better variable names but at the time we thought they worked because these were the variable names in the formulas on the Wikipedia page. This lab really helped us to understand how RSA encryption works.