CS4150 : Computer Networks Lab Report

Lab-11 (RSA and Digital Signature)

1. Code Overview

- **def gcd (a, b)** is used to find gcd of two number a and b.
- **def findModInverse (a, m)** is used to find the modulo inverse of a and m.
- **def asciiConversion (eA, eB, nA, nB, dA, dB)** is used to convert parameter into ascii code.
- **def fileWrite5 (eA, eB, nA, nB, dA, dB)** is used write parameters into respective files.
- In the main function first I'm generating four prime numbers (pA, qA, pB, qB) in one of {10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30} bits. Then by using these prime numbers generating public keys and private keys for two users A and B. And storing ASCII code of these keys into respective files.